Advanced PRA Methods R&D Plan Assessment

February 2008 Letter Report

February 25, 2008

Prepared by:
J.L. LaChance, N. Bixler, J. Forester, R. Gauntt, B. Middleton, D. Robinson, K.C. Wagner, and D. Whitehead

Sandia National Laboratories
Albuquerque, NM 87185

Prepared for:
Division of
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

FOREWORD

In recent years, the NRC has focused on approaches intended to make best use of existing Probabilistic Risk Assessment (PRA) methods to address safety and regulatory issues. Development of new PRA methods may have the potential to more accurately or effectively address current and future safety issues (e.g., issues associated with new reactors). In its 2006 review of the NRC's research activities, the Advisory Committee on Reactor Safeguards (ACRS) noted that risk assessment is a crucial technology and recommended that the staff review ongoing developments. In its review of the NRC's Long Term Research Program, the ACRS reiterated this point, stating:

> "NRC's research has developed for the most part the PRA techniques in use today. PRA has become an essential element of the regulatory process. It is essential that NRC not allow development of PRA methods to stagnate. We certainly endorse continued examination of improved methods (including those for Level 1 PRA) to develop these methods and to improve the utility of these risk-assessment methods for the regulatory process."

As indicated in the staff's response to the ACRS review, the NRC is in the process of developing a PRA research and development (R&D) program plan. This plan will, among other things, consider advanced PRA modeling techniques and numerical analysis techniques from the perspective of both near- and longer-term regulatory needs.

To support this effort, Sandia National Laboratories (SNL) has been contracted by the NRC to perform an independent assessment of current state of the art PRA methods. PRA experts from Sandia identified challenging issues that can be addressed using current PRA models and methods, and potential new issues that will arise if these models and methods are applied to future nuclear applications. Sandia addressed how advanced PRA modeling and numerical analysis techniques that are under development can address these issues and challenges, and identified the strengths and weaknesses of the various modeling and analysis techniques for resolving them. The experts identified the most promising uses of the of the various advanced PRA modeling and numerical analysis techniques under development, and what is needed to bring the tools to fruition. All though the assessment focuses on PRA methods-related needs for reactors (both new and advanced reactors as well as operating reactors), it also addresses needs for some fuel cycle facilities.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

NOMENCLATURE

ATD	atmospheric transport and dispersion
ATWS	anticipated transient without scram
BDD	Binary Decision Diagrams
BBN	Bayesian Belief Network
BN	Bayesian Network
BWR	boiling water reactor
CCMT	cell-to-cell mapping technique
CDF	core damage frequency
CFD	computational fluid dynamics
DCH	direct containment heating
DFM	dynamic flowgraph methodology
ECCS	emergency core cooling system
EOC	error of commission
EOF	emergency operating procedure
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERG	emergency response guideline
FORM	First Order Reliability Method
GNEP	Global Nuclear Energy Partnership
GSI	Generic Safety Issue
HB	Hierarchical Bayes
HEP	human error probability
HFE	human factor event
HRA	human reliability analysis
IAEA	International Atomic Energy Agency
IPE	Individual Plant Examination
ISA	integrated safety assessment
LERF	large early release frequency
LRF	large release fraction
LHS	Latin Hypercube Sampling
LOCA	loss of coolant accident
LOSP	loss of offsite power
LPSD	low-power/shutdown
LWR	light-water reactor
MCUB	minimal cutest upper bound
MHTGR	Modular High Temperature Gas Reactor
MSL	Mars Science Laboratory
MMRTG	Multi-Mission Radioisotope Thermoelectric Generator
NEA	Nuclear Energy Agency
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NRR	Office of Nuclear Regulation
PBMR	Pebble Bed Modular Reactor

PDS	plant damage state
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSA	probabilistic safety analysis
PSF	performance shaping factor
PSHA	probabilistic seismic hazard analysis
PWR	pressurized water reactor
qMC	quasi-Monte Carlo
R&D	research and development
RCS	reactor coolant system
RES	Office of Nuclear Regulatory Research
RHR	residual heat removal
SAG	Severe Accident Guideline
SAMG	severe accident management guideline
SBO	station blackout
SME	subject matter expert
SNL	Sandia National Laboratories
SOARCA	state-of-the-art reactor consequence assessment
SORM	Second Order Reliability Method
SRP	Standard Review Plan
SSC	structures, systems, and components
USI	Unresolved Safety Issue

1. INTRODUCTION

In 1995, the Nuclear Regulatory Commission (NRC) issued a policy statement on the use of probabilistic risk assessment (PRA) in all regulatory matters. The policy statement states that "...the use of PRA technology should be increased to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach." The policy statement recognized that the NRC staff must continue to develop new and improved PRA methods and regulatory decision-making tools and must significantly enhance the collection of equipment and human reliability data for all of the agency's risk assessment applications. It also recognizes, and encourages, continuation of industry initiatives to improve PRA methods, applications and data collection to support increased use of PRA techniques in regulatory activities. With the current drive to build new reactors and the efforts to design advanced reactors, new advanced PRA methods may be more effective and accurate than existing PRA methods in addressing safety and regulatory issues. In addition, new PRA methods may be required to address specific design and regulatory issues related to advanced reactors (e.g., modeling of passive system and digital instrumentation and control).

This report presents an independent assessment of current advanced reactor PRA research and development (R&D) efforts in the context of their ability to address safety and licensing issues for both current and new reactors. In addition, it identifies areas where new R&D initiatives (both advanced methods and improvements in existing methods) may be required to address emerging issues for both existing and new reactors (including advanced reactor designs).

1.1 Background

Since the landmark Reactor Safety Study in 1975, the NRC has been an international leader in the development and use of risk information to support decision making. The 1995 PRA policy statement affirmed the Commission's belief that PRA methods can be used to derive valuable insights, perspective, and general conclusion as a result of an integrated and comprehensive examination of the design of nuclear facilities, facility response to initiating events, the expected interactions among facility structures, systems and components, and between the facility and its operating staff. The policy statement indicated:

1. The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

2. PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for additional regulatory requirements in accordance with 10 CFR 50.109. Appropriate procedures for including

PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

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

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

In response to this policy statement, the NRC in recent years has focused its attention on approaches intended to make the best use of existing PRA methods in regulatory matters. The NRC staff has indicated that development of new PRA methods may have the potential to more accurately or effectively address current and future safety issues (e.g., issues associated with new reactors). In its 2006 review of the NRC's research activities [1], the Advisory Committee on Reactor Safeguards (ACRS) noted that risk assessment is a crucial technology and recommended that the staff review ongoing developments. In its review of the NRC's Long Term Research Program [2], the ACRS reiterated this point, stating:

"NRC's research has developed for the most part the PRA techniques in use today. PRA has become an essential element of the regulatory process. It is essential that NRC not allow development of PRA methods to stagnate. We certainly endorse continued examination of improved methods (including those for Level 1 PRA) to develop these methods and to improve the utility of these risk-assessment methods for the regulatory process."

In a similar vein, the Advisory Committee on Nuclear Waste & Materials (ACNW&M), in its review of NRC's Long Term Research Program, stated that:

"The staff should ensure that [risk assessment] codes used in ISAs are up-to-date and should continue to develop them consonant with both their application to advanced systems and current computer technology. The best risk tools available should be applied to the design features and human actions that are important to facility operation and oversight."

Currently, the NRC is in the process of developing a PRA R&D program plan. This plan will, among other things, consider advanced PRA modeling techniques and numerical analysis techniques from the perspective of both near- and longer-term regulatory needs.

1.2 Objectives

To support the development of this PRA R&D plan, Sandia National Laboratories (SNL) has been contracted by the NRC to perform an independent assessment of current state of the art PRA methods. Sandia is uniquely qualified to provide this assessment. Sandia has been

involved in the development and application of PRA methods for approximately 30 years. This includes a prominent role in all of the NRC-sponsored bench mark PRA studies including NUREG-1150, the Risk Methods Integration and Evaluation Program (RMIEP), several low-power and shutdown (LPSD) PRA studies, and the Fire Risk Scoping Study. Currently, Sandia is leading the state of the art reactor consequence assessment (SOARCA) project. Sandia has also contributed to major PRA application studies that have addressed issues such as pressurized thermal shock, combustible gas control, decay heat removal, steam generator tube ruptures, and station blackout. Sandia has always been a major developer of state of the art PRA methodologies and codes including full-power and LPSD PRA methodologies (Level 1 through 3), the ATHENA human reliability analysis (HRA) process, PRA data analysis (NUREG/CR-6823), fire PRA (NUREG/CR-6850), and the MELCOR and MACCS codes.

More recently, Sandia has been supporting the NRC in developing PRA methods and data necessary for evaluating advanced reactors. These efforts have addressed passive system modeling and the data necessary for evaluating gas cooled reactors.

The overall objective of this project is to assess the state of the art in advanced PRA modeling and numerical analysis techniques. A review of these method's strengths and weaknesses in terms of how they apply to current and future nuclear safety issues is included in this report. The methods that have been identified as particularly promising are discussed in further detail.

The assessment focuses on PRA methods-related needs for assessing the risk from reactor operation (both new and advanced reactors as well as operating reactors), but also addresses risk assessment needs for some fuel cycle facilities. The considerations in performing the assessments include:

- current and potential future nuclear safety issues,
- the current PRA state of the art,
- the potential significance of the issues with respect to risk and to uncertainty in PRA results,
- the potential value and anticipated use of the methods and models, and
- the extent to which the modeling and analysis techniques are being currently developed in the U.S. and abroad.

The identification of the challenges to the use of current PRA method and models, and the assessment of the merits of advanced PRA modeling and numerical analysis techniques reflect the views of the PRA experts at SNL. The results of this project, and the basis for these results (including any key assumptions), are documented in this letter report.

1.3 Report Organization

This report documents an independent assessment by SNL PRA experts of the strengths and weaknesses of advanced PRA modeling and numerical analysis techniques that are currently under development and also identifies additional methods development that the SNL experts believe may be required for both new and advanced reactors. Section 2 discusses Sandia's

assessment approach including the identification of safety issues and PRA challenges and an evaluation of current PRA methods being developed to deal with these challenges. Section 3 presents the safety issues and PRA challenges as they pertain to light-water reactors and advanced reactors. Section 4 describes current PRA developmental efforts sponsored by the NRC and other groups. Section 5 presents subsections addressing specific areas that are relevant in evaluating state of the art methods. A summary of the assessment results are provide in section 6.

2. ASSESSMENT APPROACH

This chapter documents the approach that was proposed by Sandia for the assessment of advanced PRA methods and approved by the NRC staff. The context for this assessment is the adequacy of PRA models and techniques for evaluating current and future safety issues. Although the focus of the assessment was on advanced PRA methods, the SNL assessment also includes suggestions for improvements in existing PRA methods.

2.1 Summary of Approach

The Sandia assessment includes the following tasks and approaches:

1. Identification of current and potential safety issues for new and advanced reactors that can be assessed using PRA. Current safety issues pertinent to existing and new reactors were identified by reviewing existing documentation on current safety issues including outstanding generic safety issues and unresolved safety issues, and new emerging issues. In addition, future safety issues related to new and advanced reactor designs were identified based on existing assessments and knowledge of those designs. Passive system and digital I&C reliability are examples of the type of issues that were identified in this effort. Current and future PRA applications particularly in the risk-informed regulation (RIR) arena that present a challenge to existing methods were also identified. The literature search was supplemented by the knowledge of Sandia experts with regard to additional potential safety issues that can be addressed using PRA techniques and applications of PRA in the regulatory arena. This effort is documented in Chapter 3.

2. Identification of the current PRA state of the art methods development. Sandia experts in different areas of PRA identified the current state of the art in advanced PRA modeling and numerical analysis techniques currently under development. Sandia experts in all technical elements of Level 1, Level 2, and Level 3 PRAs; in the analysis of internal fires, floods, and external events; transportation risk; and in the evaluation of risk from LPSD modes of operation were utilized in this effort. The review focused on the research efforts being supported by the NRC. However, efforts were made to also examine industry funded efforts and international PRA modeling development (this effort was limited by the availability of information on industry and foreign developmental programs). Chapter 4 presents the results of this effort. The Sandia experts were also tasked to identify areas that may require new PRA R&D efforts not currently being addressed (documented in Chapter 5). The product of this effort is a compendium of current PRA developmental efforts and identification of additional areas that may require new methods development.

3. Review of the capability of advanced PRA modeling and numerical analysis techniques currently under development to address current and future safety issues and challenges. Sandia PRA personnel identified how the advanced PRA models and methods identified in Task 2 can address the safety issues and PRA application challenges identified in Task 1, particularly identifying any strengths and weaknesses in those applications. When

weaknesses were found in the methods currently under development, the most promising methods were identified and recommendations were made for resolving the weaknesses. The most promising uses of the techniques currently under development were also identified. In cases where no new methods are being developed to address a safety issues or PRA challenges or for addressing a weakness in existing methods, the need for new PRA methods was identified. In addition, alternative approaches to those currently under development that may better address safety issue resolution and PRA challenges were also identified. This effort is documented in Chapter 5.

2.2 Assessment Bases

This assessment of PRA R&D needs is based primarily on the need to address important safety and licensing issues for both current and new reactors and also to address challenges in the use of PRA. The identification of important issues and challenges is based primarily on NRC documentation but does include to some extent, issues identified by the Sandia PRA experts. In the latter case, the basis for the issue or PRA challenge is documented.

The assessed strengths and weaknesses of current and advanced PRA methods to address these issues and challenges are also based on the judgment of the experts. No prescriptive criteria were forced on the reviewers. However, in general, the following attributes were used in the process:

- ability of the method to address an important issue or existing PRA limitation,
- timing of the issue resolution (i.e., needed to resolve in either the short- or long-term),
- status of method development,
- ease in method application, and
- whether the method is widely accepted and in use (applicable only for existing PRA methods needing improvement).

3. SAFETY ISSUES AND PRA CHALLENGES

This chapter identifies safety issues for both current and advanced reactor designs that potentially can be addressed in a risk-informed framework. In addition, it identifies challenges to the utilization of current PRA methods in risk-informed applications. By identifying these issues and challenges, improved PRA methods needed to address these issues can be identified and evaluated. Although we are aware of most of the issues and the current status of their resolution, the following discussion may have missed some details. The NRC staff should review the following discussion taking into account their own knowledge base.

3.1 Current Safety Issues for Light-Water Reactors

Current LWR safety issues are listed in several sources. The primary source is NUREG-0933, "A Prioritization of Generic Safety Issues" [3]. NUREG-0933 describes the process for prioritizing identified safety issues in order to efficiently allocate resources to address the issues that have a high potential for reducing risk. Both operating and future plants are considered in the priority ranking process. The prioritization process is risk-informed in that it involves the generation of a quantitative risk estimate for each issue as well as a cost estimate for resolving the issue. A numerical impact/value ratio is calculated for each issue by dividing the estimated cost by the estimated potential for risk reduction. A priority ranking (HIGH, MEDIUM, LOW, or DROP) is assigned based on both the safety significance of the issue and the calculated impact/value ratio.

Most of the issues identified in NUREG-0933 have already been resolved and have resulted in new regulatory requirements including rule making, new Regulatory Guides, and changes to the Standard Review Plan (SRP); or a resolution mandated in NUREG-0737 [4]. The resolution of some of these issues included risk arguments generated using PRA models. The remaining issues that are applicable to operating and future reactor plants are listed in Appendix B of NUREG-0933, Revision 22. They include:

1. Issues that have been resolved with requirements (most of the issues listed in NUREG-0933, Revision 22 are in this category)
2. Issues categorized as HIGH- or MEDIUM-priority issues and scheduled for resolution (only three issues are HIGH priority, none are MEDIUM in NUREG-0933, Revision 22)
3. Unresolved safety issues (USIs) scheduled for resolution (none in NUREG-0933, Revision 22)
4. Issues that are scheduled for prioritization (one issue is identified in NUREG-0933, Revision 22)

In accordance with 10 CFR 52.47(a)(1)(iv), any future application for design certification must contain proposed technical resolutions for the issues in categories 2 and 3 above. In addition, future reactors must also address issues that were resolved with no impact on operating reactors but contain recommendations for future reactor plants. In Revision 22 of NUREG-0933, Appendix B, there is only one issue in this category: Generic Safety Issue (GSI) 89 – "Stiff Pipe

Clamps." A summary of the outstanding GSIs that must be addressed by both current and future reactor plants is provided in Table 1.

Table A Outstanding Generic Safety Issues

Issue No.	Title	Discussion
GSI-89[1]	Stiff Pipe Clamps	This issue involves the potential that stiff pipe clamps could induce pipe stresses. Possible solutions listed in NUREG-0933 did not include the use of PRA methods.
GSI-156.6.1[2]	Pipe Break Effects on Systems and Components	This issue addresses the safety concern of whether the effects of pipe breaks inside containments have been adequately addressed in the design of some plants. Risk significance of pipe break effects inside the containment can be evaluated using PRA. Currently, such effects are generally excluded from PRAs. The reevaluation of 10 CFR 50.46 is considering this issue.
GSI-163[2]	Multiple Steam Generator Tube Leakage	This issue addresses the safety concern associated with multiple steam generator tube leaks during a main steam line break that can not be isolated. This issue is an integral part of the NRC Steam Generator Action Plan. PRA is being used to evaluate the risk associated with steam generator tube ruptures.
GSI-191[2]	Assessment of Debris Accumulation on PWR Sump Performance	This issue addresses the potential for debris blockage of PWR sumps. The frequency of core damage due to debris induced loss of ECCS recirculation was evaluated in NUREG/CR-6771 [5].
GSI-199[3]	Implications of Updated Probabilistic Seismic Hazard Estimates in Central and Eastern United States	This issue addresses the concern for the seismic design bases of all nuclear power plants in the central and eastern United States, based on the new composite seismicity model for this region. This issue has not yet been prioritized.
GSI-186[4]	Potential Risk and Consequences of Heavy Load Drops in Nuclear Power Plants	This issue resulted from a NRC staff review of licensee programs for handling heavy loads which revealed a substantially greater potential for severe consequences resulting from the drop of a heavy load. The resolution of this issue does not involve the use of PRA.
GSI-189[4]	Susceptibility of Ice Condenser Containments to Early Failure from Hydrogen Combustion During a Severe Accident	Efforts to risk inform 10 CFR 50.44 indicated these types of plants are potentially susceptible to failure due to hydrogen combustion during a severe accident. Analysis of the issue involved the use of risk assessment techniques.

Table A Outstanding Generic Safety Issues

Issue No.	Title	Discussion
GSI-193[4]	BWR ECCS Suction Concerns	This issue addresses the concern for the possible failure of ECCS caused by unanticipated, large quantities of entrained gas in the suction piping from BWR suppression pools. This issue could be evaluated using PRA techniques.

Notes:
1   New requirements for future plants recommended on this issue.
2   High-priority safety issues.
3   Issue to be prioritized in the future.
4   Work on these issues is in progress.

Issues that are of sufficient gravity that they may require immediate action are excluded from the prioritization process in NUREG-0933. Generally, immediate actions take the form of a Bulletin or Order. In addition, issues that do not meet the criteria for designation as generic issues but are important to the safety at specific plants are brought to the attention of licensees through issuance of Information Notices and /or Generic Letters. Generic Letters can also require licensees to perform analyses to address issues. An example is Generic Letter 88-20 which requested all licensees to perform an Individual Plant Examination "to identify any plant-specific vulnerabilities to severe accidents and report the results to the Commission." Currently there are 106 of these types of generic communications listed in Appendix E of NUREG-0933.

Other issues that did not meet the criteria for designation as a generic issue have been deemed important enough to require the development of action plans to address those concerns. Some of the issues addressed by action plans are listed below (all except the last one are discussed in Appendix D of NUREG-0933) and most have utilized PRA methods in the issue resolution:

- cracking of BWR reactor internals (PRA was used to verify the prioritization schedule for the internals inspection program [6]),
- pressurized thermal shock (PRA was used to assess the potential for vessel failure [7]),
- dry cask storage of spent fuel (a risk assessment was recently completed and documented in NUREG-1864 [8]),
- effectiveness of Thermo-Lag fire barriers (not addressed with PRA),
- reactor coolant system drain down during refueling (resolved by evaluating the potential for this event and the conditional core damage probability),
- updating the SRP for use in licensing new reactors (not addressed with PRA),
- PRA implementation plan (has led to the NRC increasing their use of PRA in regulatory matters), and
- steam generator tube ruptures (utilizes risk methods to evaluate the risk from tube ruptures [9]).

To address emerging issues subject to risk-informed decision making, the NRC Office of Nuclear Reactor Regulation (NRR) has established LIC-504, "An Integrated Risk-Informed

Decision-Making Process for Emergent Issues" [10]. The policy identified in LIC-504 includes the use of sound science and state-of-the art methods to establish risk-informed decisions that are not covered by established regulatory processes. As with any risk-informed application, the risk evaluation must be capable addressing the issue at hand, have the appropriate PRA scope, and address defense-in-depth, and safety margins. Although it is not possible to determine what PRA methods need to be developed to address future, unforeseen issues, it is clear that the improving the state-of-the-art in PRA will improve the potential that risk-informed methods can be used in their resolution.

3.2   Safety Issues Related to Advanced Reactor Designs

Technical issues identified by the USNRC staff throughout the review of several advanced reactor designs (PRISM, MHTGR, CANDU 3, and PIUS) were presented to the commissioners in SECY-93-092 [11]. Ten issues were identified during the preliminary review of these designs that were a result of the applicants proposing to deviate from current light-water reactor (LWR) when existing regulations were not applicable to the technology or when the applicant considered deviation warranted on the basis of the reactor design and their proposed alternative criteria. Some of these issues are applicable to existing and advanced light-water reactors. The ten issues are listed below with the NRC staff recommendations at that time and possible uses of PRA-related methods and improvements needed to address the issue (the reader is encouraged to review SECY-93-092 for a complete description of these issues):

1. Accident Evaluation – The issue was to identify appropriate event categories, associated frequency ranges, and evaluation criteria for events that would be used to assess the safety of advanced reactors. Advanced reactor designers proposed to analyze events that are less probable than the present design basis accidents for LWRs and to ensure that these accidents will have acceptable consequences (dose levels) to the public. The NRC staffs recommendation was to select licensing events deterministically supplemented by insights from a PRA for the design. A full Level 3 PRA would be beneficial in such an effort. It should be noted that the process for determining licensing basis events proposed in NUREG-1860 [12] is similar to the applicants suggested approach which is also being pursued by the designers of the PBMR.

2. Source Term – The issue is whether mechanistic source terms should be used to evaluate proposed designs. Advanced reactor applicants proposed to use siting source terms from the accidents considered in the design of the reactor rather than the non-mechanistic approach specified in 10 CFR Part 100. The staffs' recommendation was that a mechanistic analysis should be utilized as long as the modeling capability is realistic as possible. In fact, this recommendation was made previously for LWRs and resulted in an alternative source term approach documented in NUREG-1465 [13]. The severe accident behavior predicted in a realistic Level 2 PRA for advanced reactor (or LWR) designs could be utilized in this mechanistic approach.

3. Containment Performance - The issue is whether advanced designs will be allowed to employ alternative approaches to traditional leak tight containments (e.g., by using high-integrity fuel particles and a confinement building such as proposed for the PBMR). The staff concluded that new reactor designs with limited operational experience require a containment system whose integrity must be maintained for 24 hours after core damage

(part of defense-in depth philosophy). A full Level 3 PRA would provide an assessment of fission product release and alternative containment designs. Development of models to address the behavior of advanced fuel, reactor, and containment/confinement designs during licensing basis events (including severe accidents) will be required.

4. Emergency Planning – The issues is whether advanced reactors with passive design safety features should be able to reduce emergency planning zones and requirements. The NRC staffs recommended that no changes to existing regulations governing emergency planning be made at that time. The staff also indicated that accident analysis as outlined under Accident Evaluation be factored into emergency planning (part of defense-in depth philosophy). Thus again, a full Level 3 PRA could be used to assess this issue further.

5. Reactivity Control System – The issue is whether a reactivity control system that does not utilize control rods (e.g., liquid boron injection systems) can be used in a reactor. The NRC staff concluded that a reactivity control system without control rods could be acceptable if an equivalent level of safety is provided. Part of this evaluation could involve a risk assessment of ATWS events.

6. Operator Staffing & Function – The issue is whether advanced reactor designs should be allowed to operate with a staffing complement that is less than that currently required by LWR regulations. The NRC staff concluded that operator staffing may be design dependent and intends to review any justification for a smaller crew size by evaluating the function and task analyses for normal operation and accident management. The HRA evaluations performed for the plant PRA can provide insights into this issue.

7. Residual Heat Removal - The issue is whether an advanced reactor design that relies upon a single completely passive, safety-related residual heat removal (RHR) system is acceptable. Several advanced reactor designs utilize such systems. The NRC staff indicated that a single, completely passive, safety-related RHR system may be acceptable. Research efforts have focused on evaluating the reliability of such passive systems.

8. Positive Void Reactivity Coefficient – The issue is whether a reactor design in which the overall inherent reactivity tends to increase under specific conditions or accidents would be licensed. Sodium voiding during postulated core disruptive accidents in liquid sodium reactors can lead to positive reactivity coefficients but this is offset by negative temperature reactivity feedback. The NRC staff proposed that applicants of advanced reactor designs with positive void coefficients (e.g., liquid sodium and CANDU 3 reactors) analyze the consequences of events such as ATWS, unscrammed LOCAs, and transients affecting reactivity control that could lead to core damage as a result of positive void coefficients. The staff action could thus depend on the results of risk assessment results for these types of accidents.

9. Control Room and Remote Shutdown Area Design – The issue is whether current requirements for a seismic Category I/Class 1E control room and alternate shutdown panel be fulfilled by a remote shutdown area and a non-seismic Category I, non-Class 1E control room. Several advanced reactor designs did not have safety class control rooms or alternate shutdown panels based on the argument that accidents do not require operator response due to the passive safety features of the designs. The staff disagreed with this

conclusion and stated that "Until passive LWR policy for design requirements of control rooms and remote shutdown facilities is determined, the staff will apply current LWR regulations and guidance to the review of advanced designs." Thus, this issue could benefit by the evaluation of passive safety system reliability in achieving safe shutdown during postulated accidents.

10. Safety Classification of Structures, Systems, and Components – This issue concerns the criteria for determining safety-related structures, systems, and components (SSCs) in advanced reactors. For advanced reactor designs that utilize passive systems, the number of specified safety-related SSCs is substantially less than for current LWRs. In addition, non-safety related active systems are also utilized in some designs to provide defense-in-depth capabilities for reactor coolant makeup and decay heat removal. The staff position at that time was to apply current LWR criteria for identification of safety-related SSCs in advanced reactors and that requirements for non-safety-related systems be consistent with the NRC position for passive LWRs. The NRC development of 10 CFR 50.69 addresses the use of risk-informed processes to classify SSCs.

In the SRM for SECY-93-092, the Commission approved the staff's recommendations for issues 1, 2, 3, 5, 6, 7, and 8. The Commission concluded that there was insufficient information at that time to reach a conclusion on the emergency planning and to depart from current control room and safe shutdown requirements, and that resolution of the safety classification issue should await further development of the advanced reactor designs.

Following a large transition in the Commission and ACRS members, the first four issues were again revisited in SECY-02-0139 [14] and again in SECY-03-0047 [15] with similar or updated recommendations by the USNRC staff. Three overarching policy issues were identified:

- How should the Commission's expectations for enhanced safety be implemented for future non-LWRs? The safety of advanced plants can be quantitatively measured using a Level 3 PRA.

- Should specific defense-in-depth attributes be defined for non-LWRs? Defense-in-depth can be partially evaluated using PRA.

- How should NRC requirements for future non-LWR plants relate to international safety standards and requirements? This issue can not be addressed with a PRA application.

In addition, four policy issues were identified that had a more specific technical nature including implications for PRA methods and use:

- To what extent should a probabilistic approach be used to establish the plant licensing basis? The NRC staff recommended that a probabilistic approach be used in the identification of events to be considered in the reactor design and the safety classification of structures, systems, and components; and replace the single failure criterion with a probabilistic (reliability) criterion.

- Under what conditions, if any, should scenario-specific accident source terms be used for licensing decisions regarding containment and suitability? The NRC staff recommended the use of scenario-specific source terms, provided there is sufficient

understanding and assurance of plant and fuel performance and deterministic engineering judgment is used to bound uncertainties.

- Under what conditions, if any, can a plant be licensed without a pressure retaining containment building? The NRC staff recommended the use of functional performance requirements to establish the acceptability of a containment or confinement structure (i.e., a non-pressure retaining building may be acceptable provided the performance requirements can be met). This recommendation is coupled to the recommendations on Issues 4 and 5 (event selection and source term) discussed above and, similar to those issues, would represent a risk-informed and performance-based method to account for the unique aspects of each reactor design.

- Under what conditions, if any, can emergency planning zones be reduced, including a reduction to the site exclusion area boundary? The NRC staff recommended that that no change to emergency preparedness requirements be made.

In the SRM for SECY-03-0047, the Commission approved the staff's recommendations for three of the four technical issues, the exception being the containment/confinement building issue. The Commission concluded that there was insufficient information at that time "to prejudge the best options and make a decision on the viability of a confinement building." The staff was directed to develop functional performance standards and then submit options and recommendations to the Commission. With regard to the policy issues, the staff was directed to establish a usable definition of core damage and to determine if the concept of large early release frequency is meaningful or if a Level 3 PRA would be required. The staff was also directed to consider updating the Commission Policy Statement on "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" to include a more explicit definition of defense-in-depth, risk-informed regulation, and performance based regulation.

3.3 PRA Challenges in Risk-Informed Regulation

The Commission PRA Policy Statement encourages greater use of PRA to improve safety decision making and regulatory efficiency, including the use of PRA to support decisions to modify an individual plant's licensing basis. The risk-informed approach enhances the traditional deterministic approach by:

- explicitly considering a broader range of safety challenges
- prioritizing the challenges on the basis of risk significance, operating experience, and engineering judgment
- considering a broader range of countermeasures to mitigate the challenges
- explicitly identifying and quantifying uncertainties in analyses
- testing the sensitivity of the results to key assumptions

A risk-informed regulatory approach is also used to identify insufficient conservatism and provide a basis for additional requirements or regulatory actions. The NRC is actively moving toward increasing the use of risk insights and information in three strategic arenas: nuclear reactor safety, nuclear materials safety, and nuclear waste safety.

In the reactor safety arena, risk-informed activities occur in five broad categories: (1) applicable regulations, (2) licensing process, (3) revised oversight process, (4) regulatory guidance, and (5) risk analysis tools, methods, and data. Activities within these categories include revisions to technical requirements in the regulations; risk-informed technical specifications; a new framework for inspection, assessment, and enforcement actions; guidance on risk-informed in-service inspections; and improved standardized plant analysis risk models.

Licensed activities addressed under the materials and waste safety arenas include uranium recovery, sealed sources and devices, irradiators, interim storage of spent fuel, transportation of radioactive materials, disposal of spent fuel, decommissioning, waste disposal, medical use of isotopes, nuclear fuel fabrication, and uranium enrichment. This diversity of regulated activities presents special challenges because a single approach to "risk-informing" the materials and waste regulatory applications is not practical.

Many of the risk-informed efforts that have been pursued for reactors are related to resolution of issues identified in Sections 3.1 and 3.2, some of which have lead to rule making to utilize risk-informed approaches in licensing actions. Other applications address the need to focus resources on safety-related items and thus increase the effectiveness of the NRC and reduce unnecessary burden on licensees as well as the NRC. Some areas where risk-informed approaches have been applied include:

- Reactor oversight process
- Modifications to individual plant licensing basis (Regulatory Guide 1.174 applications)
- In-service inspection (Regulatory Guide 1.178)
- In-service testing (Regulatory Guide 1.175)
- Technical specifications (Regulatory Guide 1.177)
- Special treatment requirements (10 CFR 50.69)
- Combustible gas control in LWRs (10 CFR 50.44)
- Acceptance criteria for the ECCS in LWRs (10 CFR 50.46)
- Fire protection
- Pressurized thermal shock rule
- Steam generator tube ruptures
- Station blackout rule
- ATWS rule
- Maintenance rule

Although, risk-informed regulation is viewed by NRC and industry as highly successful, there remain several technical challenges related to the use of PRAs in risk-informed regulation. Some of the challenges listed below were identified through interviews of key NRC staff members and selected industry representatives which was documented in NUREG/CR-6813 [16]. Other challenges were identified by the Sandia experts involved in this assessment. Important PRA challenges for use in risk-informed applications include the following:

1. Scope of the PRA used in the applications – Many plants do not have LPSD or seismic PRAs. When the scope of the PRA is incomplete, the PRA must be either upgraded to

include the missing pieces, or it must be demonstrated that the missing elements are not significant risk contributors.

2. Risk metrics - For LWR applications, CDF and LERF are the metrics used in most risk-informed applications. Different metrics will likely be required for advanced reactors.

3. Lack of completeness within the specified scope –Examples of this is included inadequate treatment of support system initiators, inadequate resolution of accident sequences, and inadequate treatment of dependencies, particularly those involving human actions.

4. PRA quality – The quality of a PRA used in a risk-informed application must be addressed per the requirements in Regulatory Guide 1.200.

5. Aggregation of results from different levels of analysis – Current fire PRAs involves conservative screening and evaluation of the risk from internal fires. Aggregation of results from analyses with different levels of detail and approximation can bias a risk-informed decision.

6. Treatment of aleatory and epistemic uncertainty in the PRA – Parameter uncertainty must be addressed to ensure that point estimates of the required metrics represent means. Modeling (epistemic) uncertainties need to be evaluated to ensure the robustness of risk-informed decisions.

7. PRA quantification – Truncation and simplification methods used during PRA quantification can significantly affect the value of importance measures used in many risk-informed applications.

8. Reliability of digital systems- Methods to evaluate the reliability of digital systems need to reach maturity.

9. Reliability of passive systems – The functional reliability of passive systems must be determined to evaluate the risk for advanced reactor designs.

10. Treatment of aging – Long-term degradation of passive components due to corrosion and other aging mechanisms is generally not performed.

11. Latent human errors - Consideration of errors in the design and construction of digital and passive systems is necessary to evaluate their reliability.

12. Errors of commission – Errors of commission are generally excluded from HRA evaluations.

More detailed descriptions of these PRA-related challenges are presented in Chapter 5. Many of these challenges are being addressed by the NRC through their research efforts. Chapter 4 presents a summary of current NRC research efforts. It should be noted that although many of these challenges do not require advanced PRA modeling, they do require improvements in existing PRA methods.

4. CURRENT PRA R&D EFFORTS

This chapter briefly describes PRA research efforts sponsored by the NRC, U.S. industry, and foreign entities. The primary focus is on the NRC-sponsored research since limited information on industry and international efforts is available. Although every effort was made to identify NRC planning documents related to PRA R&D projects, it is recognized by the authors that some likely will have been missed. While the emphasis of this review is on identifying advanced PRA modeling projects, other PRA-related efforts are also identified. Pertinent PRA projects are reviewed in Chapter 5 with regard to their strengths and weakness in addressing the issues identified in Chapter 3.

4.1 PRA Research Sponsored by the NRC

Current risk-informed activities being pursued by the NRC are listed in the Risk-Informed and Performance-Based Plan (RPP) database located on the NRC Web site (http://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp.html). The RPP database provides a high-level summary of RPP initiatives and their status. The RPP replaces the risk-informed activity documentation presented in the Risk-Informed Regulation Implementation Plan (RIRIP) [17]. A summary of PRA research efforts at the NRC listed in these documents is presented in Appendix A. PRA projects are also listed in the ACRS review of NRC safety research program, NUREG-1635 [18].

In 2003, the NRC staff issued SECY-03-0059, "NRC's Advanced Reactor Research Program" [19]. With regard to PRA, the objectives of the identified activities was to develop guidance for reviewing PRAs submitted as part of an advanced reactor licensing application and to support the development of a risk-informed regulatory framework. Specific tasks related to advanced reactor PRAs include:

- Initiating event identification and quantification
- Accident progression and containment performance (including source term)
- Systems modeling of passive and digital systems
- Data collection and analyses for advanced reactor components
- Human reliability analysis methods for advanced reactor designs
- Risk metrics for advanced reactors
- Integrated safety, safeguards, and security

The research activities described in the above documents are for short-term activities. In October 2007, the NRC staff issued a long-term research plan [2] that documents future technical issues and associated long-term (i.e., greater than 5 years) regulatory research activities which are not currently identified within the agency's planning documents. With regard to PRA, the long-term research plan discusses advanced modeling techniques for Level 2/3 assessments. Specifically, it describes the use of dynamic techniques to better integrate phenomena-based modeling into risk assessment and the development of fast-running phenomenology-based Level 2 computer codes.

Examination of the NRC-sponsored activities indicates that the majority of the projects are related to extension of existing PRA methods and risk-informed applications. The following projects were considered by the authors as advanced PRA R&D efforts:

- Digital systems PRA – The major activity under this initiative is to identify or develop acceptable modeling methods, assess failure data, determine criteria for the level of modeling, assess uncertainties and determine how to interface digital systems with the rest of a PRA.
- Passive system modeling methods - Includes a review of passive system modeling techniques and recommendations on the best approaches, and an application of a selected method on an advanced reactor design.
- Dynamic PRA methods development – Includes support for development of two different approaches.
- State-0f-the-ARt Consequence Assessment (SOARCA) project - The SOARCA is a project that will be used to develop a realistic estimate of the potential effects on the public from a nuclear power plant accident, where low-likelihood scenarios could release radioactive material into the environment and potentially cause offsite consequences. The project will also evaluate and improve, as appropriate, methods and models for realistically evaluating both the plant response during such severe accidents, including evacuation and sheltering and the potential public risk.

4.2 Industry Sponsored PRA Research

The primary industry group performing PRA research is the Electric Power Research Industry (EPRI). The Risk and Safety Management program at EPRI develops analytical tools and methods that nuclear utilities can use to function more effectively in a risk-informed regulatory environment. Some of the PRA developmental efforts performed under this program include:

- Next generation of PRA tools
- Uncertainty in risk-informed decision making
- Seismic PRA methods
- Fire PRA methods
- HRA methods for fire PRA
- Risk-informed regulatory support
- Configuration risk assessment
- Grid risk and reliability
- Risk Analysis and Management for Critical Asset Protection (RAMCAP) security assessments
- Internal Flooding Guide
- Treatment of loss of offsite power in PRA
- Declarative Modeling Software

Details about these projects are not readily available. However, many of these activities appear to address some of the issues and PRA challenges identified in Chapter 3. Several of these projects are joint efforts with the NRC include development of a fire PRA methodology and fire

17

HRA methods. EPRI is also coordinating efforts with the NRC in developing guidance on incorporating uncertainty into risk-informed decision making.

One known project at EPRI related to advanced PRA methods involves development of advanced quantification techniques. Concerns about the use of PRA quantification approaches such as the Minimal Cutset Upper Bound (MCUB) with truncation resulting in inaccurate risk results including misleading importance measures has lead EPRI to explore the use of Binary Decision Diagrams (BDDs) to generate exact solutions of fault trees. Since the use of BDDs is currently only possible with small fault trees, EPRI is exploring the use of a combination of quantification approaches to solve fault tress in an optimal manner.

4.3   International PRA Research

Several international groups support the development and application of PRA. They include the Nuclear Energy Agency (NEA), a specialized agency within the Organization for Economic Co-operation and Development (OECD) and the International Energy Agency (IAEA). Both organizations have member states which they rely upon for financial and technical support.

Risk assessment activities within the NEA are performed under a working group on risk assessment (WGRISK). Over the past twenty years, WGRISK has looked at the technology and methods used for identifying contributors to risk and assessing their importance. Work during much of this period was concentrated on Level-1 PSA methodology. In recent years the focus has shifted into more specific PSA methodologies, issues, and risk-informed applications, including:

- human reliability
- software reliability
- low power and shutdown risk
- seismic PRA
- other external events
- risk criteria
- Level 2 PRA

Specific information on these projects is not readily available. However, all of these activities address issues and challenges identified in Chapter 3.

The IEA has several active PRA activities they are currently pursuing. They include:

- safety significance of near field earthquakes
- safety significance of long-term reactor operation and aging management
- safety performance indicators for fuel cycle facilities
- assessment of source term, radionuclide transport within containment/confinement and release to the environment for research reactors
- development of a methodology for risk-informed in-service inspections
- analysis and development of safety performance indicators for nuclear power plants

18

Specific information on these projects is not readily available. However, all of these activities
address issues and challenges identified in Chapter 3.

5. EVALUATION OF CURRENT STATE-OF-THE-ART PRA METHODS DEVELOPMENT

This chapter provides an assessment by SNL PRA experts of the current state-of-the-art PRA methods development. Although the primary focus is on assessing the NRC PRA R&D program, some discussion is presented on industry and international developmental efforts. The assessment is subdivided into two topical groups: advanced PRA methodologies and enhancements of existing methodologies. The advanced PRA discussion begins with a general discussion that provides a general basis for covering such topics as passive system modeling, dynamic PRA, and the type of uncertainty techniques that would be useful in both applications. This group of topics also includes assessments of Level 2 and 3 PRA techniques, digital system modeling, and advanced numerical techniques. The second topical group includes an assessment on research efforts related to existing PRA methods. Included under this area are HRA, fire and seismic PRA, and transportation risk assessment.

The assessment approach documented in Chapter 2 was utilized and involved the identification of both strengths and weaknesses of current PRA development efforts for addressing safety and licensing issues, and to meet existing PRA challenges. Suggestions for pursuing specific areas of R&D are provided.

5.1 Advanced PRA

The intent of this section is to open a dialogue on what the next generation of PRA should look like. As a bit of foreshadowing, the section does not present a specific solution. Rather, it identifies what characteristics advanced PRA methods should have, suggests that there are limitations to current methods, and of holes in what has been done thus far.

Dynamic PRA and passive system modeling and required uncertainty techniques are not treated as separate topics, but rather as something falling under the general umbrella of "Advanced PRA." Considerable effort has been expended on various passive system modeling and dynamic PRA methods many of which have resulted in quite exceptional insights into unique risk analysis problems. The intent of the following discussion is not meant to be disparaging to these research activities in any sense, but to highlight specific positive or negative aspects of various approaches.

5.2 Desired Characteristics of Advanced PRA

Before jumping into assessing the limitations of existing PRA methods, it is beneficial to approach the assessment from the perspective of what type of problems needs to be addressed and what general issues are involved. We will not be able to address all these issues with a single method, but this will provide a basis for comparing various advanced PRA methods.

To do a thorough risk analysis it is necessary to consider all information available. Data and information gathering is growing increasingly expensive and we must be efficient in how the data is acquired and used. The risk analysis approach *must be applicable during all-phases of*

analysis, with equal emphasis on being useful during system design as well as during system operation and retirement. Early in the system design, a risk analysis can have the largest payback for dollar invested. However, this is when the least is known about the system and therefore presents a unique challenge.

Certainly testing of complete systems is seldom accomplished and a significant amount of testing of even moderately complex subsystems is becoming increasingly rare. Whatever method is used should have the *capability to help focus data gathering* so that the information garnered from testing has the greatest impact on characterizing system risk.

The approach must have the *capability to include data from all levels of system indenture* and data from similar systems, e.g. different suppliers of diesel generators. Test data might be available from connectors, complete power conditioning systems or from complete system tests.

It *must be possible to consider data from a variety of sources*. Risk analyses are growing increasingly dependent on the use of computer simulation. Structural analysis, vibration characterization, fluid flow, and thermal balance modeling are only a few of the very difficult situations where computer modeling has been a critical element in system analysis. It is essential that information from these computer simulations be available in the risk analysis. Along a similar line, passive systems present a unique challenge to traditional PRA; there is general reliance on computer simulations to characterize the operation of passive systems. Not all data are created equal and traditional fault tree methods have no object means of differentiating between failures from computer simulations, failures observed during accelerated testing, and failures observed in an operational environment. In addition, expert opinion is treated the same as field data.

Failure information might be available as either probability point estimates or the more desired situation of a complete density function description. Clearly the estimates of risk for any system involve a degree of uncertainty. If this uncertainty is not characterized and considered, then the value of additional testing, computer modeling is without a foundation. Any new approach must be *capable of dealing with both types of probability information: point estimates and full conditional density function*.

Many times the only data available is expert opinion; it is important that an advanced PRA method be capable of not only *incorporating expert information*, but all be able to assess the sensitivity of the results to expert judgment.

This is distinct from the *need to be able to deal with human error* from the perspectives of both omission and commission. With the possible increasing reliance on passive safety systems, undesired human intervention in a passive system will become more likely.

Consideration of time dependent behavior is becoming a necessary capability of PRA. Operation of complex systems is becoming increasingly dependent on digital instrumentation and control systems. These types of systems typically operate in a rather discrete fashion, controlling a unique sequence of events. While a bit of a generalization, these systems differ from traditional event modeling in the shear number and complexity of the sequence of discrete events that are

possible. In addition to discrete event sequence modeling, characterization of degradation in a more continuous sense is also required, e.g. corrosion. Related issues include failure due to fire progression, and seismic induced events. So whatever approach is finally identified, it is critical that the approach have the *capability to include both discrete and continuous forms of time dependent degradation and failure.*

Non-proliferation issues suggest there will likely be less capability to do preventive maintenance and there may be increased dependence on real-time monitoring. Perhaps not an essential but a strongly desired capability is related to the *ability to incorporate performance degradation data from real-time monitoring* in a risk analysis. This would assist in a faster response time to failure events, possibly even promoting preventive action in contrast to post-event reaction to failure.

Finally, each of these capabilities carries a burden of an inherent level of uncertainty. These uncertainties accumulate to point where they can have a significant impact on the confidence we have in our probabilistic characterization of risk. Computer models are certainly only abstractions of some physical system or operation. Even test data, while the best of possible data sources, is generally collected under artificial circumstances. On the other end of the scale, expert judgment is by its nature fraught with uncertainty. Must understand and appreciate the weaknesses in the risk analysis and the value of additional information to increase the confidence in the final risk assessment. It is imperative that whatever approach (or approaches) is chosen, that it is *capable of characterizing the inherent uncertainty in the PRA results.*

The above is not a complete list, but it does provide a basis for assessing the basic capabilities of what has been done thus far and evaluating the potential of these methods for new research.

5.2.1.1 Dynamic Flowgraph Methods

NUREG/CR-6901 [20] made an attempt to review a number of possible methods for dynamic PRA with the specific focus on risk assessment of digital systems. The focus was on Markov modeling, dynamic flowgraph modeling and Petri nets. Other methods upon which judgment fell included: dynamic event trees, Monte Carlo, dynamic fault trees, all Bayesian methods, GO-FLOW, event sequence diagrams, and a number of other variations on these. The conclusion of the report was that dynamic flowgraph modeling (DFM) was the clear winner followed by Markov modeling.

Despite making some strong conclusions on fairly weak arguments, one important, critical point was raised: *for systems where dynamics operation is an important consideration in a risk analysis, the fault/event/sequence tree topology may change over time.* The general approach used by DFM and its cousins is to generate the fault tree continuously as the system operates and the system state changes.

The 'real-time' generation of fault trees can be quite complex for even simple systems. Some very impressive software tools have been developed to assist and these are summarized in NUREG/CR-6942 [21] (as well as the presentations at the PRA/PSA workshop held 22-23 October, 2007).

In general, the dynamic generation of failure event sequences has been used for many years (e.g. Cassini launch risk analysis). It is an important capability of any next generation risk analysis methodology. Unfortunately, it has a few significant limitations that keep it from being a risk analysis panacea. These include the difficulty with complexity growth as time intervals become smaller, such as in the case of a degradation process like corrosion. The number of discrete decision points becomes immense. In general, DFM-type methods can only deal with a small subset of the type of time dependent elements within a risk analysis.

NUREG/CR-6942 suggests that to handle continuous time processes, the best alternative is the Cell-to-Cell mapping technique (CCMT). However, while CCMT is continuous time, it is fundamentally a discrete state space approach. Degradation processes are not often very discrete.

DFM-type methods provide only a point estimate of the risk; there is no consideration of uncertainty in risk estimates. It might be possible, with considerable effort, to formally include uncertainty. The alternative would be to drop DFM-type methods and investigate alternatives with inclusion of uncertainty a specific objective.

Finally, even for analyses where DFM is most applicable, DFM-type methods are not very effective during system design without a considerable suite of assumptions.

5.2.1.2 Shell Method

Wrapper methods of risk analysis involve a shell or 'wrapper' around a traditional engineering analysis tool, i.e. finite element code. This type of approach is being researched by Ohio State University. In the simplest form, the shell sampled a set of system parameters from appropriate probability distribution functions and then executed an analysis packages using these values for input. Various outputs of the analysis package were monitored and collected for statistical analysis. Typical shells might involve either Monte Carlo type methods or Derivative Methods.

The underlying analysis package might be something as simple as a single equation describing the boundary between success and failure for a system. With the evolution of high performance computing these analyses often involved detailed physical models of, for example, thermal dynamics, fluid flow, or structural dynamics. These models are relatively detailed and can sometimes take hours to perform a single analysis. Examples of such analysis codes might include MELCOR or RELAP.

The shell or wrapper, involved random sampling methods such as plain Monte Carlo, Latin hypercube sampling (LHS), quasi-Monte Carlo (qMC) sampling, importance sampling, and a multitude of variations. These methods, LHS in particular, became very popular with nuclear power plant risk analysts. In addition to random sampling methods, derivative methods gained popularity in the structural reliability area and formed the basis for many new structural building codes. As the name implies, derivative methods require first or second order derivative information. For complex problems, these are usually found using simple perturbation about a local point. This local point changes as the solution converges and, if the underlying system

23

performance function is not 'smooth' than these derivatives can be troublesome and then FORM/SORM may be inappropriate. Sandia explored the state of the art in derivative methods in 1998 and published a survey of techniques [22]; a number of unpublished reports of Monte Carlo methods followed but were unpublished as funding dried up [23 & 24].

Typical methods include First-order and Second-order Reliability Methods (FORM/SORM), fast probability integration, and again, a multitude of variations. Probably the most extensive software package used to evaluate new shell methods was the CRAX/Cassandra package developed at Sandia. [25]

Monte Carlo methods suffer from the shear number of analysis simulations. LHS provides significant relief in this respect, and qMC offers some unique advantages for large analyses. Derivative methods significantly reduce the number of simulations even further than either LHS or qMC methods, but suffer from difficult approximations for significantly non-linear analysis problems.

An alternative method that blends the best of the Monte Carlo simulations with the best of the derivative methods was developed at Sandia in 1999 and a patent application was submitted. This new approach significantly reduced the number of simulations required with no loss in accuracy. (The application eventually expired due to lack of funding.) [26 & 27].

The difficulties with the shell method include:

- Need for a detailed model of the physics associated with the operation and failure of the system
- Computational cost of running extensive simulations
- In the most basic form, provided only point estimates for risk

Recent investigations at Sandia have resulted in advanced shell methods that include uncertainty on the risk estimates [28].

5.2.1.3 Bayesian Networks

A Bayesian network (BN) or Bayesian Belief network (BBN) is typically presented as a directed acyclic graph with nodes representing variables and arcs representing assertions of conditional independence. The BBN represents the conditional independence assumptions among a set of variables, thus specifying the joint probability distribution.

Fault trees and Bayesian networks have been shown to be identical in structure; there is a one-to-one correspondence between BN and fault trees. However, Bayesian networks extend the capabilities of fault trees to include many very desirable characteristics of advanced probabilistic risk analysis methods

Unfortunately, BN has the same difficulty as fault trees when dealing with complex, discrete, dynamic system modeling. Like fault trees, BN rely on a fixed topology between events. This poses significant problems for situations, e.g. digital systems, where the dependent relationship

between events changes as a function of time.

5.2.1.4 Hierarchical Bayesian Methods

Hierarchical models are models that explicitly account for the uncertainty in the physics model being employed, the parameters used in the models, the information available, etc. Hierarchical Bayesian (HB) methods provide the mathematical framework for formally analyzing the conditional structure of the interdependencies between the information. Bayesian networks are generally considered a subset of hierarchical Bayesian methods.

HB methods have been around for many years. However, with advances in computational capabilities and mathematical algorithms, there has been resurgence in HB methods for more complex problems. [29].

Hierarchical methods have been shown to be superior to fault trees for nuclear weapon reliability analysis, providing additional insight into where to focus testing [30]. HB methods have been used to model time dependent failure data, e.g. for modeling fatigue crack growth in nuclear power plants. Specifically, this involved estimating the density and size distribution of subclad flaws in French Pressurized Water Reactor vessels [31].

The ability to merge information from degradation problems and Bayesian networks or fault trees was demonstrated by Sandia as part of a NERI project [32 &33].

A fairly simple risk analysis of large communications facility, in support of Sprint/Nextel, has been completed by Sandia using HB methods; the problem had some simple dynamic operational issues similar to those analyzed using DFM [34 & 35].

Chapter 8 in NUREG/CR-6823 provides a simple introduction with emphasis on applications to nuclear power plants.

Finally, HB methods have been shown to be capable of forecasting failure events before they become critical. When implemented, this would permit operators to anticipate events before they become critical. The benefits of this type of predictive analysis are even more powerful when the off-line risk analysis is coupled with on-line monitoring [33].

On-line fault diagnosis and failure prognosis in complex dynamic systems is a growing interest in many fields with demanding reliability, cost, and safety requirements. Particle filters are a powerful class of Sequential Monte Carlo (SMC) algorithms for Bayesian State Estimation in dynamic, nonlinear systems with colored noise. Sandia has begun investigating Particle Filtering algorithms with a focus on online fault diagnosis and prognosis applications. The PF Diagnosis framework can be extended to function as a long-term forecasting tool to predict the remaining useful life (failure prognosis) of a faulted system or component.

Benefits of using hierarchical Bayesian methods include:

- Applicable during all phases of analysis

25

- Ability to support assessment of the value of additional, focused, testing
- Integration of data from all levels of system indenture
- Data from a variety of sources
- Objectively include expert opinion
- Point and full distribution information for probability estimates
- Deal with human error
- Continuous forms of degradation and failure
- Potential to incorporate real-time monitoring data
- Ability to characterize the uncertainty in the risk estimates

As with BN, the down-side of hierarchical Bayesian methods is the dependence on an established topology characterizing the time-dependent nature of some system failures. The efforts by Sandia in support of Sprint/Nextel provided some insight into the possibility of including discrete dynamics, but these were very simple problems compared to what has been handled by DFM.

5.2.1.5 Example Applications

Probably the best example of a risk analysis where all the major risk analysis capabilities have been brought together is the Sandia Safety Analysis Report (SAR) for the plutonium-dioxide fueled Multi-Mission Radioisotope Thermoelectric Generator (MMRTG) proposed to be used in the Mars Science Laboratory (MSL) mission. The National Aeronautic and Space Administration (NASA) is anticipating a launch in fall of 2009, and the SAR will play a critical role in the launch approval process. As in past safety evaluations of MMRTG missions, a wide range of potential accident conditions differing widely in probability and seventy must be considered, and the resulting risk to the public must be presented in the form of probability distribution functions of health effects in terms of latent cancer fatalities.

The basic descriptions of accident cases are provided by NASA in the MSL SAR Databook for the mission, and on the basis of these descriptions, Sandia applies a variety of sophisticated computational simulation tools to evaluate the potential release of plutonium dioxide, its transport to human populations, and the consequent health effects.

Given these basic descriptions, Sandia analyzes thousands of possible event sequences and builds up a statistical representation of the releases for each accident case.

These accident sequences are identical to those suggested by DFM. The risk analysis involves a variety of uncertainty methods to support the risk analysis. These methods are individually chosen to be the best application for a particular portion of the risk analysis.

- Shell methods based on traditional Monte Carlo analysis drive the accident sequence modeling.
- Some fairly sophisticated hierarchical Bayesian methods are used to incorporate test data.
- Complex computer simulations are sampled using HB methods to account for model uncertainty and avoid excessive computational overhead.

- Shell methods based on quasi-Monte Carlo and LHS methods are employed for the consequence analysis.
- Hierarchical Bayesian methods are employed to characterize the uncertainty in the final risk estimates.

Due to the limited time scope of the analysis, degradation is not explicitly considered. However, integration of degradation results, specifically relate to the launch vehicle reliability have been considered and can be handled quite directly.

5.2.1.6 Conclusions

The DFM and Markov methods currently being investigated are powerful tools critical to advanced risk analysis methods. However, these methods are rather limited as they currently exist. To fully address the requirements of advanced probabilistic risk analysis methods, these methods, must be integrated with other uncertainty analysis methods.

This integration requires a change in the nature of the mathematics of the underlying probability models within DFM. Current DFM methods must evolve to incorporate techniques underlying Bayesian networks. The generation of event sequences would not have to change substantially, but the assessment of event probabilities would have to change. Some difficulties are expected since BN consider the statistical dependencies between events, while DFM only considers the physical dependencies. The Sandia work with Sprint/Nextel has suggested that it is possible, but, again, these were rather simple problems.

This move toward Bayesian networks, and hierarchical Bayesian methods in general, would open the doors to incorporating information from other sources, other levels of system indenture, etc. Uncertainty characterization of risk would be straightforward; a natural fallout from the shift in perspective.

The next big issue is the incorporation of time dependent information such as that from a passive safety system or degradation/aging models. These are effectively the same type of problem with the same risk analysis implementation issues. Sandia has recognized this as a major issue and has begun some very preliminary studies in this area.

There will still remain situations requiring shell analysis methods. Sandia has the laid the groundwork for the most sophisticated shell methods available [27]. Considerable work still remains, but the general principles have been demonstrated.

5.3   Level 2 PRA

Level 2 PRA research efforts are part include the SOARCA project, which involves advancement of the state of the art in accident modeling and consequence assessment.

5.3.1 Current Level 2 Research

Most of the active research in Level 2 analysis is generally focused on severe accident (phenomenology) research. The results of the severe accident research are used to update code models or resolve generic safety issues. The insights, resolutions, and quantitative results are directly and indirectly incorporated into the event structure and quantification of the Level 2 models.

5.3.1.1 SOARCA

The NRC is in the process of developing Level 2 SPAR models for operating nuclear power plants. As part of the on-going state-of-the-art consequence assessment (SOARCA) program, Level 1 SPAR models are being used to analyze internal and external initiating events at a few reference plants. The intent of the program is to include design, operation and emergency preparedness improvements over the past 25 years into this assessment and to use the latest computer code models to accurately reflect existing plant capabilities, performance and emergency response activities. In addition, in recent months the NRC has required licensees to improve their mitigation measures to address extreme damage states. In response to these requirements, licensees have submitted written plans describing the mitigation measures being developed, and are in the process of developing procedures and purchasing the necessary equipment, to have these mitigation measures in place in the very near future.

The SOARCA mitigation measures analyses include an assessment of the licensees' emergency operating procedures (EOPs), severe accident mitigating guidelines (SAMGs), and the newly required extreme damage state improvements currently being implemented. Available mitigation measures, including the primary SSCs (which includes portable equipment), as well as the necessary support systems and resources, were verified to be available based on the initiating event, subsequent failures, and resulting initial conditions. In addition, any pre-staged supporting equipment required for successful implementation such as transport capability, fuel, hoses, connectors, tubing, tools, etc. were verified to be available. A time-line of operator actions and equipment lineup or setup times were developed for the implementation of the available mitigation measures using plant procedures, emergency response requirements, and conservative time estimates.

Several shortcomings were identified. First, few if any mitigation measures were not included into the Level 1 SPAR models. Consequently, the mitigation measures were addressed externally to the specific sequence selections in perhaps a non-integrated manner. For sequences that were dominated by human errors, the specific time duration of the human error condition was difficult, if not impossible, to identify how and whether support groups such as the plants Technical Support Center (TSC) or Emergency Operating Facility (EOF) could assist in identifying human errors, given relatively large amounts of time to successfully implement corrective actions.

Second, Level 1 SPAR cutsets with frequencies just below the cutoff threshold for the SOARCA program Level 1 SPAR models included seemingly incredible sequences that had vague or poorly defined initiating and boundary conditions. As the internal event initiator frequency

decreases, the remaining cut sets include less carefully analyzed conditions. For example, many cutsets were identified with frequencies within a decade of the analysis threshold that included ill-defined characteristics,

Finally, the highest frequency cutsets were dominated by external initiators with a poor characterization of the plant status and damage. Consequently, if mitigation actions were considered, then there was not an integrated assessment of their successful implementation. For example, flooding would reduce access to certain regions, whereas, seismic events may include damage to systems or piping that may be significant to mitigation efforts.

5.3.1.2 Regulatory Definition of Tolerable Consequences

Several international organizations (mostly regulatory bodies) are performing work to establish or refine definitions of maximum tolerable 'consequences' within the purview of Level 2 PRA. Most of these metrics focus on the concepts of a 'large early release (LERF)' and/or 'large release (LRF).' Two examples include:

- In 2006, the HSE/NII in the U.K. issued a revised set of "numerical targets and legal limits' for societal risk. (They had previously only enforced PRA results to conform to numerical targets for individual risk.) The new societal target could impact the way in which PRAs for British AGRs are performed, which currently do not explicitly address severe accident progression as we know it traditional "Level 2" PRA. [

- The Swiss regulator (HSK) has performed some work to establish two reportable criteria for Level 2 PRA results, LERF and LRF. The former is based on the minimum I-131 release to result in an acute health effects; the latter is based on the maximum tolerable Cs-137 release for long-term environmental consequences (land contamination).

- The NRC research plan [18] includes an effort to expand the current SPAR models to provide estimates of LERF. It is unknown whether the research will use the generic guidelines for "Category I" LERF assessment in the ASME Standard or new criterion, such as the two previous examples. The generic guidelines are based on a simple and conservative approach developed by Brookhaven some time ago (NUREG/CR-6596 [36]).

In addition to phenomological research, two examples of ongoing Level 2 PRA methods research were identified.

- MELCOR/LHS uncertainty analysis -- this technique has been used at SNL to remove the dominance of 'expert judgment' in Level 2 uncertainty analysis. In particular, MELCOR is run many times with sampling of uncertain parameters using Latin Hypercube Sampling (LHS) to characterize the impact of uncertainties on next and progression in an integrated computational framework.

- "Dynamic PRA" – Ohio State is performing research to seamlessly integrate Level 2 and 3 probabilistic risk assessments with fast running, simplified MELCOR and MAACS models. This type of research is expected to improve the coupling between the Level 2 and Level 3

analyses. We are unaware of similar research to improve the interface of the Level 2 to Level 1. Typically, these interfaces rely on grouping or binning with a loss of information on specific sequence characteristics.

5.3.2 Level 2 Research Needs

The following are suggested research efforts related to Level 2 PRA methods:

1. Improved methods for integrating the Level 1, 2, and 3 PRA analyses (e.g., expansion of the efforts by Ohio State for dynamic PRA and SNL for uncertainty characterization). The two cited efforts on ongoing Level 2 PRA methods research examine improving the coupling and uncertainty propagation between Level 2 and Level 3. One of the most difficult aspects of PRA methodology is the coupling of Level 1 to Level 2. Typically results are grouped into a small number of plant damage states, which have similar characteristics. This process is typically done by hand and requires considerable expert judgment. It would be desirable to automate the coupling between all three analyses, such that uncertainty effects could be propagated consistently through the three analyses and unanticipated interactions to cutest characteristics that feed into plant damage states are addressed accurately.

2. Improved techniques for the characterization of damage developed in external events into the Level 2 analysis. In the SOARCA program, examined sequences for the plants analyzed have been dominated by external event initiators. The rigor of the external events analysis was perceived to be much lower than the internal events. Limited damage state information was passed to the Level 2 analysis, which was restricted to the success criteria. Consequently, it was impossible to discern the status of other equipment, which might be used for mitigation.

3. Integration of mitigation and operator actions extending into the time-domains covered by Level 2 analysis from the Level 1. In the SOARCA program, some sequences were dominated by human error from the Level 1 analysis. The expected time domain of those errors as well as possible future errors in the Level 2 analysis or correction of previous errors due to the introduction of new advising groups, such as the TSC or EOF, need to be handled consistently and shared between the analyses. Similar to identification of other damages in external events, a consistent methodology for handling human reliability, including activities and potential mitigations is needed from the Level 1 and within the Level 2 analysis.

4. Eventually, it may be desirable to develop more sophisticated codes for modeling severe accident behavior. Such codes could utilize computational fluid dynamics. However, it is believed that the cost/benefit ratio for such an effort would likely not be favorable. That is, the fidelity of the results may not be much better due to uncertainties in severe accident behavior but the cost and time required to use such a code would be significantly higher than for running codes like MELCOR.

The following are suggested research efforts related to phenomenological research:

1. Development of technical guidance resources for severe events that lead to early containment failure and their plant-specific quantification. Events such as direct containment heating, steam explosions, hydrogen burns, and liner melt-through (Mark I containments only) are quantified using analysts judgment of existing research that could lead to inconsistent and varying results. Due to their extreme importance on a large early release, a consistent methodology and application guidance is needed. It is anticipated that a guidance handbook could be developed with citations to examples of acceptable research that could be applied in a consistent way.

2. Relative to the extreme phenomena cited above, is the past research applicable to new reactor designs. In particular, the direct containment heating (DCH) work in the 1990s examined current generation containment designs (esp. their variations in the reactor cavity). Research is required determine whether the findings from those studies bound the new designs. In anticipation of NRC reviews of new licensing applications, the reviewers of new designs need guidance on their review of the vendor's PRA submittals.

3. Furthermore, it is uncertain whether the finding from those studies encompass new fuel assembly designs (e.g., 8x8 BWR fuel to 10x10 assemblies) and new understandings of core degradation behavior (e.g., longer in-vessel phase with higher in-vessel debris temperatures but increased oxidation).

4. Finally and also relative to the DCH, NRC's principal severe accident analysis code, MELCOR, does not address this phenomena. While the early containment failure issue resolution research from the 1990s examines the potential for a large early release, the mechanistic response of the phenomena without early vessel failure (e.g., typically the large frequency branch during such events) is not well characterized. Do the energetic events greatly accelerate or de-accelerate the timing to late containment failure? How does it affect the source term? To provide addition guidance for future PRAs and their reviews, an integrated phenomenological representation of the events should be incorporated into MELCOR. The code could be provided for PRA auditing or to develop a guidance handbook.

5. The characterization of equipment following and during sequences initiated by external events also requires a guidance handbook for level 2 analysis. Can mitigation actions be performed? How did the event effect the environment? For example, SOARCA sequences had 0.3 and 1.0 G events. Were the auxiliary firewater tanks available? Have walls or buildings fallen down? What is the status of containment spray piping and connections? Short of detailed research, a guidance document that estimates damage in external events to equipment, structures, etc., such that conditions not specifically identified in the Level 1 plant damage state can be consistently evaluated in the Level 2 analysis.

6. The ANS Level 2 Standard working group has recently requested ASME Section 2I to develop guidelines for 'best practice' methods of defining criteria for containment failure (fragility). Among the possible outcomes of this work will be a recommendation that containment "leakage" be modeled as a continuous function of containment internal pressure, rather than a threshold for "failure" as applied in most (if not all) Level 2 PRA analyses to date. The implications of this approach are not clear, and no organized work has been performed to evaluate its impact on containment response and/or source terms. If a continuous leakage function is the proper (or preferred) way to characterize structural response, a manner in which this behavior can be represented in PRA needs to be developed. Current practice typically treats containment "failure" in a discrete manner (normal leakage an "enhanced leakage' catastrophic failure.) Research is needed to develop more realistic containment response models that include the effects of more continuous stress strain models, the effects of and elevated temperature, and the effects of degradation due to aging.

7. Relatively recent information from Phebus suggests the time-honored chemical speciation used in most Level 2 PRA source term analyses may have flaws. MAAP, for example, continues to assume all iodine is released in the form if CsI and remaining cesium is released as CsOH. Changes in these (and other) nuclide groups have been proposed and used in recent MELCOR calculations. However, the impact of these changes on "typical" fission product source terms has not been quantified, nor has the technical basis for changes to the traditional radionuclide grouping scheme been firmly established of documented. A state-of-knowledge paper/report should be prepared to propose changes to the grouping scheme, if they're warranted.

8. There's a general problem that many of the (international) metrics for LERF and/or LRF are expressed in terms of ACTIVITY released, not fission product mass. This is problematic for Level 2 PRA and the deterministic codes that support them because neither MAAP nor MELCOR (don't know about ASTEC) provide any tool to convert released mass to activity. The problem is further complicated by the fact that typical LERF/LRF thresholds are defined as a fixed quantity of activity ($2x10^{15}$ Bq of I-131, for example) without any indication of how this level of activity is to be calculated. The fact that iodine mass released to the environment is a continuously increasing function of time, but iodine specific activity is a decreasing function of time makes it difficult to know how the concept of "released activity" should be calculated. Some investigation into this and alternative LERF metrics would be worthwhile.

5.4   Level 3 PRA

For the purposes of consequence modeling, there is little that is inherently different for an advanced reactor than for the existing generation of nuclear power plants (NPPs). However, the state of the art is advancing and expectations for performing consequence analyses have evolved since NUREG-1150. The improvements affect both the gathering of data needed to drive consequence models and the models themselves. Just as the next generation of reactors is expected to be better than the current fleet, the expectations for consequence analysis in support of Level 3 PRAs should be higher than for those done in the past.

5.4.1 Meteorological Data

Consequence analyses performed for NUREG-1150 and subsequently for severe accident mitigation alternative (SAMA) analyses and other Level-3 PRA analyses have been based on single weather station data averaged over one-hour intervals. While the angular resolution of wind direction measurements at nuclear power stations is required to be no more than ±5°, the consequence analyses have used a lower-fidelity, 16-compass-direction grid (22.5° sectors).

Recent consequence calculations for the SOARCA program are using hourly data at a resolution of 64 compass directions. Current capabilities already allow for quarter- or half-hourly intervals weather data instead of the traditional hourly intervals. Consequence analyses based on higher-fidelity weather data are now becoming standard practice. Requirements for such data should be anticipated for advanced reactor PRAs. These higher-fidelity requirements would not put any additional burden the plant owners in terms of instrumentation, only on the post-processing of the data.

Future development of atmospheric transport and dispersion (ATD) modeling capabilities could create a need for multi-station or three- or four-dimensional gridded weather data. Three-dimensional gridded data are currently available from NOAA and the EPA. Possible ATD improvements and supporting data requirements are discussed below.

5.4.2 Site Data

Site data (e.g., population distribution over a grid) may be required at a higher angular resolution than in the past, as noted in the previous subsection. The current capability is to define population distributions over 16 compass sectors and to interpolate that data onto a finer grid, up to 64 compass directions. Code modifications to implement the capability for higher angular resolution site data are being discussed. Pursuing a higher-resolution site data capability will support the needs for advanced reactor PRAs.

5.4.3 Source-Term Data

Isotopic core inventories in advanced reactors will be different than in existing NPPs. One or more ORIGEN calculations will be needed to determine core inventories for each type of advanced reactor. For example, recent analyses for SOARCA used a set of 50 ORIGEN calculations to provide decay heat data for each of the volumes in a MELCOR calculation. The same ORIGEN data were digested and used in the MELMACCS interface to drive MACCS2 consequence analyses. Similar data needs should be anticipated for advanced reactors.

The current strategy for analyzing source terms for consequence analysis begins with one or more MELCOR calculations. Data are extracted from the MELCOR plot file using a utility known as MELMACCS, which generates input records for MACCS2 containing the pertinent source-term information. Some upgrades of the MELMACCS interface will undoubtedly be required to support advanced reactors. For example, any new chemical groups that are implemented in MELCOR will need to be addressed in the MELMACCS interface. Also, new

core inventory data, as described in the previous paragraph, will need to be added to the MELMACCS interface.

5.4.4 Dose Conversion Factors

Recent consequence analyses, including analyses for SOARCA, are based on recently developed dose conversion factors (DCFs) taken from FGR-13 for internal doses and FGR-12 for external doses. This DCF database includes 825 isotopes, all dose pathways, and an extensive set of organs. It supports analysis of acute and long-term health consequences and analysis of dose thresholds.

One limitation of the existing DCF database is that it is only for 1 μm activity median aerodynamic diameter (AMAD) aerosols. If this limitation on aerosol size is appropriate for advanced reactors, the current database should be sufficient for the anticipated consequence analyses. If the median aerosol sizes are expected to be significantly larger or smaller than 1 μm, then additional work is need to develop a more extensive DCF database.

5.4.5 Atmospheric Transport and Dispersion Model

The current state of the art for NRC consequence analysis is the Gaussian plume model for atmospheric transport and dispersion (ATD). This model sacrifices fidelity for computational speed, which is important given the number of analyses needed for a level-3 PRA. Data for a single weather station are sufficient to drive such a model. Recent analyses, e.g., SOARCA, have used 64-compass-sector weather data to maximize the capability of the Gaussian plume model to account for wind shifts. Because of limitations in the meteorological data that is readily available, the SOARCA analyses are based on wind data averaged over 60-minute time periods even though MACCS2 is now capable of accepting data at 15- and 30-minute time intervals.

A comparative study showed that the simple Gaussian plume approximation is sufficient to get factor-of-two accuracy when reporting consequences as annual averages and when complex terrain and complex wind fields are relatively unimportant. This study shows that the Gaussian plume approximation is sufficient for the majority of the existing NPPs if factor-of-two accuracy is acceptable.

The Gaussian plume model does not account for the complex wind phenomena that can be important in some situations. For example, weather patterns near oceans and large water bodies can be influenced by land and sea breezes, which give rise to complex, three-dimensional wind fields. In most cases, these complex wind fields are expected to diminish consequences as compared with the predictions based on a straight-line Gaussian plume model.

Other situations that create complex wind fields are NPPs located in canyons and below palisades. Such topographical features can result in local wind conditions that deviate from the synoptic conditions. Using a Gaussian plume model to predict consequences in such situations could result in over- or under-estimates, depending on the locations of population centers compared with the prevailing wind directions.

Current computational capabilities now allow higher-fidelity ATD modeling to be performed on a routine basis for consequence analysis. An example is the consequence analysis performed for the safety analysis reports (SARs) supporting space missions with nuclear materials on board. Sandia is currently supporting the Mars Science Laboratory (MSL) Mission and using Gaussian puff models with two- and three-dimensional wind-field data. Performing a total of 2000 weather trials for each of about 20 accident scenarios (a total of about 40,000 realizations) requires a few days of CPU time on a modern computer. Using multiple processors can compress the time needed to perform such a set of calculations to a day or less. Such high-fidelity consequence analyses will likely become routine in the near future for a variety of applications, including level-3 analyses for NPPs. Such capabilities would reduce the level of conservatism inherent in the current models and would allow complex issues to be resolved with a greater level of confidence than current capabilities can support.

Development of a Gaussian puff model for consequence analyses of NPPs would improve fidelity even with single weather station data because the puff trajectories could bend to follow wind shifts. However, the fidelity of such a model would improve significantly if multi-station data were used to construct two- or three-dimensional wind fields. Thus the meteorological data needs would likely expand with a Gaussian puff model. Two possibilities for obtaining higher fidelity wind-field data are discussed below.

Two-dimensional wind field data could be constructed by obtaining surface data from surrounding weather stations, such as those supported by the National Weather Service. These data are readily available, but usually require some level of massaging to eliminate erroneous data (e.g., from stuck weather vanes) and from data recovery problems (e.g., from unavailability due to severe weather conditions or routine maintenance). The multi-station data could be interpolated by using an inverse distance squared weighting (a standard approach). This option should be expected to be somewhat labor-intensive, depending on the number of weather stations to be included in the analysis.

A second option is to use three- or four-dimensional gridded data from NOAA or the EPA to drive a Gaussian puff model. The gridded data cover the entire USA in two or three physical dimensions and time as an additional dimension. The horizontal resolution of the data is 5 km at a minimum and in some areas it is 2.5 km. There are future plans to increase the resolution to a uniform 2.5 km, but there is no timetable for this at present. The data are created using observations from weather stations across the country along with analysis tools to assure mass consistency and to project the evolution of weather patterns. These data would not require fixing or patching and thus would not be labor intensive to use. Such data, in concert with a Gaussian puff model, would offer the highest level of fidelity short of a fully three-dimensional, particle-tracking approach like the one used in the National Atmospheric Release Advisory Center (NARAC) LODI code. Using a code like LODI for consequence analysis is considered too computationally intensive for the foreseeable future.

5.4.6 Emergency-Phase Model

The current emergency-phase modeling capabilities in the MACCS2 code, with modest refinements, are considered adequate for the foreseeable future. These capabilities include the

ability to employ a network evacuation model in a very general manner. Recent advances allow the evacuation network to overlay a road map to facilitate selection of evacuation directions. Also, evacuation speeds can be varied to account for traffic bottlenecks and high-speed roadways.

One aspect of the evacuation modeling capability should be improved to better treat emergency response. This improvement would allow cohorts to be defined more generally. For example, the SOARCA project has assumed evacuation out to a 20-mile radius. However, the population within the more standard 10-mile radius would evacuate differently than the population between 10 and 20 miles. Current capabilities do not allow cohorts to be defined differently in sub-regions of the sheltering and evacuation zone; they must be defined uniformly throughout entire zone. This development would improve the generality with which emergency response can be modeled in future consequence analyses.

5.4.7 Long-Term-Phase Model

The current capabilities for analyzing long-term health consequences are also considered adequate for the foreseeable future, including advanced reactor applications. These capabilities allow general dose-response models to be incorporated into a consequence analysis, including annual and lifetime threshold models. However, an area of needed improvement is the economic consequence capability, which is described below. The current economic consequence model is coupled with the health consequence model in MACCS2, and thus it can have an indirect impact on health consequence predictions.

The economic model in MACCS2 is commonly used in SAMA analyses and other cost/benefit analyses associated with licensing activities for the current reactor fleet. It is anticipated that cost/benefit analyses will also be needed in the regulatory process for advanced reactors.

The current economic model in MACCS2 is more accurately a cost model and treats the following cost categories:

- Per diem costs for evacuated and relocated individuals
- Crop disposal costs from accidents during the growing season
- Temporary loss of use of farm and residential land
- Cleanup costs, up to the value of the property
- The value of condemned property
- One-time moving expenses incurred during relocation

The current model lacks flexibility in some areas where decisions may be less based on economics and more on politics. For example, cleanup costs are currently limited to be no more than the value of the property being cleaned up. Political decisions could dictate that cleanup be performed regardless of cost or at least at costs well above the value of the property, like at some of the superfund sites.

Several other costs, not in the above list, are included in SAMA and other cost/benefit analyses performed for the NRC, as follows:

36

- Onsite cleanup and decontamination
- Cost of replacement power
- Costs resulting from offsite and onsite exposure to radioactive material (currently $2000/person rem).

In reality, some compensating economic factors would reduce the economic costs that are assessed in the current model, e.g., reduction of federal farm subsidies when farm land is taken out of production because it cannot be farmed. These compensating factors are not included in the current model.

An evaluation of the current economic model in MACCS2 should be undertaken. The fidelity of the current economic model should be enhanced to ensure completeness, to eliminate conservatisms by accounting for compensating effects, and to add flexibility to accommodate politically driven decisions.

5.5   Digital I&C Modeling

This section provides an independent assessment of the techniques available for modeling of digital systems in a PRA. Many of these techniques have already been reviewed in some manner previously [37, 38, 39]. Chu, et al [37] performed an assessment of "traditional" techniques for the modeling digital systems. Aldemir, et al [38] assess multiple techniques using eleven criteria[1] that they state must be met for a methodology to be implemented. None of the techniques met all the criteria. Aldemir, et al [39] present a proof-of-concept for the use of Markov models and Dynamic Flowgraph Methodology (DFM) for modeling of digital systems. The use of Markov models and DFM was due to the results of the previous study documented in NUREG/CR-6901 [38].

Before discussing the techniques presented, it is first necessary to define some terms that will be used in the subsequent discussion. For the purposes of this assessment, Type I interactions are defined to be interactions between the digital system and the physical processes being controlled. Type II interactions are defined as interactions among the components of the digital system itself. These definitions are consistent with those given in NUREG/CR-6901. "Traditional" methods (with regard to modeling digital I&C systems) are methods which *do not* explicitly account for the time element in system evolution. "Dynamic" methods are defined to be those methods which *do* explicitly model the time element in system evolution. It is not clear that these definitions are equivalent to the definitions used by Chu, et al [37]. However, these are the definitions used by Aldemir, et al [38, 39].

Digital systems require three distinct types of analyses that must be addressed. The first is the interaction among the components of a digital system; the second involves interactions between

---

[1] Some of the criteria used in NUREG/CR-6901 seem to be quite arbitrary. For example, criterion 6 states that "the data used in the quantification process must be credible to a significant portion of the technical community." We believe that this statement is not quantifiable and the terminology leaves much to be desired. Other criteria that are used also exhibit obscurity. In particular, if criteria 3, 5, and 6 are omitted, then much ambiguity in the method selection process will be omitted, also.

the digital system and other systems. The third – and possibly most complex – analysis that must be considered for digital systems is the assessment of software reliability. Software errors can be divided into two classes. Class A software errors are defined as those errors which are made apparent whenever a path that contains the error is used. These errors are – in principle – easy to find. However, the number of paths in any software can be prohibitive, thus making it difficult – in practice – to determine all of the Class A errors. Even if all of the Class A errors are found, the process of "removing" or "fixing" the error can create other errors and thus increases the amount of testing that must be performed. The upside of Class A errors is that if all paths in the software are tested and no errors are discovered, then it can be assumed that, by definition, no Class A errors exist. Class B errors, on the other hand, are more difficult to diagnose. Class B errors are those software errors which can exist within a path, but may be dependent upon the input or the environment in which the digital system exists. If a Class B error exists within a given path in the software, one can test that path an infinite number of times without discovering the error. This makes it difficult to even define a reliability assessment technique that can be used.

5.5.1 Traditional Techniques

This section reviews the state-of-the-art in traditional PRA techniques and their applicability to assessment of digital systems. One drawback of traditional methods is the fact that, *by definition*, they do not explicitly account for the dynamic nature of digital systems. The traditional techniques are reviewed below (in no particular order). The review includes a discussion of the strengths and weaknesses of each technique.

The most commonly used traditional technique in use today is the "Event Tree/Fault Tree (ET/FT) method". This method has some advantages. First of all, it is currently used for all NPP PRAs in the United States. It has a well-established history with many software tools available to users. The ET/FT method is also easily understood if the correct combination of event trees and fault trees "hanging" from the event trees is used. All these strengths essentially enumerate the separate advantages of being the first technique to be used in the nuclear community. The reason these qualities are strengths is because they will not require the extensive, basic training that will be needed to implement the other traditional techniques discussed in this report. Although the ET/FT method has its advantages, some weaknesses have also been identified. Some methods of using the ET/FT method essentially leave out the fault trees. This leads to extremely large numbers of end states. For example, the PRA associated with the feedwater and condensate system of Watts Bar Nuclear I indicates over 10 million end states. This prohibitive number of end states makes it nearly impossible to visually capture the system properties. The inability to view the system as a whole and obtain a visual perspective on the system becomes time consuming when trying to understand and/or "debug" a faulty system model.

A second traditional technique is the "Go-Flow Methodology". Two explicit strengths have been identified for this technique. This methodology is similar to fault trees, but focuses on success instead of failure of the system being analyzed. The math involved is fairly routine probability and statistics. Both of these aspects make the Go-Flow methodology attractive because it can draw upon the experience that has been built in the ET/FT method. However, there have also

been some weaknesses identified with the Go-Flow technique. The first is that the method does not provide structural information regarding the system being analyzed. This presents a problem when one wants to understand the physical concepts of the system. A second weakness is that importance measures (such as Fussell-Vessely, Risk Achievement Worth, and the Birnbaum measure) are not provided by the technique. A lack of importance measures can be an issue because there are no guides to determine the best way to improve the system without the importance measures.

A third traditional technique involves the use of Binary Decision Diagrams (BDDs). BDDs are data structures that represent Boolean functions. One strength of BDDs is that, in principle, they can be used for any system that event trees and fault trees can handle. However, they have one very strong weakness. Solving a BDD depends strongly upon the ordering of the variables and the ordering of the variables is an NP-complete problem. NP-completeness refers to a class of problems for which no efficient algorithm has been shown for solving the problem. In practical terms, this means that NP-complete problems (e.g., ordering of BDDs) are unsolvable for systems with as many variables as those in a nuclear power plant.

The fourth traditional statistical technique for PRAs of digital systems involves the use of Markov chains. A Markov chain is, by definition, a stochastic process with the Markov property. The Markov property refers to the idea that the probability of transitioning from one state at time t_0 to another state at time t_1 depends solely upon the state at time t_0. Markov processes are sometimes referred to as being "memory less" due to this property. Similar to the previously described traditional methods, some strengths of Markov models are that the math involved is fairly simple and that they can solve any system that the ET/FT method can solve. Weaknesses related to Markov models are prohibitive, though. Like the ET/FT method, the number of states for Markov models grows quickly with system complexity. A state vector for the example in the ET/FT paragraph of this section would have the same number of components as the number of end states in the ET – over 10 million. However, the transition matrix for this same system would have 10 million squared – over 10^{14} – entries. When trying to predict future states of a system, errors in the transition matrix will grow exponentially. These weaknesses are just the ones that are associated with Markov models *while assuming the system under study can be modeled as a Markov process in principle*. It is not clear whether digital systems can be modeled as Markov processes. Digital systems may have memory based on the logic that is being implemented. Strictly speaking, this rules out Markov modeling. [2] Techniques are available which allow this difficulty to be circumvented at a computational expense which grows exponentially with the amount of memory of the system. This increases the power required beyond even that which is mentioned above. Another weakness of Markov models is that it is difficult to implement uncertainty analysis with this type of model. The only quantifiable uncertainty analysis seems to be sensitivity analysis which, once again, would drastically increase computational requirements. The last weakness of traditional Markov models to be discussed is the inability of these models to accurately address repair rates of systems [3].

---

[2] If the only difference in a given process and a Markov process is that the given process has memory, then the process is technically an Ito process. An Ito process can be transformed into a Markov process by defining each trajectory which leads to a given current state as a separate process. For example, if a system has two states with a memory of two time steps, one can transform this into a Markov process with four states. If this same system has a memory of three time steps, the Markov model would have eight states.

Maintenance is an important part of any nuclear power plant and the ability to model repair rates is important.

5.5.2 Dynamic Techniques

This section reviews the most prominent dynamic PRA techniques and their applicability to assessment of digital systems. *By definition,* dynamic techniques are those which explicitly model the temporal aspect of systems. Unlike traditional techniques, these dynamic techniques all have some means – in principle, at least – of addressing the evolution of the system over time. This, in itself, is a major strength of all dynamic methods and should be kept in mind although it is not discussed in the paragraph devoted to each of the techniques below.

The first prominent technique to be reviewed is actually a class of methods grouped under the title 'Bayesian Analysis'. The authors feel that it is appropriate to discuss what seem to be some misunderstandings related to Bayesian techniques. Chu, et al [37] and Aldemir, et al [38] imply that Bayesian techniques are not able to model dynamic interactions. In a typical Bayesian model, the time aspect of a system can be modeled as easily as any covariate. Much of the misunderstanding may stem from the fact that little has been written *in the nuclear community* about Bayesian techniques. Zhang and Golay [40], Yue and Chu [41], and others have suggested the use of Bayesian techniques for specific applications. However, it should be noted that Bayesian techniques can be used in any model in which traditional statistics can be used since the set of traditional statistics is a subset of the set of Bayesian statistics. Bayesian techniques are currently in use in the financial industry and in the medical industry. Most of the work in the financial industry is proprietary in nature, but some references from the medical industry have been provided [42, 43, 44]. Bayesian analysis has also been used in the analysis of health monitoring of critical systems [45]. Currently, Sandia National Laboratories is in the process of drafting a report that outlines a technique for using Bayesian analysis to dynamically model the reliability of passive systems for nuclear power plants.

Bayesian methods have many strengths; the major ones are identified in this paragraph. First of all, the technique is very general which makes it possible to apply it to almost any system of practical interest, including digital systems. All three of the issues related to digital systems that are discussed in the introduction to this section can be modeled using Bayesian methods. This is a great improvement over many of the techniques that are currently being discussed. The ability to assess software reliability alone makes this technique attractive. Another strength of Bayesian methods involves combining different types of information. Many of the systems that need to be analyzed in the digital arena have little or no historical data. Bayesian analysis allows the analyst to combine expert judgment with historical data and advanced regression analysis. Weights can be applied to the different data sources in order to place more emphasis on those sources which are more closely related to the system being analyzed. Hierarchical Bayesian analysis allows multiple layers of uncertainty to be incorporated so that a consistent, quantifiable measure of the uncertainty in the analysis is inherent in the results. The models can also be easily updated when new data become available *without recalculating the entire output of the model.* They can even be updated in real time if combined with appropriate sensor systems. Another advantage of using Bayesian methods is that multiple software tools are available which decrease the time required to develop the code for the Bayesian models. These software tools

use GUIs which allow the user to develop the model by using a drawing tool. The code is generated automatically from the picture which is developed.

Two weaknesses have also been identified. The first weakness involves the complexity of the math that is used. Some traditional PRA practitioners have expressed displeasure with the idea of placing distributions on some parameters that have historically been treated as having point values. Much of this comes from a misunderstanding of the math involved. Admittedly, the math is a bit more involved, but it is ultimately as valid as any other statistical technique. However, convincing some of the current PRA leaders that the benefits outweigh the complexities of the math may be difficult. The second weakness of Bayesian methods is tied very closely to one of their strengths. The ability to incorporate expert judgment opens the technique to the possibility of someone manipulating the results by using grossly inappropriate inputs to the model. However, it should be noted that this same type of negligence can be used in classical techniques by simply falsifying the data or by selectively removing data that should be used in an analysis.

The second dynamic technique to be reviewed is that of 'Dynamic Markov Models'. This technique is simply an extension of the traditional technique of 'Markov Models' that is discussed above. The same strengths exist, including easily understood mathematics and the ability – in principle – to solve any system that the ET/FT method can solve. However, the same weaknesses also exist. The number of states in the state vector becomes very large for any realistic system. This leads to a prohibitive need for computational power when trying to address the many digital systems that will be used in any new nuclear power plant. Digital systems rely on circuits which may have memory. By definition, these systems do not have the Markov property. Thus, any model of the system will have to take this into account. The number of states will grow exponentially with the amount of memory used for operation. Thus, if the digital memory is never erased, then the number of states for the Markov model of the system will grow exponentially with the number of times the logic of the system is invoked. Another weakness is that, similar to traditional Markov methods, errors due to state transition probabilities grow exponentially with time. It is also difficult to implement any consistent, quantitative approach to uncertainty assessment of the PRA results using Markov models. Another major weakness of dynamic Markov models is their inability to accurately model repair rates [3]. Since maintenance is an inherent part of any nuclear power plant, this should definitely be considered when choosing an appropriate method for performing digital PRAs.

The third dynamic technique reviewed is termed 'Dynamic Flowgraph Methodology' [10]. Not much has been found that relates this technique to digital systems in nuclear power plants. However, one strength of this technique is that it integrates all aspects of the digital system. The weaknesses of the technique are that the results are qualitative rather than quantitative and it has not been proven that the results can be integrated into an existing PRA.

The fourth dynamic technique reviewed for this report is the technique of 'Petri Nets'. A major advantage of Petri nets is that they generate fault trees. Therefore, they seem to be compatible with current PRA techniques (i.e., ET/FT). One weakness is that certain aspects of Petri nets assume exponential distributions, which are probably not appropriate for all aspects of digital systems.

The last dynamic technique reviewed involves the use of 'Dynamic Event Trees'. Dynamic event trees are essentially the same as traditional event trees, except they have a temporal aspect added to them. The most obvious advantage of dynamic event trees is that they can be easily integrated into a traditional PRA. The weaknesses, however, are more numerous. They are essentially the same as the weaknesses of dynamic Markov models. Ultimately, the computational power required is expected to be much more than can be provided for any nuclear PRA. The number of states associated with dynamic event trees and the computational requirements for any uncertainty analysis are prohibitive.

5.5.3 Future Research

The following is a discussion of some areas of research that should be further considered. Some of the suggestions are accompanied by a short explanation of why this research is important.

1. Bayesian Approach to Software Reliability Assessment – The issue of software reliability is possibly (probably?) the most complex issue facing digital system reliability. Part of this is due to the fact that a software failure is not easily defined. Software itself always executes according to how it was designed and *never degrades*. Failure of software can only be defined in terms of failure of the system in which the software is imbedded. However, a Bayesian approach to assessing software reliability would allow the use of expert judgment as a prior. This could then be updated as software testing is performed. As the number of tests increases without failure, an assessment of the reliability of the software will become more certain. The current drawback is that if an error is found and fixed, then the assessment has to be started over since the process of fixing the error can introduce new errors. If this process of starting over every time can be addressed, then the Bayesian approach would cover all bases of "addressing" software reliability.

2. Addressing Reliability as a Function of Software Complexity and Software Engineering Process – This research idea stems from the statements presented in #1 above. The term "software reliability" is a bit of a misnomer. Since software will always perform the action it was designed to perform under given conditions and never degrades, what actually needs to be estimated for any given piece of software are:

   a. The number of mistakes or omissions the software engineer makes
   - and -
   b. The rate at which the software inputs will trigger one of these mistakes or omissions.

   Based on these two principles, the tasks that should be performed are:

   a. Assessing the complexity of the software as a function of the number and arrangement of nodes and transitions. The most obvious choice for this assessment would rely on information theoretic measures such as Shannon entropy or KS entropy.

42

b. Assessing the reliability of humans to perform a task as a function of the complexity of the task and the process involved in performing the task.

This research could provide a means of predicting the reliability of a software code. It would also provide a means of defining the process for which software is created by assessing *a priori* the expected reliability of the software created and allowing a new process to be suggested. This "process" discussed here includes:

- Time frame for producing the software.
- Number of software engineers needed.
- Number of modules needed for the software.

5.6   Quantification Techniques

As mentioned previously, the use of PRA quantification approaches such as the use of the rare event approximation or the minimal cutset upper bound (MCUB) approximation with truncation can potentially result in inaccurate risk results including misleading importance measures. Furthermore, exacting quantification schemes do not explicitly include evaluation of success branches when evaluating event tree sequences. In some PRA codes, success branches are accounted for using a DELETERM approach where cutsets for the system success are used to remove cutsets in the system failure results.

To address these concerns, EPRI, as well as others, have been exploring the use of Binary Decision Diagrams (BDDs) to generate exact solutions of fault trees. An initiative called Open PSA has been established as a forum to bring together different groups who are addressing such issues and who are developing the next generation of PSA tools. EPRI is participating in this initiative. Since the use of BDDs is currently only possible with small fault trees, different approaches are being examined to provide mechanisms for solution of the large fault trees that are generated in most PRAs.

EPRI is exploring the use of a combination of quantification approaches to solve fault tress in an optimal manner. Their approach involves the use of a trademarked calculational scheme (believed to use truth tables) that provides an exact solution of a fault tree but does not provide cutsets. The exact solution value is used to establish a truncation limit for a MCUB evaluation that generates cutsets. A BDD solution of the resulting cutsets is then performed which provides an exact solution of those cutsets. The results are stable importance measures and risk results.

Others participating in the Open PSA initiative have indicated some success using developed algorithms to provide solutions of large BDDs. The Open PSA website (http://open-psa.org/resources/ provides resources that provide a good discussion on BDDs and possible solution algorithms.

The NRC should consider initiating its own program in advanced fault tree solution techniques including the use of BDDs for solution of SPAR models. The NRC may want to explore the possibility of a collaborative effort with EPRI or others working in this area. Finally, continued NRC involvement in the Open PSA initiative is important for keeping abreast of research in

advanced PRA tools which includes not only BDDs but also new types of PRA user interfaces that provides better quality control on generated models and generation of PRA documentation. For example, EPRI also is generating Declarative Modeling capabilities that allow attributes such settings under various conditions (TRUE or FALSE) to be specified, simplify recovery and post processing of cutsets, and simplify logic models. Such capabilities may be beneficial to the generation of SPAR models for future plants.

5.7 Human Reliability Analysis

Human reliability analysis continues to presents challenges in risk assessment. Currently, there is a very active research program both at the NRC, with industry, and internationally. Additional research will be needed to address outstanding issues and new issues related to advanced reactor designs.

5.7.1 Current HRA Research

The NRC has recognized that the quantification of human reliability and the identification and modeling of human failure events continues to be a challenge in risk assessments. Due to the range of different HRA methods available, with significant differences in their scope, approach, and underlying models and data, it is clear that human reliability modeling introduces large uncertainties in PRAs. In the last few years the NRC has taken a number of steps to address this situation. In particular, the development of HRA Good Practices (NUREG-1792 [46]) provides guidance for meeting RG1.200 and the ASME PRA Standard and thereby supports the performance of a quality HRA. In addition, the evaluation of a number of commonly used HRA methods against these good practices (NUREG-1842 [47]) identified potential strengths and weaknesses of these methods that could bear on the validity and reliability of their results, particularly with respect to the quantification process.

Based on these results and on earlier benchmarking studies (e.g., ISPRA study) that showed significant variability in the results produced by different HRA methods for the same event and by different teams using even the same methods, the NRC has initiated a number of efforts to provide a basis for improving HRA technology and to extend the state-of-the-art as needed to be able to address applications for which existing methods were not specifically designed (e.g., fires and advanced reactors). These efforts include the following:

- An ongoing international effort (including regulatory and industry representatives from more than 10 countries) to investigate the validity and reliability of HRA methods and identify ways to improve the methods as needed, by testing their application to nuclear power plant operating crew performance in the HAMMLAB simulators at the Halden Reactor Project in Norway
- The development of an event database (Human Event Repository and Analysis [HERA]) tool to support HRA and the basis for predictions
- Completion of the ATHEANA User's Guide (NUREG-1880 [48]), a "second generation" HRA method that provides guidance for more realistic assessment of human performance and the identification of errors of commission

- An ongoing effort between the NRC and EPRI to develop a fire specific HRA quantification method to support NUREG-6850 and NFPA 805
- Projects to identify human performance issues for advanced reactors, gaps in existing HRA methods related to advanced reactors, and potential research needs.

The international HRA community is also taking steps to improve the state-of-the-art in HRA by participating in the international benchmarking study noted in the first bullet above and by striving to improve HRA methodology with 2nd generation HRA methods such as CESA, MERMOS, and NARA. In addition, both KAERI and the Halden Reactor Project have been conducting experiments in nuclear power plant control room simulators and collecting data to help understand human performance in control rooms and to support the development of a database to support HRA quantification (e.g., OPERA).

Finally, the US nuclear power industry (e.g., as represented by EPRI), also recognizing potential limitations in the validity and reliability of HRA methods, has been developing the EPRI HRA Calculator$^{®}$ to facilitate the application of HRA and to help standardize the process with the hope of improving consistency of application. The HRA Calculator is a software tool to support application of several HRA methods typically used by industry. EPRI is also working with the NRC in the development of a fire HRA quantification process and there are plans to work with the NRC in another joint effort to investigate and propose either a single HRA model for the agency and industry to use in full power PRAs or a set of methods to be used depending on the specific circumstances, along with guidance for selecting when to use the different methods.

5.7.2 Research Needs

Although the discussion of current research in the area of HRA illustrates that significant steps are being taken to evaluate, improve, and extend HRA methods for use in PRA, there are several critical areas needing additional research.

5.7.2.1 Improving HRA Judgments and Analysis

Evaluations of HRA methods (e.g., NUREG-1842) and the initial data from the ongoing HRA benchmarking studies suggest that the judgments made in HRA about the contribution of different performance shaping factors (PSFs) and the strength of their effects in accident scenarios can be subtle and difficult. In addition, the analysis performed to understand scenario context and identify the drivers likely to influence operating crews in specific scenarios (qualitative understanding) can be complicated. Most existing HRA methods and even HRA process documents like SHARP1 do not provide adequate guidance to support this analysis. For example, in recent years it has become clear that more of a cognitive task analysis is needed to understand operator performance, as opposed to only the more traditional human factors task analysis and its emphasis on how the human interacts with the system. Although studies like the benchmarking effort can help identify where the various methods tend to have problems, determining the types of additional guidance that needs to be provided to analysts to improve the results from the methods may not necessarily be obvious. In other words, what type of guidance will be effective to support this analysis and improve the ability to predict operating crew performance? ATHEANA and other 2nd generation methods such as MERMOS and CESA have

taken steps to address this issue, but it is not yet clear that these approaches are adequate, particularly for supporting application of simpler, less resource intensive HRA approaches such as SPAR-H. A concerted effort to identify and test the types of information and analysis guidance (e.g., cognitive task analysis for nuclear power plant scenarios) that will improve HRA is needed.

5.7.2.2 Simulator Experimentation and Data Collection

There are several ways in which the continued collection of human performance data from simulators can improve HRA.

- With respect to improving analyst's judgments in HRA, the more that is known about how different levels of PSFs and their interactions affect control room performance, the easier it will be to develop appropriate guidance. Thus, the type of research done at Halden, particularly research examining the effects of different PSFs such as scenario complexity, team dynamics, and stress in PRA like scenarios, would be very useful.

- A major limitation in HRA is that there is an inadequate empirical basis to support the quantification of human failure events in PRAs. In other words, the quantitative data (e.g., basic human error rates and PSF multipliers) in HRA methods used to derive human error probabilities (HEPs) do not have a strong empirical basis. Since there are very few actual accidents in the nuclear power industry, one way to obtain useful data is through the systematic collection of operating crew performance during simulator exercises (e.g., during training). If the nuclear power industry and the NRC would systematically collect human performance data during training scenarios involving PRA related accident scenarios, enough actual trials may be run to collect failure rate data on various human failure events modeled in the PRA. Although there are some problems with generalizing such data to real world events and there are several data collection issues (e.g., adequate experimental controls) that would need to be addressed to obtain as valid and reliable data as possible, such data collected across hundreds of crews performing PRA related accident scenarios should provide insight into the likelihood of error and the factors driving performance. Even If the data can not be considered definitive, it might still serve as "anchoring" information for use deriving predicted HEPs for use in PRA. In addition, such data collection would provide information about needed "fixes" in plant characteristics that could be used to reduce the potential for human error and lower estimates of HEPs in PRAs.

5.7.2.3 Human Performance in Advanced Reactors

With the introduction of computerized control rooms and digital instrumentation and control in advanced reactors, the way operators interact with the plant will change dramatically (e.g., see Reference 49). While computerized control rooms and digital I&C will in all likelihood greatly facilitate operator control of the plant, there are a number of issues related to operator interaction with these computer systems that could negatively impact operator performance and effect error rates. These issues have not been considered in HRA and it is unclear whether existing HRA methods can appropriately address these issues without modifications. Digital I&C based

simulators could be used to investigate how operating crews use these systems and where potential problems might arise that could affect the probability of error in certain scenarios or conditions.

The bottom line is that existing HRA methods were not developed to address operating conditions projected for advanced reactors. In addition to the computerized control room, there are number of new conditions (not normally treated by current HRA approaches) that will be created by the planned designs for new reactors. Examples include long-term and slowly evolving accidents, inclusion of multiple reactor modules that share the same control room, and a greater reliance on passive systems. These conditions will impact the tasks and roles of operating crews and thereby influence the likelihood of human actions and their probabilities. Given that previous HRA methods did not explicitly address these conditions, revisions to human error probabilities and new guidance for obtaining appropriate probabilities may be needed. While most of the human related characteristics of new reactors should facilitate performance and reduce the impact of the human role, at least some investigation of potential negative consequences and their impact on performance should be performed [50].

5.7.2.4 Extension of HRA to Other Conditions

In addition to extending HRA to address fire initiated accident scenarios, there are several other important conditions that have not been specifically or adequately addressed by HRA. They include the following:

- Severe-accident conditions. In the past (e.g., individual plant examinations (IPEs), and other Level 2 and Level 3 analyses), PRA/HRA modeling has tended to not address the role of operating crews in modeling severe accident conditions. In general, in the IPEs, crew actions after core damage were not credited. However, severe accident management guidelines (SAMGs) are available and it would appear that there are a number of actions operating crews, in conjunction with a technical support group (TSG), could perform to mitigate the consequences of a severe accident. There are a number of conditions in the context of a severe accident that have not been addressed by HRA, such as the availability and adequacy of procedures and training to support the actions, the impact of crews having to interact with a TSG to decide a course of action, which in many cases may have to be knowledge-based rather than procedure-based, the availability of staff and equipment needed to perform the actions, and a new set of environmental conditions to consider. Much of the information needed to advance HRA to be able to understand and model such conditions would come through working with appropriate licensee staff in a range of specific plants and plant types.

- Low power and shutdown conditions, particularly in the context of a fire. Although HRA models like ATHEANA can be used to address these conditions, guidance on the additional context that needs to be considered and their impacts has not been explicitly provided.

- Fuel Handling and related activities. Although PRAs of fuel handling and related activities have not been common, to the extent they might become useful, investigation of

potential error modes, the specific factors that could influence the likelihood of errors in these activities, and what guidance might need to be added to HRA methods, would be useful.

5.7.2.5 Other HRA Related Areas Needing Research

- Development of HRA methods that rely primarily on the role of time. The ACRS has recently proposed [18] "that an alternative approach to HRA is to recognize the importance of time taken by the crew to complete a task and to develop a probability distribution for this time. The failure probability, then, is calculated from this distribution as the probability that this time will exceed the available time." There are a number of potential advantages from such an approach but there are also potential limitations. One potential advantage is to be able to integrate such modeling with the current time-based human cognitive models being developed for NASA and the DOD. Also, as is discussed below, computer based cognitive models of crew performance (including team behavior) in accident scenarios could be very useful in supporting dynamic PRA modeling.

- Development of computer models of human cognitive performance in control rooms that eventually could directly generate HEPs based on scenario conditions and knowledge of factors influencing performance. Such models would, from an HRA perspective, greatly enhance the ability to do dynamic PRA. Using current "manual" approaches to HRA functionally prohibits the ability to realistically do dynamic PRA. Such models might also be used to allow assessment of the impact of plant changes on human performance. Of course, the development of models that could be used to address plant specific performance would be non-trivial. It seems likely that separate models would be needed for each plant (or at least plant type) in order to be able account for plant specific characteristics. Additional investigation is needed to determine if such modeling could be effective and benefit HRA approaches.

5.8 Seismic PRA

Seismic PRA is now in widespread use throughout the nuclear-power industry worldwide, by the operating NPPs themselves, by the various national regulatory agencies, and by the designers of new NPPs. The performance of a seismic PRA can systematically accomplish several very important objectives; specifically, it can contribute:

- to understanding the seismic risk arising from NPPs,
- to understanding the safety significance of seismic design shortfalls,
- to prioritizing seismic safety improvements,
- to evaluating and improving seismic regulations, and
- to modifying the seismic regulatory/licensing basis of an individual NPP.

However, there are three important methodology issues regarding seismic PRAs and its resulting uncertainties that have been widely recognized for many years. These issues were reiterated at the "Specialists Meeting on Seismic Probabilistic Safety Assessment (SPSA) of Nuclear

Facilities", held in Jeju, Korea on 6-8 November 2006. Summaries of these issues are repeated in the following sections

5.8.1 Probabilistic Seismic Hazard Analysis (PSHA)

Results of properly conducted PSHA studies for regions with low to moderate seismicity typically exhibit large uncertainty. One source of uncertainty is the fact that there are very few strong-motion earthquakes in such regions, so that attenuation relationships must start with those taken from other regions with available strong motions. Seismic hazard experts typically select regions with analogous tectonics and structure, and may also rely on simulations using seismological models based on regional geophysical features. A proper PSHA in such cases must reflect the uncertainty due to insufficient knowledge of the regional ground motions. This can lead to inconsistencies or to large uncertainties, depending on the choices made by the seismic hazard experts. In such situations, a strategy to improve knowledge and to reduce uncertainty should involve improving strong-motion data collection, and research to improve regional-specific attenuation relations.

To address this issue PSHA must be performed in as realistic a way as possible, in order to reach a probabilistic result in the form of a realistic distribution that includes all of the uncertainties and all of the variability observed in nature, and adequate consideration of dependencies among the governing factors. In addition, PSHA results should be compared to all available observations, especially for return periods where records are available, in order to get an objective comparison and to improve the confidence in the results, at least in that range of return periods. An extensive comparison should be performed between PSHA results conducted in different regions, including low to moderate seismicity regions as well as high seismicity regions, especially in the range of return periods where observed data are available. In this effort, comparisons should be made on a one-to-one basis, with study type and quality being key control variables. A well-executed PSHA would normally include these three desirable features described above, along with several additional state-of-the-art characteristics, as for instance required in the ANS Standard. Since seismic hazard analysis forms a key element of seismic PRA with major safety and cost impact on nuclear power plants, NRC guidance on PHSAs should be reviewed to ensure future PSHAs meet these requirements.

5.8.2 Human Reliability Modeling of On-Site and Off-Site Responses

There remains continuing uncertainty in quantifying the response of plant operators and emergency organizations after earthquakes. Partly, the problem is generic with all human reliability analysis: uncertainties and the lack of data. However, there are specific characteristics of earthquakes that make post-earthquake actions more difficult to analyze and quantify. Among these characteristics are physical and mental consequences of a seismic shock. Such consequences are due in part to the damage and accessibility of equipment, consequential events such as fires that would increase the operators' workload and stress, conflicting goals of the government authorities in case of a large earthquake, accessibility to the site and other possible factors.

Similar efforts to develop HRA quantification methods for seismic events as is currently being done for fire events should be considered (see Section 5.7.1). In addition it may be beneficial to collect information from conventional industrial sites after large earthquakes as a way to increase our knowledge about operator and emergency-organization responses after seismic events.

5.8.3 Treatment of Correlations

Seismic PRA analysts have struggled with the problem of how to quantify the correlations in the failures of similar equipment or similar structures due to the earthquake. Everyone accepts that some correlations certainly exist, for example in the response of two identical pumps located near each other, or arising from the identical design and construction of two identical shear walls. Quantifying these correlations has seldom been done in a rigorous way. Analysis is complex, testing has produced ambiguous insights at best, and the experience data base from real earthquakes is difficult to interpret. The analysts have usually used sensitivity studies to identify where the numerical results are sensitive, but they have also usually assigned large uncertainties to the numbers.

The experience with the seismic PRAs for existing U.S. plants is that the seismic core damage frequency is usually dominated by one or more low-seismic capacity singletons, i.e. single contributors to a PSA cut set. In these cases, therefore, the impact of correlation was judged to be small, if any. The situation may be different in future in situations where the design basis earthquakes are higher and the goal is to demonstrate a relatively low seismic risk. Assuming perfect dependence between redundant co-located components may be too conservative in situations where low-capacity singletons are avoided by design. Further examination of this issue may be warranted.

5.9 Internal Fires

A cooperative effort with EPRI resulted in the development of a fire PRA methodology document (NUREG/CR-6850 [51]). Although this document advanced the state-of-the art in fire PRA, there were several areas that were not improved or have limited guidance. They include:

- the number of combined fire-induced spurious actuations that should be modeled
- dynamic versus static modeling of fire damage and operator response
- multiple fires
- multiple initiating events occurring from the same root cause (e.g., fire and flood in combination)
- smoke damage
- modeling of seismic-induced fires
- effectiveness of fire protection systems
- effectiveness of passive fire barriers

Further development of the fire PRA methodology to address some of these limitations would provide more accurate results in NFPA 805 applications. Furthermore, expansion of the fire PRA methodology to address fires during LPSD was initiated but has been placed on hold

primarily due to the lack of EPRI support at this time. Eventual expansion of the fire PRA methodology development to LPSD conditions would be beneficial for NFPA 805 applications.

Finally, recent industry experience with applying the NUREG/CR-6850 has provided feedback on the methodology. Some potential problems have been identified. The validity of these problems needs to be reviewed and if found to be substantiated should be corrected.

5.10 Fuel Cycle Facility Risk Assessment

Closing of the nuclear fuel cycle will require operation of reprocessing plants. For such facilities, the type of risk assessment method necessary to meet the Integrated Safety Assessment (ISA) requirements in 10 CFR Part 70 has not been determined. SECY-99-100 [52] provided a summary of ISA approaches for different material-related activities. PRAs were listed for transportation activities and evaluation of dry cask storage. However, the SECY did not address the type of reprocessing /fuel fabrication facility that would likely be in operation in a closed fuel cycle. Preliminary consideration by the NRC staff on licensing requirements of reprocessing facilities being considered as part of the Global Nuclear Energy Partnership (GNEP) plans as raised the possibility that a PRA may be required.

It is not known if a PRA has ever been performed for a reprocessing facility. The hazards associated with such a facility would include fires, explosions, and criticalities. Possible consequences include not only radiological doses to workers and the public but also chemical toxicity considerations. The data, methods, and models needed for a reprocessing facility PRA needs to be identified and/or developed. A guidance document for reprocessing facility PRAs also would be beneficial to this effort.

5.11 Transportation Risk Assessment

The traditional risk assessment method associated with transporting radioactive materials was first described in NUREG-0170 [53]. The radiation doses and risks from routine, incident free transportation are assessed by modeling the radioactive cargo as a sphere moving on the transportation route at a particular speed. The radiation source is the external dose rate of the cargo modeled as a virtual source at the center of the sphere. Doses and risks are calculated for a variety of receptors: e.g., residents along the transportation route, occupants of vehicles sharing the route with the radioactive cargo, vehicle crew and maintenance workers, escorts, etc. Transportation by highway, rail, barge, and air can be modeled. Doses to receptors are generally proportional to the cargo dose rate and inversely proportional to the vehicle speed and the square of the distance between vehicle and receptor. Collective dose is calculated by integrating over the selected population and multiplying by the route segment length and the number of shipments. This scheme is modeled by the program and code RADTRAN [54], which benchmarking shows is slightly conservative [55]. RADTRAN has been streamlined and improved; RADTRAN II was used in NUREG 0170 and the current version is RADTRAN 5.6 [56]. However, the basic scheme presented in NUREG 0170 is still the basic scheme used in RADTRAN.

Transportation accidents can result in release of radioactive material and/or loss of lead gamma shielding (in lead-lined casks). Most accidents, however, result in no damage to cargo, but may result in doses to receptors because the vehicle sits in a particular location for several hours. Risks from accidents that involve releases or loss of shielding are modeled based on event trees that describe the universe of accidents. Each particular type of accident has an associated conditional probability and a release fraction for each physical type of potentially released material. Although NUREG 0170 pioneered this model, the first data-based event tree was published in Reference 57. The latter work was refined and updated in Reference 58. Since the dose from an accident depends on the amount of released material reaching a receptor, RADTRAN disperses released material using a Gaussian dispersion model and assumes that the receptor is directly downwind. Doses from loss of lead shielding are modeled analogously to doses from a vehicle that stops during routine transportation. Collective doses are calculated by integrating over the plume footprint and multiplying the result by the number of shipments. Risk is further calculated by multiplying by the traffic accident rate.

5.11.1 Current modeling methods

In 2003, a graphical user interface (GUI) input file generator was launched [59] and RADTRAN was programmed so that almost all input parameters were entered by the analyst. Only the occupational dose to railyard workers is integrated ("hard-wired") into the RADTRAN code. Input parameters include:

- Cargo package and vehicle dimensions
- Cargo external dose rate
- Radiological inventory of the package
- Vehicle speed
- Number of each type of worker associated with the transportation
- Shielding for each type of receptor
- Number of packages per vehicle
- Number of vehicles (number of shipments)
- Population densities of various receptors
- Density of vehicles sharing the route
- Number of stops
- Exposed population at stops
- Accident rate along the route
- Conditional accident probabilities
- Fractions of the inventory released under various accident conditions
- Appropriate thermal and meteorological parameters
- Associated default parameters like breathing rate, lane widths, gamma and neutron attenuation and buildup factors, fraction of outdoor air in buildings, etc

All of the listed parameters are user input and all default values can be overridden. Until 2005, all input parameters had to be single-valued. The sensitivity of doses from routine transportation to various parameters could be calculated by RADTRAN but probabilistic analysis was not possible.

5.11.2 Application of PRA

In 2005, an uncertainty model was launched that allowed distribution of any and all input parameters [60 & 61]. The uncertainty model uses the MELCOR uncertainty engine and allows the user to choose from several different distributions (e.g., Gaussian, lognormal, uniform, beta, etc.) for each distributed input parameter. The engine then samples on each distribution using Monte Carlo sampling, a RADTRAN creates an input file for each sample set (up to 500 samplings) and runs the batch file. The RADTRAN outputs may then be displayed as pdf, cdf, or ccdf graphs.

5.11.3 Research and Development Needs

1. At present RADTRAN has no way to handle coupled input parameters, even though a number of them are known to be coupled (e.g., route length and population, package size and external dose rate, package size and vehicle size). A scheme for handling coupled parameters in RADTRAN would greatly enhance the PRA capabilities of RADTRAN (which are currently rudimentary). Such a scheme needs to be developed and coded.
2. RADTRAN disperses released material using Gaussian dispersion, which greatly overestimated concentrations closer than 50 to 100 meters to the source. In particular, the area near and adjacent to the transportation cask cannot be modeled with Gaussian dispersion, so that releases from, e.g., a hole in the cask cannot be modeled accurately. A near-field model is needed.

RADTRAN could rather easily be modified to assess effects of releases of chemically hazardous materials in an accident. Although this can currently be done by a very well-versed RADTRAN user, the workaround is cumbersome at best. The model should be expanded to include chemically hazardous materials.

6. SUMMARY AND CONCLUSIONS

This chapter presents a summary of the results of an evaluation of the status of the development of advanced PRA modeling and numerical analysis techniques. It includes an evaluation of the current PRA research efforts sponsored by the NRC, a limited review of efforts being sponsored by industry and other international organizations, and provides suggestions for additional PRA research and development. The evaluation was performed by a Sandia National Laboratories team of PRA subject matter experts (SMEs).

The summary of our evaluation is provided in the form of a numbered list that delineates our suggestions with regard to advanced PRA methods development and the bases for those suggestions. The bases for the suggestions are generally related to the need to improve reactor safety through identification and resolution of safety and licensing issues, and for improving the quality of risk inputs for use in risk-informed regulatory decisions and for addressing known PRA challenges. Issues related to both current reactors and future reactor designs are discussed.

1. Dynamic PRA - In addition to the physics modeling approach to dynamic PRA being pursued by Ohio State University, a different approach is being examined by the University of Maryland. The Maryland approach is easier to implement but has limited application. Although the Ohio State method can be used in broader and more detailed applications, further development is warranted. One identified enhancement that could be explored is the possible use of Bayesian networks to facilitate and enhance the modeling. In addition, SNL believes that a hybrid method is possible and would address some of the weakness of the Ohio State method. Such a hybrid approach has been employed by SNL to evaluate the safety of the Mars Science Laboratory.

2. Passive System Modeling – SNL has previously reviewed approximately 60 different passive system modeling techniques for the NRC and issued a letter report in 2006 recommending the use of the Reliability Methods for Passive Systems (RMPS) framework developed under the auspices of the International Atomic Energy Agency (IAEA). An application of that method to an ESBWR was being pursued but was not completed. Sufficient work has been done by others to prove the RMPS concept and further demonstration by the NRC does not appear to be warranted. That project is being closed out. Instead, a similar dynamic PRA method being developed for the NRC by Ohio State University, and that allows for modeling of passive systems, should continue to be pursued. See the discussion under Uncertainty Analysis for suggested improvements to sampling methods that could be employed in this approach.

   Related to the issue of passive system modeling is the need to evaluate the risk impact of aging effects such as degradation of the containment and neutron embrittlement of the reactor vessel. Such evaluations would complement the existing deterministic evaluations used in the licensing renewal process.

3. Uncertainty Analysis – The NRC staff has recently issued draft NUREG-1855 that provides guidance on incorporating epistemic uncertainty into risk-informed decision making. The recommended process for treating model uncertainty is through the performance of sensitivity analyses. Use of additional, advanced methods for treating model uncertainty should be explored.

   a. Uncertainty analysis methods were reviewed in terms of their potential use in driving dynamic PRA models or passive system models. The use of Monte Carlo stratified sampling methods such as Latin Hypercube Sampling (LHS) and quasi-Monte Carlo, and analytical methods such as First and Second Order Reliability Methods (FORM/SORM) have all been used in some applications. Sandia has developed a method that combines quasi-Monte Carlo sampling and analytical methods such that the number of samples required to evaluate the functional reliability of a passive system component is relatively small. Testing of this method is still required but it shows great promise for use in passive system modeling.
   b. With regard to treatment of uncertainty in PRAs, the movement towards the use of hierarchical Bayesian methods described in NUREG/CR-6823 would provide a method for incorporating different levels and types of uncertainty in an integrated fashion.

4. Level 2 PRA Analysis – Most of the current work being sponsored by the NRC in the Level 2 PRA arena is related to the state-of-the-art consequence assessment (SOARCA) project and the continued development and application of severe accident codes such as MELCOR. The SOARCA project has provided some impetus for our suggestions that HRA methods need to be enhanced to address severe accident conditions and that continued SPAR model development, particularly with regard to external events is desirable. The use of a simplified MELCOR and MACCS models by Ohio State as the driver for their dynamic PRA models has provided the added benefit of seamlessly integrating Level 2 and 3 methods (as opposed to the binning of results that was utilized in the NUREG-1150 PRAs for coupling Level 1, 2 and 3 analyses). The application of these simplified versions of the codes in a dynamic PRA framework would be a useful tool for use by the NRC in determining possible accident progressions in the case of an actual event. Additional Level 2 PRA tasks areas that would help improve the state-of-the art of PRA and reduce known uncertainties include:

   a. The applicability of past severe accident phenomena research findings to new reactor designs (e.g., conclusions about direct containment heating on new containment designs) should be examined. Incorporation of a better direct containment heating model into the MELCOR code would be required if this phenomena is assessed to be important.
   b. The quality of Level 2 PRAs would also benefit from the development of a technical guidance document on modeling of severe events that lead to early containment failure (e.g., steam explosions, hydrogen burns, and direct containment heating) that would replace the current reliance on the analysts' judgment.

c. Recent information from Phebus experiments suggests that currently used chemical specifications used in Level 2 PRA source term analyses may be flawed. Changes in nuclide groupings have been proposed but have not been documented and their impact on source terms needs to be determined.

d. The modeling of the containment performance due to over pressure events historically has been very simplistic in that limited levels of leakage have been modeled. The modeling of containment leakage as a continuous function of pressure and temperature, rather than based on a failure threshold, could be developed based on existing data from scaled model experiments. Its use would more realistically evaluate containment performance.

5. Level 3 PRA – The MACCS2 code is currently the NRC-sponsored code being used in Level 3 PRAs to determine the consequences from reactor accidents. The code uses a straight line Gaussian plume model for atmospheric transport and dispersion and thus sacrifices accuracy for computational speed. The lack of accuracy can be significant for some sites with complex wind patterns (e.g., near oceans or canyons). Incorporation of a Gaussian puff model, which follows wind shifts, into MACCS would improve the accuracy of consequence assessments. Additional improvements are possible and include:

a. Modification of the code to handle higher angular resolution site data (meteorological and population) would improve the accuracy of the results.

b. An improvement to the emergency response model to allow simulation of different responses within different radius from the plant would improve the calculated results (the code currently requires uniform treatment within a specified zone).

c. The economics model in MACCS2 could be enhanced to ensure completeness of all impacts, to eliminate conservatisms by accounting for compensating effects, and to add flexibility to accommodate politically driven decisions.

6. Digital Instrumentation and Control Systems – Two recent reviews of different methods for analyzing digital I&C systems have performed. One assessed traditional methods (i.e., methods that do not explicitly account for the time element in the system operation) and dynamic methods which include the time element. SNL agrees with a conclusion of the traditional method review performed by Brookhaven National Laboratories that incorporation of digital I&C system reliability into an event and fault tree approach seems to be a logical path. However, we do not strongly support the further examination of either simple or dynamic Markov models (this is the recommended approach suggested in the dynamic method review performed by Ohio State University). Furthermore, we disagree with the conclusions reached by Ohio State University about Bayesian models and believe that there may be some misunderstanding on their part related to Bayesian techniques (e.g., that they can not model dynamic interactions). Bayesian methods are applied in other fields (medical and financial) that involve dynamic conditions. Thus, SNL suggests that the Bayesian methods offers sufficient benefits that warrants further consideration for modeling digital I&C systems. One significant benefit

is that it provides a method for addressing software reliability particularly taking into account the software complexity and the developmental process.

7. Quantification Techniques - Since SAPHIRE is the tool used for evaluating SPAR models, continued maintenance and enhancement of the codes is critical to the staff's ROP and RIR efforts. Some improvements to numerical techniques for solving PRA models, if incorporated into SAPHIRE, would increase the accuracy of the code evaluations and resulting regulatory decisions (e.g., risk importance measures and their use in several RIR applications). Specifically, the use of Binary Decision Diagrams (BDD) should be examined as one means to improve the PRA model quantification process. Hybrid approaches, such as those being pursued by EPRI, should be considered as means to overcome limitations associated with BDDs (e.g., not solvable for large fault trees).

In addition to assessing advanced PRA R&D efforts and needs, the Sandia SMEs also assessed current methods and identified potential areas for improvements. The results of this assessment are provided below.

1. Human Reliability Analysis (HRA) – Based on the importance of human errors on reactor safety, significant work to improve HRA methods and data is ongoing at the NRC, internationally, and at EPRI. The NRC work includes an international effort to benchmark existing HRA techniques against actual plant operating crew performance, development of the Human Event Repository and Analysis (HERA) database to support HRA and the basis for predictions, a joint effort with EPRI to develop a fire-specific HRA quantification method, and other projects to identify human performance issues for advanced reactors. SNL supports continued work in these areas but believes that the following additional HRA research would be beneficial:

   a. While the benchmarking study will help identify where various HRA methods tend to have problems, additional work will be required to determine the type of additional guidance that needs to be provided to analysts to improve the quantification of human error probabilities (HEPs).
   b. Expanded examination of the effects of different performance shaping factors (e.g., in simulator exercises), including their interactions, would improve HRA predictions.
   c. The empirical basis to support the quantification of human error events could be expanded by the systematic collection of operating crew performance during simulator exercises (i.e., during training exercises)
   d. New and advanced computerized control rooms and the use of digital I&C will change the way operators respond to conditions. How these control room advancements and plant designs affect HEP predictions needs to be addressed.
   e. As with the case for internal fires, HRA methods need to be expanded to address other important scenarios that have not been specifically or adequately addressed. Specifically, actions performed during LPSD accidents and under severe accident conditions (e.g., those directed by severe accident management guidelines with

input by personnel from a technical support center). In addition, latent errors during the design and construction process are an important issue for passive system reliability and for digital system programming.

f. Potential expansion of PRA to analyze fuel reprocessing facilities may require enhancement of HRA methods that can evaluate HEPs during accidents in those types of facilities.

g. Investigate potential for HRA methods that rely primarily on time. One potential advantage is to be able to integrate such modeling with the current time-based human cognitive models being developed for NASA and the DOD.

h. Development of computer models of human cognitive performance in control rooms that eventually could directly generate HEPs based on scenario conditions and knowledge of factors influencing performance. Such models would, from an HRA perspective, greatly enhance the ability to do dynamic PRA.

2. Seismic PRA – Seismic PRA is now in widespread use throughout the nuclear-power industry worldwide. However, there are three important methodology issues regarding seismic PRAs and its resulting uncertainties that have been widely recognized for many years.

a. Results of properly conducted PSHA studies for regions with low to moderate seismicity typically exhibit large uncertainty. Since seismic hazard analysis forms a key element of seismic PRA with major safety and cost impact on nuclear power plants, NRC guidance on PHSAs should be reviewed to ensure future PSHAs meet these requirements.

b. There remains continuing uncertainty in quantifying the response of plant operators and emergency organizations after earthquakes. Similar efforts to develop HRA quantification methods for seismic events as is currently being done for fire events should be considered. In addition it may be beneficial to collect information from conventional industrial sites after large earthquakes as a way to increase our knowledge about operator and emergency-organization responses after seismic events.

c. Seismic PRA analysts have struggled with the problem of how to quantify the correlations in the failures of similar equipment or similar structures due to the earthquake. Quantifying these correlations has seldom been done in a rigorous way. Assuming perfect dependence between redundant co-located components may be too conservative in situations where low-capacity singletons are avoided by design. Further examination of this issue may be warranted.

3. Fire PRA Methodology – A cooperative effort with the Electric Power Research Institute (EPRI) resulted in the development of a fire PRA methodology document (NUREG/CR-6850). Although this document advanced the state-of-the art in fire PRA, there were several areas that were not improved and identified in the report as limitations. For example, modeling of smoke damage has not been addressed in sufficient detail to evaluate its importance. Further development of the fire PRA methodology to address these limitations would provide more accurate results in NFPA 805 applications. Furthermore, expansion of the fire PRA methodology to address fires during LPSD was initiated but has been placed on hold primarily due to the lack of EPRI support at this

time. Eventual expansion of the fire PRA methodology development to LPSD conditions would be beneficial for NFPA 805 applications.

4. Fuel Cycle Facility PRAs – Closing of the nuclear fuel cycle will require operation of reprocessing plants. For such facilities, a PRA may be required to meet the Integrated Safety Assessment requirements in 10 CFR Part 70. The data, methods, and models needed for these PRAs needs to be identified and/or developed. A guidance document for reprocessing facility PRAs would be beneficial to this effort.

5. Transportation Risk – Transportation accidents can result in release of radioactive material and/or loss of lead gamma shielding (in lead-lined casks). The RADTRAN code is currently used in risk assessments of transportation accidents. Two potential areas for improvement of this code and the resulting risk assessments have been identified:

   a. A scheme for handling coupled parameters in RADTRAN would greatly enhance the PRA capabilities of RADTRAN (which are currently rudimentary).
   b. RADTRAN disperses released material using Gaussian dispersion, which greatly overestimated concentrations closer than 50 to 100 meters to the source. A near-field model is needed.

7. REFERENCES

[1]   "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program", NUREG-1635, Vol. 7, Advisory Committee on Reactor Safeguards, May 2006

[2]   "U.S. Nuclear Regulatory Commission Long-Term Research: Fiscal Year 2009 Activities," U.S. Nuclear Regulatory Commission, October 2007.

[3]   Emrit, R. et al., "A Prioritization of Generic Safety Issues," NUREG-0933, U.S. Nuclear Regulatory Commission, September 2007.

[4]   "Clarification of TMI Action Plan Requirements," NUREG-0737, U.S. Nuclear Regulatory Commission, November 1980.

[5]   "GSI-191: The Impact of Debris Induced Loss of ECCS Recirculation on PWR Core Damage Frequency", NUREG/CR-6771, Los Alamos National Laboratory, August 31, 2002.

[6]   "Safety Assessment of BWR Reactor Internals," BWRVIP-06-A, Electric Power Research Institute.

[7]   "Technical Basis for Revision of the Pressurized Thermal Shock (PTS) Screening Limit in the PTS Rule (10 CFR 50.61)," NUREG-1806, U.S. Nuclear Regulatory Commission, August 2007.

[8]   "A Pilot Probabilistic Risk Assessment of a Dry Cask Storage System," NUREG-1864, U.S Nuclear Regulatory Commission, March 2007.

[9]   "Risk Assessment of Severe Accident-Induced Steam Generator Tube Rupture," NUREG-1570, U.S. Nuclear Regulatory Commission, March 1998.

[10]   "An Integrated Risk-Informed Decision-Making Process for Emergent Issues," LIC-504,

[11]   SECY-93-092, "Issues Pertaining to the Advanced Reactor (PRISM, MHTGR, and PIUS) and ANDU 3 Designs and Their Relationship to Current Regulatory Requirements," April 8, 1993.

[12]   "Technical Basis for Revision of the Pressurized Thermal Shock (PTS) Screening Limit in the PTS Rule (10 CFR 50.61)," NUREG-1806, U.S. Nuclear Regulatory Commission, august 2007.

[13]   Soffer, L, et al., "Accident Source Terms for Light-Water Nuclear Power Plants- Final Report," NUREG-1465, U.S. Nuclear Regulatory Commission, February 1995.

[14]   SECY-02-00139, "plan for Resolving Policy Issues Related to Licensing Non-Light Water Reactor Designs, July 22, 2002.

[15]   SECY-03-0047, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs," March 28, 2003.

[16]   Fleming, K.N., "Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making," NUREG/CR-6813, U.S. Nuclear Regulatory Commission, April 2003.

[17]   SECY-06-0217, "Improvement Plan to and Update of the Risk-informed Regulation Implementation Plan," October 25, 2006.

[18]   "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program", NUREG-1635, Vol. 7, Advisory Committee on Reactor Safeguards, May 2006.

[19]   SECY-03-0059, "NRC's Advanced Reactor Research," April 18, 2003.

[20]   T. Aldemir, D.W. Miller, M.P. Stovsky, J. Kirschenbaum, P. Bucci, A.W. Fentiman, L.T. Mangan, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," NUREG/CR-6901, U.S. Nuclear Regulatory Commission, Washington, D.C., February 2006.

[21]   T. Aldemir, M.P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L.A. Mangan, D.W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, And S.A. Arndt, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NUREG/CR-6942, U.S. Nuclear Regulatory Commission, Washington, D.C., October 2007.

[22]   Robinson, D. "A Survey of Probabilistic Methods Used In Reliability, Risk and Uncertainty Analysis: Analytical Techniques I," SAND98-1189. June 1998.

[23]   Robinson, D. "A Survey of Probabilistic Methods Used In Reliability, Risk and Uncertainty Analysis: Analytical Techniques II," 1999, unpublished.

[24]   Robinson, D. "A Survey of Probabilistic Methods Used In Reliability, Risk and Uncertainty Analysis: Monte Carlo Methods," 1999, unpublished.

[25]   Robinson, D. "CRAX/Cassandra User Manual," SAND99-3162, December 1999.

[26]   Robinson, D. "Application of Spatial Statistics in Characterizing Structural Reliability and System Uncertainty," SAND99-2055, August 1999.

[27]   U.S. Provisional Patent Application Serial No. 60/251,312, entitled "Field Analysis Method and Application including Uncertainty in Complex Computer Simulations," filed on December 4, 2000.

[28] Robinson, D., C. Atcitty, "Comparison of quasi- and pseudo-Monte Carlo Sampling for Reliability and Uncertainty Analysis," AIAA-99-1589, a comparison of qMC and LHS.

[29] Robinson, D. "A Hierarchical Bayes Approach to System Reliability Analysis," SAND2001-3513, November 2001.

[30] Robinson, D., C. Atcitty, "The Application of Bayesian Methods for System Reliability Analysis," SAND2005-7300, October 2004.

[31] Celeux, G., M. Persoz, J. Wandji, F. Perrot, "Bayesian Modeling of PWR Vessels Flaw Distributions," INRIA Report No. 3551, undated report.

[32] Robinson, D., J. Zuffranieri, "A Bayesian Approach For Combining Materials Aging Analyses with Component Reliability Analyses", unpublished report.

[33] Zuffranieri, J., D. Robinson, "A Bayesian Approach for Health Monitoring of Critical Systems", IEEE Aerospace Conference, Big Sky, Montana, 5 March 2005

[34] Robinson, D., C. Atcitty, J. Zuffraneri, D. Arent, "Impact of Distributed Energy Resources on the Reliability of a Critical Telecommunications Facility," SAND2006-1277.

[35] Jun, Joonyub, A. Kandt, D. Robinson, P. Lilienthal, D. Arent, "Risk-based Approach to Incorporating Renewable Energy Into Critical Facilities," SAND2008-1101C.

[36] Pratt, W., et al., "An Approach for Estimating the Frequencies of Various containment Failure Modes and Bypass Events," NUREG/CR-6569, U.S. Nuclear Regulatory Commission, October 2004.

[37] T.L. Chu, G. Martinez-Guridi, Meng Yue, John, Lehner, And Pranab Samanta, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," NUREG/CR-XXXX, U.S. Nuclear Regulatory Commission, Washington, D.C. (Not yet published).

[38] T. Aldemir, D.W. Miller, M.P. Stovsky, J. Kirschenbaum, P. Bucci, A.W. Fentiman, L.T. Mangan, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," NUREG/CR-6901, U.S. Nuclear Regulatory Commission, Washington, D.C. (2006).

[39] T. Aldemir, M.P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L.A. Mangan, D.W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, And S.A. Arndt, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NUREG/CR-6942, U.S. Nuclear Regulatory Commission, Washington, D.C. (2007).

[40]   Y. Zhang And M. Golay, "Development of a Method for Quantifying the Reliability of Nuclear Safety-Related Software", Annual Report, Nuclear Engineering Education Research (NEER), Grant program, October 2003.

[41]   M. Yue And T. Chu, "Estimation of Failure Rates of Digital Components Using a Hierarchical Bayesian Method", PSAM8, New Orleans, LA, May 14-19, 2006.

[42]   C. Berzuini, R. Bellazzi, S. Quaglini, And D.J. Spiegelhalter, "Bayesian Networks for Patient Monitoring", *Artificial Intelligence in Medicine*, 4, pp. 243-260, (1992).

[43]   Carlo Berzuini, Riccardo Bellazzi, And David Spiegelhalter, "Bayesian Networks Applied to Therapy Monitoring", *Statistics in Medicine*, 13, 8, pp. 823-838, (1994).

[44]   Carlo Berzuini And Cristiana Larizza, "Dynamic Forecasting with Bayesian Networks," *Neural Networks in Biomedicine, pp. 195-212*, 1994.

[45]   Jason V. Zuffranieri And David G. Robinson, "A Bayesian Approach for Health Monitoring of Critical Systems," Aerospace Conference, 2005 IEEE, pp. 3641-3646 (2005).

[46]   Kolackowski, A, et al., "Good Practices for Implementing Human Reliability Analysis (HRA)," NUREG-1792, U.S. Nuclear Regulatory Commission, April 2005.

[47]   Forester, J., et al., "Evaluation of Human Reliability Analysis Methods Against Good Practices," NUREG-1842, U.S. Nuclear Regulatory Commission, September 2006.

[48]   Forester, J., et al., "ATHENA User's Guide," NUREG-1880, U.S. Nuclear Regulatory Commission, June 2007.

[49]   O'Hara, J., Higgins, J., Brown, W. & Fink, R., "Human Performance Issues in Advanced Reactors," Report No. Y6646-T4-11/03, Brookhaven National Laboratory, Upton, New York, 2004.

[50]   Forester, John, Alan Kolaczkowski, and Sean Dunagan, "Human Reliability Analysis Issues and Research Needs for Advanced Reactors," Sandia National Laboratories, NRC Letter Report, January 26, 2006.

[51]   "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," NUREG/CR-6850, U.S. Nuclear Regulatory Commission, August 2005.

[52]   SECY-99-100, "Frameworkfor Risk-Informed Regulation in the Office of Nuclear Material Safety and Safeguards," March 31, 1999.

[53]   "Final Environmental Impact Statement on the Transportation of Radioactive Materials by Air and Other Modes." NUREG-0170, U.S. Nuclear Regulatory Commission, 1977

[54] Neuhauser, K.S.; Kanipe, F.L.; Weiner, R.F, RADTRAN 5, Technical Manual, SAND2000-1256, Sandia National Laboratories, Albuquerque, New Mexico, 2000.

[55] Steinman, R. L., Weiner, R.F., Kearfott, K., "Comparison of Transient Dose Model Predictions and Experimental Measurements," *Health Physics* v. 83 (2002), p.504 et seq. 2002.

[56] Weiner, R.F. et. al,. RADTRAN 5.6, Technical Manual. Albuquerque, New Mexico: Sandia National Laboratories, 2006.

[57] Fischer, L.E.; Chou, C.K.; Gerhard, M.A.; Kimura, C.Y.; Martin, R.W.; Mensing, R.W.; Mount, M.E.; Witte, M.C., "Shipping Container Response to Severe Highway and Railway Accident Conditions," NUREG/CR-4829, U.S. Nuclear Regulatory Commission, 1987.

[58] Sprung, J.L.; Ammerman, D.J.; Breivik, N.L.; Dukart, R.J.; Kanipe, F.L.; Koski, J.A.; Mills, G.S.; Neuhauser, K.S.; Radloff, H.D.; Weiner, R.F.; Yoshimura, H.R., "Reexamination of Spent Fuel Shipment Risk Estimates," NUREG/CR-6672, U.S. Nuclear Regulatory Commission, 2000.

[59] Weiner, R.F. Osborn, D.M., Hinojosa, D., Penisten, J.J., Heames, T.J., Orcutt, D.J., RADCAT 2.3 User Guide, SAND2005-1963, Sandia National Laboratories, 2006.

[60] Penisten, J.J., Dennis. M.L. Weiner, R.F, "Uncertainty in Modeling Risks of Transporting Radioactive Materials," ANS Winter Meeting, Washington, DC, November 2005.

[61] Weiner, R.F. Dennis, M.L., Penisten, J.J., Heames, T.J. Osborn, D,M, "Incorporating Uncertainty in RADTRAN Input Files," SAND2006-5679, Sandia National Laboratories, 2006.

[62] SECY-07-0074, "Update on the Improvements of the Risk-informed Regulation Implementation Plan," April 26, 2007.

APPENDIX A

RISK-INFORMED AND PERFORMANCE-BASED INITIATIVES AT THE NRC

This appendix provides listings of NRC-sponsored activities in risk-informed regulation and PRA development from several sources.

Table A-1 lists the Risk-Informed and Performance-Based Plan (RPP) projects presented in SECY-07-0074 [62]. The table provides a high-level summary of the RPP initiatives and their status.

Table A-1. Risk-informed and performance-based projects at the NRC.

Regulatory Functional Area	Initiative	Program or Project	Project Description and Major Activities	Major Project Activities
Oversight	Reactor Oversight Process (ROP)	ROP	Develop a risk-informed assessment process for determining NRC actions based upon performance indicator and inspection information.	Implement process to monitor licensee performance with respect to reactor safety cornerstones and to monitor licensee activities using performance indicators. Depending on the assessment results, inspection resources may be expended to focus on licensees with degraded or declining performance. Implement Mitigating System Performance Index (MSPI) program. MSPI monitors risk associated with changes in performance of selected mitigating systems, accounting for plant-specific design and performance data.
Oversight	Accident Sequence Precursor	Accident Sequence Precursor	Systematically review and evaluate operating experience to identify precursors to potential severe core damage sequences, documenting precursors, categorizing them by plant-specific and generic implications, and providing a measure of trends in nuclear plant core damage risk.	Determine the safety significance of events and their regulatory implications; provide feedback to improve probabilistic risk assessment (PRA) models; and provide NRC Strategic Plan performance measures and the ASP occurrence rate trending for the annual Performance and Accountability Report to Congress.
Oversight	Risk-informed Decision-Making	Improve NRR risk-informed decision making	NRR Office Instruction for emergent issues Training on use of risk in decision making	Revise LIC-504, "Integrated Risk-Informed Decision Making Process for Emergent Issues," to incorporate feedback from pilot application Develop course on modeling assumptions and uncertainty of risk models for technical reviewers. Develop course on uncertainties in risk-informed decision making for managers.
Oversight	Maintenance of PRA Infrastructure	Logic Model Development SAPHIRE Code	Develop SPAR models for each unique plant-specific design, as applicable; maintain models to support user needs Maintain SAPHIRE code and GEM interface to support user needs and new methods	Develop Level 1 Rev. 3 SPAR Models Develop External Event SPAR Models Develop Low Power / Shutdown Models Develop Level 2/LERF Models Develop the SAPHIRE and GEM Interface and maintain them
Oversight	Maintenance of PRA Infrastructure	Technical Guidance Technical Support	Provide guidelines for analysis of events; maintain guidelines in support of revised methods and user needs Maintain analysis methods to support user needs; provide on-call technical assistance to senior reactor analysts and NRR	Provide integrated handbook for the analysis of internal, external, and low power/shutdown events, LERF, and Level 2 Provide revised methods and write tutorials for estimating CCF, equipment unavailability, independent failure probability, and initiating event frequency Provide event-specific methods and SPAR model modifications (MD 8.3, ROP, ASP) Provide SDP analysis reviews, as requested Provide support to RASP help desk (methods and models)

Table A-1. Risk-informed and performance-based projects at the NRC.

Regulatory Functional Area	Initiative	Program or Project	Project Description and Major Activities	Major Project Activities
Rulemaking	Special Treatment	Risk inform 10 CFR 50.69	Develop an alternative risk-informed approach to special treatment requirements in Part 50 to vary the treatment applied to structures, systems, and components (SSCs) on the basis of their safety significance, using a risk-informed categorization method. (NRR/ADRA/DRA)	Issue final rule for new § 50.69 to allow risk-informed approach to special treatment requirements.
		Pilot Application	Industry proposing alternative approach to passive categorization aspects of 50.69.	Complete review of 50.69 implementation at 1 pilot plant.
	ECCS requirements	LOCA re-definition	Change technical requirements of 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors"	Issue final rule for revised 50.46 to redefine large LOCA
		LOCA/ LOOP	Remove requirement to consider LOOP in conjunction with large LOCA.	Complete safety evaluation of BWROG LOCA-LOOP topical report Issue final rule to remove LOCA-LOOP requirement
Rulemaking	H2 gas control	10 CFR 50.44	Change the requirements for combustible gas control.	Staff activities complete
	PTS	10 CFR 50.61a	Voluntary risk-informed alternative pressurized thermal shock limits.	Re-define Reference Transition Temperature
	Risk-informed Part 50	10 CFR 53	Determine need for separate rule to risk-inform Part 50 (ANPR RIN 3150-AH81)	Receive and evaluate public comments on the ANPR. Provide public comment summary and recommendation to the Commission (SECY)
Licensing	Risk-informed ASME Code Case	N-716	Alternative risk-informed in-service inspection methodology	Support ASME review and approval. Review two pilot plant applications.
		N-752	Alternative risk-informed repair and replacement of passive components	Support ASME review and approval.
		OMN-3	Alternative to RG 1.175 risk-informed surveillance interval for IST	Support ASME review and approval.
		N-751, 752, 753	Alternative to RG 1.178, risk-informed in-service inspection	Support ASME review and approval.
	Topical Reports	WCAP-16168	Risk-informed extension of reactor vessel weld inspection from ten to twenty years	Review and approve topical.
		EPRI TR-1009325 rev. 1	Risk-informed extension – permanent 15-year ILRT extension	Review and approve topical.
Licensing	Risk-related Regulatory Guides	RG 1.200	An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities	Issue Revision 1 endorsing ASME Standard on at power, internal events, Level 1 and LERF PRA. Issue draft to Revision 2 endorsing PRA standards on external events, internal fires and low power/shut down.
		RG 1.201	Guidelines for Categorizing SSCs in NPPs According to Their Safety Significance	
	Risk-related Standard Review Plan Sections	Section 19.0	Probabilistic Risk Assessment and Severe Accident Evaluation.	New SRP section to address COL and Design Certification.
		Section 19.1	Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities	Update to incorporate Revision 1 to RG 1.200, which adopts ASME PRA Standard Addendum B.

Table A-1. Risk-informed and performance-based projects at the NRC.

Regulatory Functional Area	Initiative	Program or Project	Project Description and Major Activities	Major Project Activities
		Section 19.2	Review of Risk-Information used to Support Permanent Plant-Specific Changes to the Licensing Basis: General Guidelines.	Revise and update. (Re-numbered from original SRP Chapter 19.)
Licensing	Risk-Informing the Standard Review Plan (SRP)		Develop a reviewer's "desk guide" for NRO technical staff to apply risk insights to the review of new reactor license applications for those areas of the SRP that are amenable to being risk-informed. Specific objectives include: • Ensure effective review, identifying any non-conforming aspects or other issues that would be inimical to public health and safety. • Facilitate efficient review using a graded approach, in which the level of resources applied to a given review area is commensurate with the importance to assuring public health and safety.	Form technical team to identify possible approaches to risk-inform the SRP to enhance new reactor review efficiency; obtain management approval of selected approach Identify SRP sections amenable to being risk-informed and develop a template to transmit risk insights for these sections Develop samples based on AP1000 design and present to management Develop guidance document for transfer of plant-specific PRA information on SRP sections. Develop and conduct training for staff who will review new reactor PRA submittals and contribute risk information to the desk guide Conduct training for staff who will use the risk insights in the desk guide Provide risk insights for each reactor type as they become available
Licensing	RI-Tech Specs	Develop risk-informed improvements to the standard technical specifications (STS).	Initiative 1	Define the preferred end state for technical specification actions (usually hot shutdown for PWRs).
			Initiative 2	Increase the time allowed to delay entering required actions when surveillance is missed.
			Initiative 3	Modify the existing mode restraint logic to allow greater flexibility (i.e., use risk assessments for entry into higher mode limiting conditions for operation (LCOs) based on low risk).
			Initiative 4b	Modify the current system of fixed completion times to allow reliance on a configuration risk management program (CRMP) to determine risk-informed completion times
			Initiative 5	Optimize surveillance frequencies
			Initiative 6	Modify LCO 3.0.3 actions to allow a risk-informed evaluation to extend operating time prior to shut down
			Initiative 7	Define actions to be taken when equipment is not operable but is still functional
			Initiative 8	Risk-inform the scope of 10 CFR 50.36.
Licensing	Fire Protection	NFPA 805 Support	Fire protection for operating nuclear power plants Pilot Application Circuit Analysis	National Fire Protection Association Standard NFPA 805 Rule and Regulatory Guide 1.205. Review NFPA-805 implementation at 2 pilot plants. Post-Fire Safe-Shutdown Circuit Analysis Resolution Program.
Licensing, Rulemaking, Oversight	Phased approach to PRA quality	PRA Standards	Develop standards and related guidance for appropriate PRA quality and the application of risk-informed, performance-based regulation in conjunction with national standards committees and industry organizations.	Develop at power, internal events, Level 1 and LERF PRA standard (ASME). Develop external events PRA standard (ANS). Develop internal fire PRA standard (ANS). Develop low power/shutdown PRA standard (ANS).
		RG 1.200	Provide guidance in 4 areas: (1) technically acceptable PRA; (2) NRC position on consensus standards and related industry guidance; (3) demonstration that PRA	Issue Revision 1 endorsing ASME Standard on at power, internal events, Level 1 and LERF PRA. Issue draft to Revision 2 endorsing PRA standards on external events, internal fires and low power/shut down.

68

Table A-1. Risk-informed and performance-based projects at the NRC.

Regulatory Functional Area	Initiative	Program or Project	Project Description and Major Activities	Major Project Activities
			used in regulatory application is of sufficient technical adequacy; and (4) documentation to support regulatory submittal	
		Prioritization	Encourage industry to shift towards phases 2 and 3 of the phased approach to PRA quality	Develop a prioritization system for license amendments based on the phased approach to PRA quality. Implement prioritization system for license amendment requests.
Licensing, Rulemaking, Oversight	Digital Systems PRA	Develop short term guidance on how to use risk-insights to assist in the resolution of key digital system issues	Develop short term guidance how to use risk-insights to assist in the resolution of key digital system issues	Issue a Regulatory Information Summary (RIS) that provides interim guidance, and acceptance criteria for licensing reviews of digital systems in operating reactors Issue licensing guidance and acceptance criteria (Regulatory Guide or other appropriate guidance) and update Standard Review Plan (SRP)
		Risk-inform digital systems reviews	Develop guidance for incorporation of risk-inform decision making in licensing reviews of digital systems for current and future reactors	Complete research to identify or develop acceptable modeling methods, assess failure data, determine criteria for level of modeling detail, assess uncertainties and determine how to interface digital system models with the rest of the PRA, to support risk-informed decision making for digital systems. Issue NUREG/CR's to provide needed technical bases Issue Regulatory Guide on Risk-Informed decision making review methods applicable to digital I&C systems Update NRC PRA data, models and tools to support NRC assessment of digital system risk and reliability Update Standard Review Plan (SRP) and other NRC guidance (RG 1.200, etc.)
Licensing, Rulemaking, Oversight	Risk-Informed Environment		Broaden staff's knowledge and acceptance of risk in day-to-day activities. Specific objectives include: • Improve individual employee priority on risk-informed regulation • Improve perception of risk-informed regulation's contribution to regulatory effectiveness • Increase management attention to processes, tools, and training that enable implementation of risk-informed regulation	Add units on risk-informed regulation to office qualification plans Increase risk knowledge among first-line supervisors through position criteria and training Provide formal training on risk-informed regulation to all NRR and NRO technical staff Develop informal web-based training on risk-informed regulation Create a web-based forum of expertise for knowledge transfer
Licensing, Rulemaking, Oversight	External Communications on PRA		Communicate the purpose and use of PRAs in NRC's reactor regulatory program more transparently to the public and stakeholders.	Update fact sheets on probabilistic risk assessment and nuclear reactor risk Redesign risk-related pages on the NRC public website Develop a brochure on risk-informed regulation Organize a broad-scope public meeting on risk-informed activities (if needed)

Table A-1. Risk-informed and performance-based projects at the NRC.

Regulatory Functional Area	Initiative	Program or Project	Project Description and Major Activities	Major Project Activities
Rulemaking		Part 40 Jurisdictional Working Group	Develop an approach to more clearly specify NRC's authority over source material to uranium and thorium that is extracted and/or purposely concentrated for the use of uranium and thorium.	Provide Recommendations/ Legislative Package to Commission
Rulemaking		Exemptions from licensing, general licenses, and distribution of byproduct material	Systematic re-evaluation of exemptions from licensing in 10 CFR Parts 30 and 40	Final Rule 1 Proposed Rule 2
Licensing, Rulemaking, Oversight	Developing a framework for incorporating risk information in the NMSS regulatory process	Update Risk-Informed Decision-Making guidance document	Develop an approach to more clearly specify NRC's authority over source material to uranium and thorium that is extracted and/or purposely concentrated for the use of uranium and thorium.	
Licensing, Oversight	Implementation of Part 70 Revision	10CFR70 Interim Staff Guidance Development Review Integrated Safety Analyses (ISA) for existing facilities	Develop guidance to address issues encountered in implementing Subpart H (Integrated Safety Analysis). Through interaction with licensees address remaining ISA review issues.	
		Revise Inspection Procedures for Part 70	Risk-informed review procedures consistent with Subpart H	
Licensing, Oversight	Incorporate Risk Information into the High Level Waste Regulatory Framework	Pre and Post Closure key technical issue resolution	Risk-Inform Pre and Post Closure key technical issue resolution	
		Model Abstraction Review Team Strategies	Develop strategies using risk insights.	
		Total System Performance Assessment, TPA 5.1	Develop TPA code version 5.1	
Licensing, Oversight	Risk-Informing Division of Spent Fuel Storage and Transportation Standard Review Plans for Storage and Incorporating Interim Staff Review Guidance-Purpose to save staff resources	Application of selected risk Methodology to revised storage SRP chapters	Proposed 3 methods, trial application on two SRP chapters, resulting in selection of methodology	
		Application of selected risk Methodology to revised storage SRP chapters	Combined efforts of NRC Staff and contractor to risk inform specific SRP chapters	

70

Table A-1. Risk-informed and performance-based projects at the NRC.

Regulatory Functional Area	Initiative	Program or Project	Project Description and Major Activities	Major Project Activities
Licensing, Rulemaking	Probabilistic risk assessment of dry cask storage systems	Pilot PRA of dry cask storage facility	A pilot PRA of one specific dry cask storage facility was performed.	

Table A-2 list the activities presented in the October, 2006, Risk-Informed Regulation Implementation Plan [17]. The activities are divided by those that are related to the NRC's safety strategic plan goal and the effectiveness strategic plan goal. Activities supporting safety or effectiveness goals may substantially differ in scope, form, and content because the nature of the activities being regulated varies greatly, as does the availability of risk assessment methods.

Table A-2 Risk-Informed Regulation Implementation Plan listed activities.

Activity Number	Activity Description
Safety Initiatives and Activities	
SA-1	Maintain a risk-informed assessment process for determining NRC actions based upon performance indicator and inspection information
SA-2	Reactor Oversight Process (ROP) support (renamed EF-20)
SA-3	Industry Trends Program support
SA-4	Reactor Performance Data Collection Program
SA-5	Accident Sequence Precursor (ASP) Program
SA-6	SPAR Model Development Program (renamed EF-21
SA-7	Incorporate risk information into the high-level waste regulatory framework
SA-8	Change technical requirements of 10 CFR 50.46 (renamed EF-22)
SA-9	Digital systems probabilistic risk assessment (PRA)
SA-10	Develop risk-informed improvements to standard technical specifications
SA-11	Fire protection for nuclear power plants
SA-12	Incorporate risk information into the decommissioning regulatory framework.
SA-13	Develop improved methods for calculating risk in support of risk-informed regulatory decision making
SA-14	Evaluation of loss-of-offsite-power events and station blackout risk
SA-15	Exemptions from licensing and distribution of byproduct material: licensing and reporting requirements
SA-16	Materials licensing guidance consolidation and revision
SA-17	Implementation of Part 70 revision
SA-18	Assessing performance of steam generator tubes and other reactor coolant system (RCS) components during severe accidents (formerly EF-5)
SA-19	Risk-Informing the Standard Review Plan (SRP) – Improving new reactor review efficiency through application of risk insights
Effectiveness Initiatives and Activities	
EF-1	Creating a risk-informed environment
EF-2	Develop standards and related guidance for appropriate PRA quality and the application of risk-informed, performance-based regulation in conjunction with

Table A-2 Risk-Informed Regulation Implementation Plan listed activities.

Activity Number	Activity Description
	national standards committees and industry organizations
EF-3	Develop and maintain analytical tools for staff risk applications
EF-4	Develop the technical basis to revise the PTS rule
EF-5	Develop methods for assessing steam generator performance during severe accidents (renamed SA-18)
EF-6	Develop structure for new plant licensing (advanced reactor framework)
EF-7	Develop and apply methods for assessing fire safety in nuclear facilities
EF-8	Coherence program
EF-9	Establish guidance for risk-informed regulation: development of human reliability analysis
EF-10	PRA review of advanced reactor applications
EF-11	Developing a framework for incorporating risk information in the NMSS regulatory process
EF-12	Develop risk guidelines for the materials and waste arenas
EF-13	Systematic decision making process development
EF-14	Probabilistic risk assessment of dry cask storage systems
EF-15	Interagency Jurisdictional Working Group evaluation of the regulation of low-level source material or materials containing less than 0.05 percent by weight concentration uranium and/or thorium
EF-16	Multiphase review of the byproduct materials program(implementation of Phase I and Phase II recommendations)
EF-17	Revise Part 36: Requirements for Panoramic Irradiators (PRM-36-01)
EF-18	Develop an alternative risk-informed approach to special treatment requirements in Part 50 to vary the treatment applied to structures, systems, and components (SSC) on the basis of their safety significance using a risk-informed categorization method
EF-19	Develop a plan for making a risk-informed, performance-based revision to 10 CFR 50 (Part 50)
EF-20	Reactor Oversight Process (ROP) support (formerly SA-2)
EF-21	SPAR Model Development Program
EF-22	Change technical requirements of 10 CFR 50.46 (formerly SA-8)
EF-23	Risk-informing of Standard Review Plans for independent spent fuel storage installations and packages