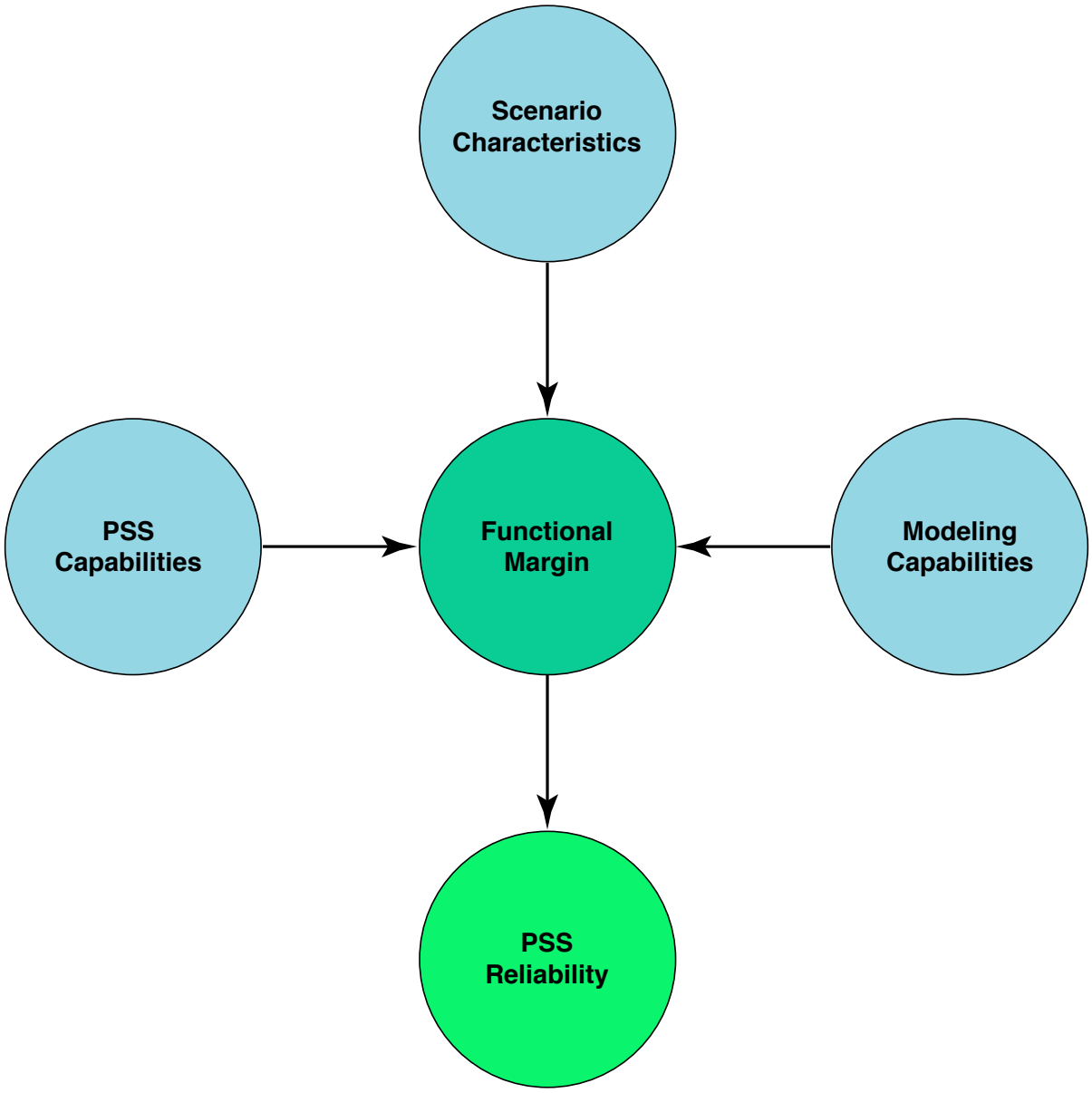
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Program on Technology Innovation: Probabilistic Risk Assessment Requirements for Passive Safety Systems



Program on Technology Innovation: Probabilistic Risk Assessment Requirements for Passive Safety Systems

1015101

Final Report, December 2007

EPRI Project Manager
S. Hess

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

ERIN Engineering and Research, Inc.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

CITATIONS

This report was prepared by

ERIN Engineering and Research, Inc.
1210 Ward Avenue, Suite 100
West Chester, PA 19380

Principal Investigator
E. Thornsbury

This report describes research sponsored by the Electric Power Research Institute (EPRI).

The report is a corporate document that should be cited in the literature in the following manner:

Program on Technology Innovation: Probabilistic Risk Assessment Requirements for Passive Safety Systems. EPRI, Palo Alto, CA: 2007. 1015101.

PRODUCT DESCRIPTION

A key feature of the next generation of nuclear power reactors is a reliance on safety systems that are passive, that is, those that rely on natural physical laws and require minimal or no intervention by plant operators. These features are intended to significantly reduce the potential for serious events while simultaneously minimizing facility life-cycle costs. In addition to these features, these reactors will be licensed within a framework that will be risk-informed and performance-based. Because probabilistic risk assessments (PRAs) of passive safety systems (PSSs) will serve as a cornerstone requirement for the licensing of advanced nuclear generating plants, this research serves as an initial step toward characterizing the issues and specifying the necessary research and development program to address them.

Results and Findings

This research provides a characterization of issues associated with PRAs of PSSs. The outcome of this initial research provides a comprehensive plan to address these issues and support the efficient licensing of reactor designs that incorporate passive safety features.

Challenges and Objectives

Safety evaluations associated with advanced nuclear designs have focused predominantly on deterministic evaluations. For many of the systems that incorporate passive safety features, PRAs have not been performed, or, for those that have, insufficient data are available to support obtaining general conclusions. Additionally, instances have occurred in which deviations from anticipated operation have occurred for passive-type systems. This research characterizes and prioritizes these issues. From this characterization, a proposed research program was developed to address the identified issues.

Applications, Value, and Use

This research provides a necessary element to support the deployment of advanced nuclear power technology. Because advanced nuclear plants rely on safety systems that are passive in nature, the capability to perform an accurate evaluation of their impact on nuclear safety risk will be a necessary condition to support the licensing and operation of these plants.

EPRI Perspective

The deployment of advanced nuclear-generating technology is a critical element of ensuring a sustainable, cost-competitive energy source. Because nuclear power does not emit greenhouse gasses, its expanded use is also a necessary component to address potential climate-change issues. Because advanced nuclear technologies employ passive safety features as a key strategy to prevent and mitigate adverse events, it is essential that an adequate analytical framework exists to assess the impact of these systems on nuclear safety risk. The research described in this

report provides a necessary characterization of the issues associated with the PRA of passive safety systems. From this characterization, a proposed research program that will support the timely licensing of the next generation of nuclear plants was developed.

Approach

In this project, the research literature was surveyed to obtain a comprehensive identification and characterization of issues associated with the reliability of passive safety systems. From this characterization, a comprehensive research program was proposed to resolve the identified issues.

Keywords

Passive safety systems
Thermal hydraulic analysis
Probabilistic risk assessment

ACRONYMS

ABWR	Advanced boiling water reactor
ACRS	Advisory committee on reactor safeguards
ADS	Automatic depressurization system
AHP	Analytical hierarchy process
APEX	Advanced plant experiment
APWR	U.S. advanced pressurized water reactor
BiMAC	Base-internal melt arrest and coolability
BWR	Boiling water reactor
CCC	Containment cooling condenser
CEA	Commissariat à l'Energie Atomique (French Atomic Energy Commission)
CFD	Computational fluid dynamics
CMT	Core makeup tank
EHRS	Emergency heat removal system
ENEA	Ente per le Nuove tecnologie, l'Energia e l'Ambiente (Italian National Agency for New Technologies, Energy, and the Environment)
EPR	U.S. evolutionary power reactor
ESBWR	Economic simplified boiling water reactor
FMEA	Failure modes and effects analysis
GDCS	Gravity-driven cooling system
GE	General Electric
HAZOP	Hazard and operability analysis
IAEA	International Atomic Energy Agency
ICS	Isolation condenser system
LOCA	Loss of coolant accident

MIT	Massachusetts Institute of Technology
NEA	Nuclear Energy Agency
NRC	U.S. Nuclear Regulatory Commission
OECD	Organization for Economic Co-operation and Development
PBL	Pressure balance line
PCCS	Passive containment cooling system
PHR	Passive heat removal
PRA	Probabilistic risk assessment
PRHR	Passive residual heat removal
PSS	Passive safety system
PWR	Pressurized water reactor
REPAS	Reliability evaluation of passive systems
RMPS	Reliability methods for passive systems
RPV	Reactor pressure vessel
TH	Thermal-hydraulic

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Purpose and Objectives

A key feature of the next generation of nuclear power reactors is a reliance on safety systems that are passively actuated and/or powered. This is in contrast to many of the safety systems in current nuclear power plants that rely on electrical or pneumatic support systems. With the increasing use of probabilistic risk assessment (PRA) in the operation and regulation of nuclear power plants, this fact raises the issue of the PRA requirements for these passive safety systems (PSSs).

For many plant designs or systems that incorporate passive safety features, insufficient data are available to support detailed quantitative conclusions regarding the reliability of passive safety systems. Additionally, the limited operating, testing, and experimental experience includes instances in which deviations from anticipated operation have occurred for some existing passive-type systems. Operating experience provides examples of foreign material obstructions as described in "Inherent Failure Modes of Passive Safety Systems" [1], failure of control rods to fall under gravity as described in "Screening of Probabilistic Safety Evaluations for Different Advanced Reactor Concepts" [2], breakage of natural circulation as a result of stratification, also in reference [2], and various latent human errors that disable or degrade nuclear systems, as described in *Review of Findings for Human Error Contribution to Risk in Operating Events* [3]. Such occurrences affect both active and passive safety systems but particularly contribute to increased uncertainty regarding the level of reliability for passive safety systems.

This report serves as an initial step toward characterizing the issues and limitations that currently exist in the application of PRA technologies to the evaluation of the reliability of passive safety systems and recommends a research and development (R&D) program to address these issues and limitations. The goal of this research is to identify and evaluate the issues and to consider the implications to both near-term advanced light-water reactors that fall under 10CFR52 and Generation IV reactors that may fall under future and possibly different regulatory regimes.

The conclusion of this report specifies a proposed research plan and schedule to address any identified deficiencies in the capabilities of current tools and methods for performing PRAs on PSSs.

Background

In the past several years, researchers have placed increased attention on the issues and techniques associated with PSS reliability. Several recent technical papers, including "Screening of

Probabilistic Safety Evaluations for Different Advanced Reactor Concepts" [2] and "State of the Art in Reliability of Thermal-Hydraulic Passive Systems" [4], provide a high-level discussion of the need for research on this subject.

A common belief related to advanced nuclear power plant designs is that reliance on passive safety systems will result in several advantages. Among these advantages are lower operating costs and a lower risk of severe accidents. Yet, the reliability-engineering community has made relatively little effort to understand the qualitative and quantitative reliability of these systems. As a result of this discrepancy, engineers and decision makers need methods with a strong basis to assess, classify, model, and evaluate PSS reliability, particularly with regard to the incorporation of PSS reliability into a plant's PRA.

Characteristics of Passive Safety System Reliability

In contrast to active systems, passive systems rely on naturally occurring forces such as gravity or pressure differential to perform their function. Although such an approach reduces a system's dependence on support systems, it can introduce other complications into the assessment of system reliability. In general, the driving forces for passive systems are lower relative to those for similar active systems. The value of these driving forces is also subject to more variation as a result of deviations in the details of an accident sequence. With lower driving forces and greater sensitivity to small variations, counter-forces such as friction that are normally negligible for active systems may have a significant impact on system operation and, thus, may need to be considered in an assessment of passive-system performance and reliability.

In practice, most passive systems are not entirely passive. Particularly for advanced light-water reactor designs, the passive systems may require some type of actuation signal and the physical movement of one or more active, powered components (for example, valves) in order to initiate the safety function. Some passive safety systems may also include active, non-powered components (for example, check valves) whose failure could impair or fail the system function.

This study uses four elements to capture these issues and characterize the important contributors to PSS reliability:

1. System capabilities – The design, features, and capacities of the passive safety system. System capabilities include consideration of associated uncertainties, experienced and postulated degradation mechanisms, the physical reliability of components, and potential failure modes of the system.
2. Scenario characteristics – The details of each scenario in which the PSS must function, including operation or failure of other systems and the definition of success for the PSS. Scenario characteristics can affect the performance of the PSS and/or modify the success criterion for the safety function.
3. Modeling capabilities – The quality of understanding of the system capabilities of the PSS and of the physical (for example, thermal-hydraulic [TH]) phenomena that govern system operation and success/failure. Additionally, limitations in operational data may increase the uncertainty of the estimation of the amount of functional margin.

4. Functional margin – The degree to which there is an opportunity for system capabilities to degrade to a point where the safety function will fail. Functional margin represents the difference between the actual system operation during an accident scenario and the minimum operation that is required to achieve the safety function.

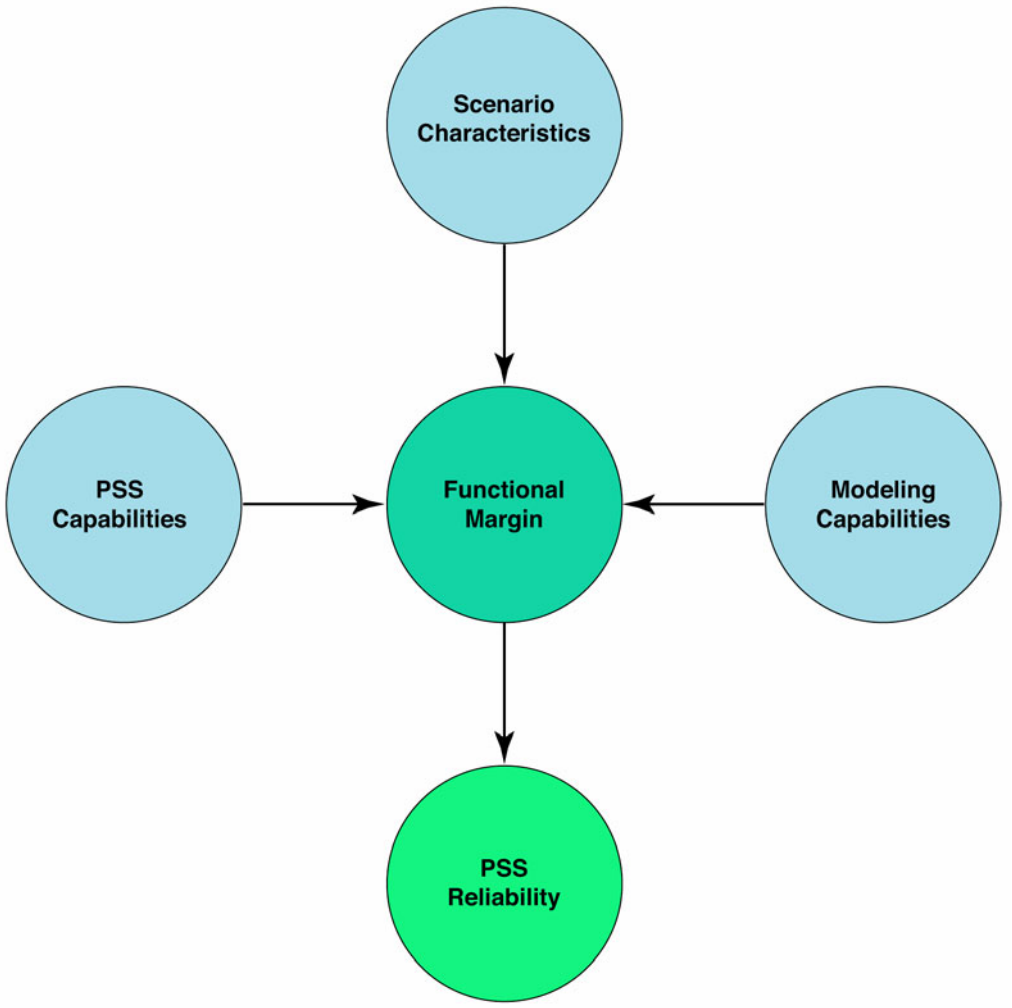


Figure 1-1
Characteristics of PSS Reliability

The combination of these factors contributes to the reliability of the passive safety system, as shown schematically in Figure 1-1. It is important to recognize that the reliability of the PSS may vary among different accident scenarios. Although this can be true of active systems as well, their reliability more often depends on the operation of equipment rather than the physical characteristics and TH details of each accident scenario. For example, an active safety-injection system with a centrifugal pump may have uncertainties regarding the ability to model the system and the specific scenario characteristics. However, the system's pumping capabilities typically are well above the required capabilities. This results in a relatively large functional margin and a negligible contribution by these uncertainties to the likelihood of failure of the system. Conversely, a PSS with relatively lower capabilities will significantly reduce the available

functional margin. The uncertainties in these elements may dominate the reliability of such a passive system.

International Efforts

The International Atomic Energy Agency (IAEA) has divided passive systems into four categories, as described in *Safety Related Terms for Advanced Nuclear Plants* [5]:

Category A. Physical barriers and static structures (for example, pipe walls or concrete buildings)

Category B. Moving working fluids (for example, cooling by free convection)

Category C. Moving mechanical parts (for example, check valves)

Category D. External signals and stored energy (passive execution/active actuation, for example, scram systems)

For Category A systems, structural-reliability analysis methods can estimate reliability through the application of the principles of probabilistic structural mechanics theory. For Category C and D equipment, operating experience data can provide the basis for the reliability calculation. However, there is so far no agreed approach regarding Category B Passive Systems, as described in "State of the Art in Reliability of Thermal-Hydraulic Passive Systems" [4]. Therefore, this report is principally concerned with phenomena associated with IAEA Category B Passive Systems (moving working fluids) and their incorporation into nuclear plant PRA models. It also addresses Categories A, C, and D, but assessment of their reliability is better understood and less controversial.

In 2002, the Organization for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) sponsored an international workshop on the challenges associated with PSS reliability. The proceedings of this *International Workshop, Hosted by the Commissariat à l'Energie Atomique (CEA)* [6], highlight some of the challenges associated with PSS-reliability scope and modeling, along with some preliminary techniques developed primarily by the European nuclear community.

Several issues arose during the meeting:

- Participants generally agreed upon the definition of a passive system and the classification of passive systems, but they noted the need for a clearer differentiation among the types of passive systems. This may be particularly applicable to near-term advanced light-water reactors, where an active component or components may actuate the passive safety system. In practice, it is not always straightforward to classify passive systems.
- The role of human actions in passive systems may be very low. In an assessment of passive system reliability, it will be necessary to clearly define the role of operators. The use of passive systems may also reduce the level of maintenance and, therefore, reduce the number of latent failures as a result of maintenance errors. However, proper maintenance may become more important in ensuring the operability of a passive system, though in-service testing may be more difficult or impossible.

- There is a clear need for more data on passive-system performance, especially related to THs.
- Understanding the safety functions for both active and passive systems and defining the correct success criteria are critical elements for determining reliability.
- The common perception that passive safety systems will be less expensive than active safety systems may not necessarily be true.
- The inherent failure modes of passive systems should include consideration of failures as a result of unexpected changes in the physical state of the system and failures as a result of changes in the environment surrounding the systems, such as through the introduction of foreign material.
- Issues specifically identified for TH passive systems include definition of failure modes, coverage of all situations, modeling of extreme conditions, model completeness, and data support for quantification.

One paper from the workshop, "Inherent Failure Modes of Passive Safety Systems" [1], provides an excellent overview of the general issue of the reliability of passive safety systems. Its key points are as follows:

- Passive systems are less susceptible to component failures than are active systems. Instead, they are subject to "inherent failures" caused by one of two types of difficulties. The first type is an unexpected change in the internal physical state, such as a result of stratification. The second type is an unexpected change in the system environment, such as the plugging of heat exchanger tubes by foreign material.
- Active systems generally are not subject to inherent failures because they can essentially "power" through these phenomena.
- Because of the unique susceptibilities of passive safety systems, it is essential to design them so that operators can monitor the system condition through in-service inspection and testing. To illustrate this need, the authors cite cases where operators found large amounts of debris in suppression pools and in a standby liquid-control tank.

In this paper, the authors provide a demonstration calculation using the RELAP computer code to simulate the system response to foreign material by parametrically varying the degree of blockage in the inlet to a containment cooling condenser (CCC). These results can then inform a safety assessment of the CCC. The paper also mentions an example of the first type of failure. In this case, a steam jet enters the pressure-balance line of a core makeup tank (CMT) with such vigor that it disrupts the insulating layer of warm liquid that normally exists on top of the pool. The steam can then condense in the water, raising the pool temperature. The authors state that the increase in water temperature will significantly reduce the driving head for water flow into the primary system. The implication of this example is that analysts and designers must be aware of key assumptions on which the operation of a passive safety system depends, especially when violation of these assumptions may not be readily detectable by the usual system-level codes used to study their operation.

The authors also point out that proper operation of some passive systems, such as a passive-containment cooling system, requires a good design and successful operation of the whole

containment system because the operation of the heat exchanger is sensitive to the distribution and transport of noncondensible gases. This also implies that a proper analysis would necessarily include the entire containment (including the effects as a result of its structural members). The final point they make is that, unlike active safety systems, passive systems are prone to degrade without becoming completely inoperative. This might make it more difficult to define suitable success criteria.

Since the workshop, some of the techniques have developed into more refined approaches. Section 2 of this report reviews these approaches.

Domestic Efforts

R&D in the United States on the reliability of passive safety systems has not been as active. A few published papers from the Massachusetts Institute of Technology (MIT) have demonstrated their development of approaches to the issue. Their technique has examined TH uncertainties in passive cooling systems for Generation IV-type gas-cooled reactors. Section 2 of this report reviews this work in more detail.

The other source of information regarding PSS reliability in the United States comes from activities at the U.S. Nuclear Regulatory Commission (NRC). During design-certification reviews for plants that incorporate passive safety systems such as the Westinghouse AP1000 and General Electric (GE) Economic Simplified Boiling Water Reactor (ESBWR), NRC reached conclusions regarding the modeling of these passive safety systems in the PRA. Section 2 of this report also reviews these approaches.

Regulatory Concerns

R&D can encompass a broad range of activities. For an R&D plan on a challenging topic such as this, it is important to maintain a proper focus. Many issues related to PSS reliability will be scientifically interesting and could become topics of research. However, the purpose of this EPRI-sponsored research will focus on the current regulatory environment.

Advanced Light-Water Reactors

The issue of passive safety-system reliability will be an important one for contemporary advanced light-water reactor designs with passive safety systems. Because the results of the overall PRA are useful both during the licensing process and for ongoing regulation of the plant, the PRA must have a sound technical basis. The prevalence of passive safety systems in many of the advanced light-water reactor designs amplifies the importance of PRA requirements for PSS reliability.

During the design-certification phase, the NRC reviews and eventually approves a reactor design based on largely deterministic arguments. Although the NRC requires that a PRA and its results provide useful insights, the regulatory requirements are still primarily deterministic. Of the expected advanced light-water reactor designs with passive safety systems, only the AP1000 has

completed design certification at the time of this report. Section 2 of this report discusses the lessons learned during the review of the AP1000 regarding PSS reliability.

The ESBWR design also contains several passive safety systems and is currently undergoing design certification review by the NRC. Several utilities plan to submit combined license applications using this design. Utilities also plan to submit applications for the GE Advanced Boiling Water Reactor (ABWR), Areva US Evolutionary Power Reactor (EPR), and Mitsubishi US Advanced Pressurized Water Reactor (US-APWR), though these designs do not rely on passive systems.

A draft IAEA report, *Description of Natural Circulation and Passive Safety Systems in Water Cooled Nuclear Power Plants* [7], provides a good overview of passive safety systems in new power plant designs. Table 1-1 lists the key passive systems and related components in plant designs that are under consideration for construction in the near future in the United States.

Table 1-1
Passive Systems in New Plant Designs

Plant Design	Key Passive Systems and Related Components
AP1000	Passive residual heat-removal system Core make-up tanks (2) Four-stage automatic depressurization system Accumulators (2) In-containment refueling water storage tank Lower containment sump recirculation Passive-containment cooling system
ESBWR	Gravity-driven core cooling system Automatic depressurization system Isolation condenser system Passive-containment cooling system Basemat-internal melt arrest and coolability device
APWR	Natural circulation of primary system to steam generators Advanced accumulators Passive autocatalytic recombiner
ABWR	Inert containment Suppression pool Containment overpressure protection
EPR	Passive autocatalytic recombiner Core melt retention system

Longer Term Generation IV Concerns

For Generation IV plant designs, the regulatory concerns are slightly different. First, a new regulatory regime is under development that may introduce a more risk-informed, or even risk-based, licensing and regulatory process. Some of these more advanced plant designs may include even more reliance on passive safety systems or features than the near-term advanced light-water reactor designs. Their accident mitigation strategies may also be significantly different from those used for light-water reactors.

High-temperature, gas-cooled reactors have received much of the attention for Generation IV plants. As a result of the use of gas-phase coolant (for example, helium) in these reactor designs, the operating and functional margins may be much smaller than those for liquid-cooled reactors. This creates two types of problems. First, the knowledge base for the behavior of gases as a reactor coolant is significantly smaller than for water-cooled reactors. Second, circulating gas systems tend to show greater susceptibility to TH variations that might cause them to fail their safety function. For these reasons, PSS reliability methods for Generation IV plants may require a more detailed approach than for the current generation of advanced light-water reactor designs. Because both the designs of Generation IV plants and their regulatory framework are in the early stages, these issues will require further investigation. Although this report briefly discusses these challenges, the focus of most of this report is on the issues related to near-term advanced light-water reactor designs.

2
STATE-OF-THE-ART MODELING TECHNIQUES

The purpose of this task is to review the current literature and describe the proposed methods from both domestic research and international activities.

Literature and Model Review

Current literature provides evidence of two primary research efforts. The first centers on a group of European researchers and their efforts to develop an approach to estimate the reliability of passive safety systems for new, light-water reactors. MIT is leading a second effort as part of their development work for Generation IV gas-cooled reactors.

RMPS/REPAS

Based on a search of the extant literature, several European researchers are leading the development of one set of PSS reliability methods. This set of methods is evident in two related methods, the REPAS (Reliability Evaluation of Passive Systems) approach [4, 8, 9, 10] and the RMPS (Reliability Methods for Passive Systems) project [4, 10, 11, 12]. These approaches focus on the development of methods for assessing the TH issues related to passive system reliability.

The first approach, REPAS, began in 1999 under the sponsorship of ENEA (Italian National Agency for New Technologies, Energy, and the Environment) in collaboration with the University of Pisa and Polytechnic of Milano. Its purpose was to identify a method to evaluate the reliability of passive systems as a whole in a more physical and phenomenological way. The various papers developed during the REPAS project describe the approach and provide a roadmap of the evaluation process. The basic procedure consists of the following steps:

1. Characterization of operational modes (design and critical parameters)
2. Definition of failure criteria
3. Detailed code modeling
4. Deterministic evaluation (“nominal cases”)
5. Assignment of probability distributions to design and critical parameters (define run set)
6. Deterministic evaluation (“probabilistic set”)
7. Quantitative reliability estimation

Beginning in 2001, the RMPS project, funded by the European Union in the Fifth Framework Research Programme, followed on the REPAS approach in order to further develop a method to

qualitatively and quantitatively evaluate the reliability of passive systems. The development of RMPS included the application of the approach to a case study on a two-phase, natural circulation passive system. The RMPS research included CEA (French Atomic Energy Commission), European research centers, Italian universities, and industry.

The RMPS research draws parallels between reliability studies of mechanical/structural components and passive safety systems. To assess the failure probability of a mechanical or structural system, analysts use a deterministic mechanical model with a probabilistic representation of input variables to address uncertainty. Similarly, RMPS requires both deterministic and probabilistic aspects for the analysis of passive safety systems. The RMPS approach first characterizes the PSS using best-estimate TH codes. The approach combines this deterministic model with variable boundary and initial conditions in order to determine PSS reliability through a combination of uncertainty propagation and sensitivity analyses. Figure 2-1 shows this process schematically, as described in *Passive System Reliability—A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants* [6].

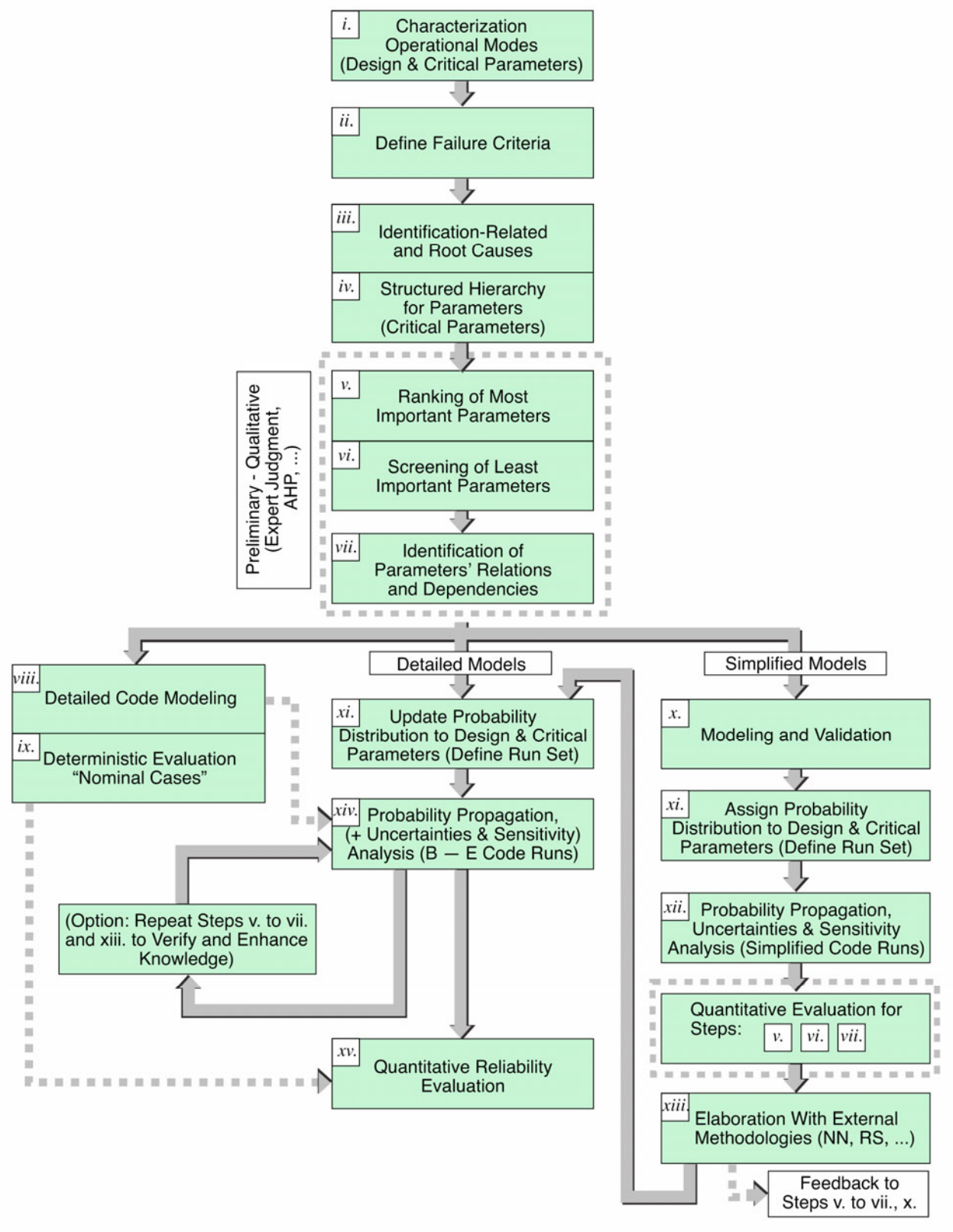


Figure 2-1
RMPS Approach [6]

Marques and colleagues applied a full example application of the process to the residual passive heat removal system for a 900-MWe pressurized water reactor (PWR), as described in "Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment" [12]. During the example application, the researchers found that assigning failure modes to the mission of the passive system could sometimes be difficult as a result of the complexity of the TH phenomena. Hazard-identification methods such as failure modes and effects analysis (FMEA) are useful, though these approaches may require the introduction of "virtual" components to capture phenomena such as natural circulation that can affect the performance of the passive system. Instead of representing a failed component, a "virtual" component would represent the functional failure of a physical phenomenon on which the PSS based its operation. For example, a "virtual" component that represents the loss of natural circulation in a cooling loop would capture the effects of this phenomenon on the performance of the passive system.

A significant concern of the study is the identification of key uncertainties and their relevant parameters. The study recognizes that the identification of the key parameters must rely upon expert judgment and uses the Analytical Hierarchy Process (AHP) to guide that activity. Another important issue identified during the project is the quantification of uncertainty. The research demonstrated that for PSS, the choice of the probability distributions can significantly affect the results of the evaluation. These distributions usually also depend upon expert judgment, particularly when there are little available data. One additional warning from the research cautions about dependence among parameters when they have common contributors to their uncertainty. For the final reliability-estimation task, the researchers discuss issues related to the complexity of the calculation and suggest approaches that use variance-reduction techniques, alternatives to Monte Carlo techniques from structural analysis, or response surface methods.

Other research related to REPAS and RMPS explores some of the individual questions needed to address the issue of passive system reliability. In one paper, "Passive System Reliability Analysis: A Study on the Isolation Condenser" [13], the author explores the higher level issue concerning the integration of PSS failure into a PRA by constructing fault trees to capture the potential failure modes of a passive safety system. Figures 2-2, 2-3, and 2-4 show the example fault tree for an isolation condenser system. The fault tree includes the failure of the PSS as a result of TH "failure" as one possible failure mode (Figure 2-4), along with more traditional component-related failure mechanisms such as valve failures and heat exchanger plugging or ruptures (Figure 2-3). The fault tree models the failure of natural circulation as a result of insufficient heat transfer to the external cooling pool, the presence of high levels of noncondensible gases, or failure of the primary pressure boundary. The fault tree then represents these TH failure mechanisms with component failures that lead to such TH failure mechanisms, such as excessive pipe fouling in a heat exchanger that results in insufficient heat transfer. Existing data sources and/or expert opinion provide the data for the basic events.

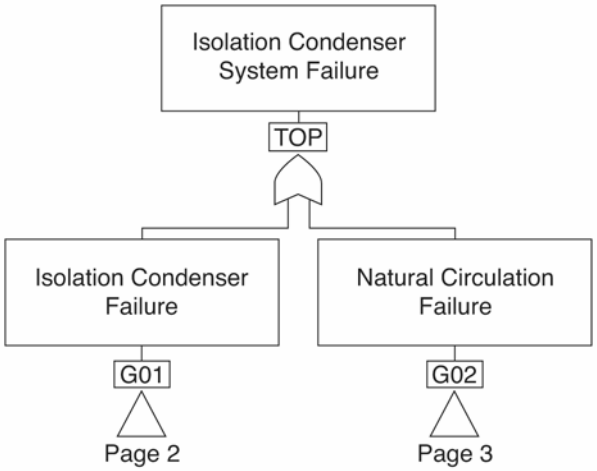


Figure 2-2
Isolation Condenser Top Gate

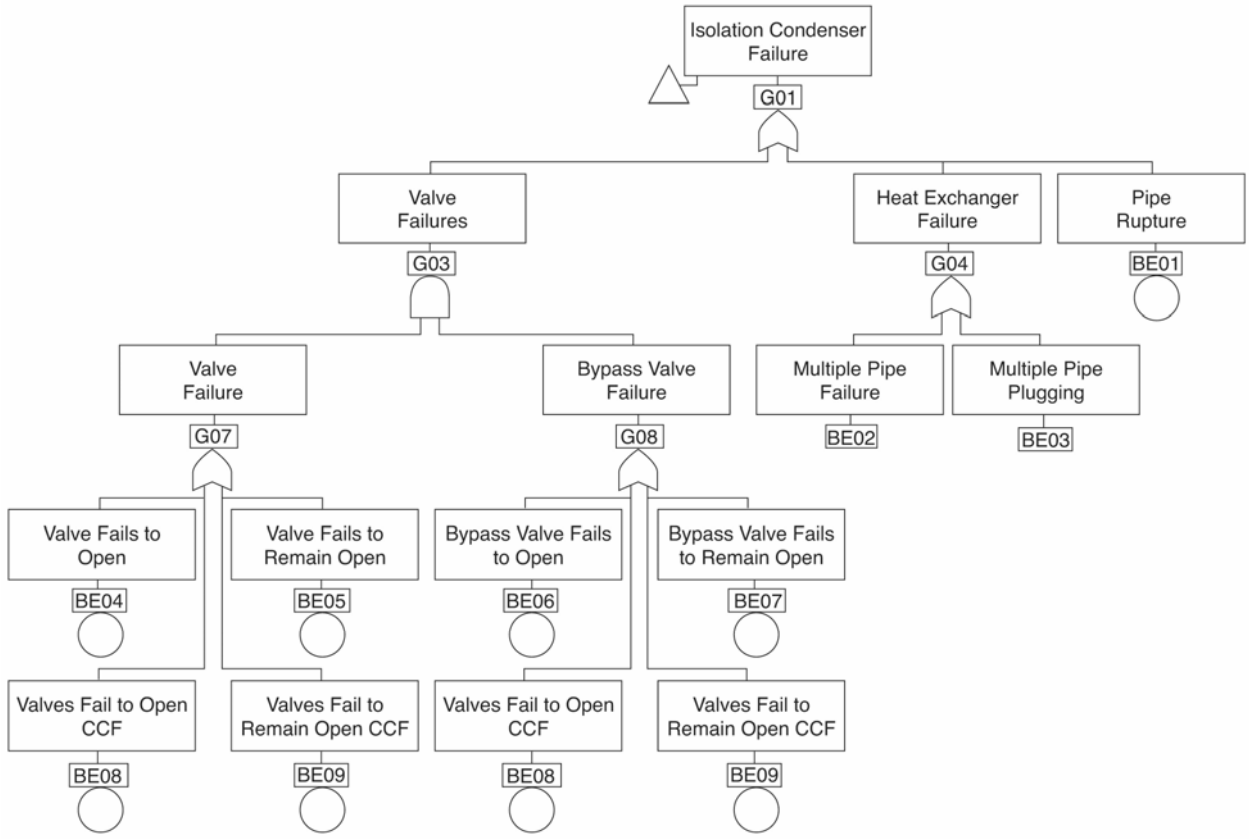


Figure 2-3
Traditional System Failures

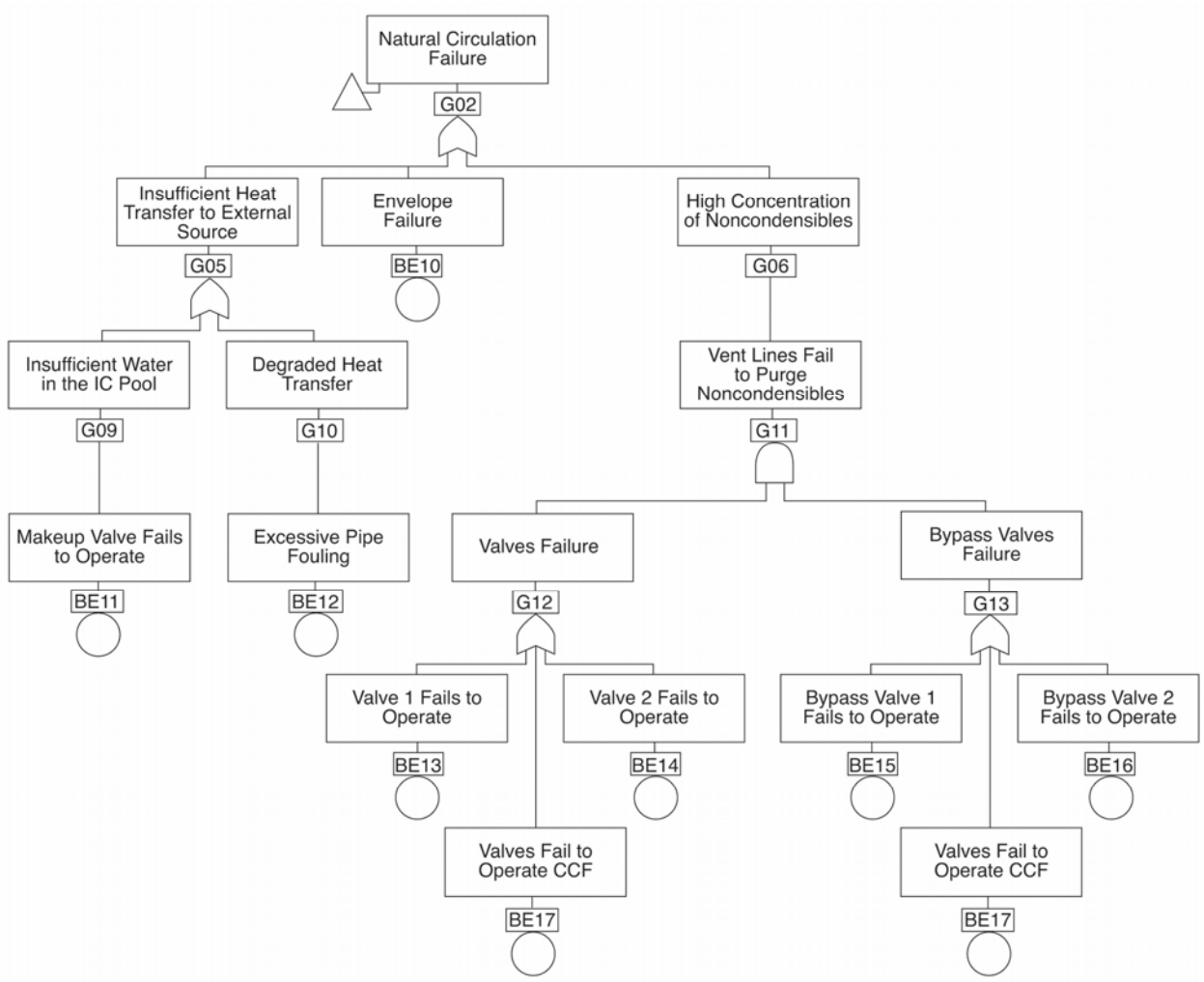


Figure 2-4
Passive System Failures

The top gate in Figure 2-2 includes failures as a result of more traditional system failures (on the left of the fault tree) and failures as a result of loss of natural circulation (on the right of the fault tree). Each of these gates expands in Figures 2-3 and 2-4 to show the failures that can cause failure of the system function. The isolation-condenser-failure half of the tree shows the types of failure mechanisms typically seen in nuclear power plant PRA, such as valve failures, common-cause failures, heat exchanger pipe ruptures, heat exchanger tube plugging, and system pipe ruptures. This tree could also include other component failures typical of current generation PRAs, such as actuation failures, support system dependencies, and operator actions.

The natural-circulation half of the fault tree decomposes the loss of natural circulation into its contributing factors. Represented in this example fault tree (see Figure 2-4) are failures as a result of insufficient heat transfer to the external cooling source, envelope failure, and a high concentration of noncondensible gases. The envelope failure event captures the likelihood of failure of the system boundary, a function that also appears in the component half of the tree as a pipe-rupture event. The failure of heat transfer to the external source could occur as a result of a

lack of sufficient water in the cooling pool due to failure of the makeup valve or as a result of degraded heat transfer due to excessive pipe fouling. The third contributor to natural-circulation failure modeled in this example is failure as a result of a high concentration of noncondensible gases. Though the system design removes these gases through vent lines, failures of these vent lines could allow noncondensible gases to accumulate and fail the function of the passive system. These failures appear in the fault tree as the appropriate valve and bypass valve failures. Operational data should be able to provide at least some failure probabilities modeled in this portion of the fault tree, such as for valve failures. However, other portions of the fault tree unique to passive systems might need to rely on expert judgment techniques. As with the traditional system fault tree, other failures such as actuation failures, support system dependencies, and operator actions could easily appear in such a tree.

In another research effort, "Evaluation of Uncertainties Related to Passive Systems Performance" [14], the author explores the issue of the identification of the key sources of uncertainty using two existing hazard-identification techniques, failure modes and effects analysis (FMEA) and hazard and operability analysis (HAZOP). Through the FMEA, the research identified factors that could disturb an example passive system (again, an isolation condenser system). These factors led to a set of critical parameters that affected the success of natural circulation in the detailed reliability analysis. The HAZOP approach examined system parameters for possible deviations from normal conditions. It then identified the consequences to the system if these parameters occur outside their design basis. The author concludes that HAZOP seems to be more suitable for PSS reliability evaluation than FMEA because it examines the functional parameters of the system rather than components. The author also concludes that future R&D should pursue the phenomenological uncertainty issues of passive systems, which are epistemic and, therefore, reducible.

Toward that end, further research explored methods to capture the epistemic uncertainty related to the physical phenomena of natural circulation systems, as described in "Addressing the Uncertainties Related to Passive System Reliability" [15]. In this case, the author used expert judgment to develop probability distributions for the critical parameters to address these uncertainties. The use of expert judgment to develop the distributions is necessary as a result of the lack of available experimental and operational data. The process addresses geometrical properties, material properties, and phenomenological uncertainties. Geometrical properties concern any differences between the as-built configuration and the analysis model, such as detailed piping arrangements. Material properties capture leakage and heat-loss uncertainties. Phenomenological uncertainties account for parameters and models that can affect the success of the natural circulation system. As an example of the parameters, the buildup of noncondensible gases in a natural circulation system is one of the most important potential causes of failure. Because the analyzed system includes vent lines to remove the noncondensibles, the fault tree models the failure of the system as a result of noncondensibles with a parameter representing failure of the vent valves. In this case, expert judgment assigned an exponential distribution to the probability of failure as a result of noncondensible gases. Other parameters in this example approach include undetected leakage, a partially closed startup valve, a heat-loss parameter, piping layout (inclination of the pipes), and plugged heat exchanger pipes. This paper concludes that the results depend directly on the expert judgment inputs to the probability distributions.

In another related research effort, as described in “The Analytical Hierarchy Process as a Systematic Approach to the Identification of Important Parameters for the Reliability Assessment of Passive Systems” [10], performed within the RMPS project “Reliability Methods for Passive Systems (RMPS) Study—Strategy and Results” [11], the research proposes the use of the analytical hierarchy process as the approach for identifying the dominant system parameters. The goal was to identify a reasonable number of relevant parameters for the analysis of PSS reliability. Because analysis of PSS reliability often makes use of expert judgment, the researchers propose and demonstrate the use of the AHP as a means to produce a credible and repeatable identification process. The AHP as applied in the referenced research project consists of three steps. The first step is the building of a hierarchy to decompose the problem. This consists of a precise definition of the top goal, followed by the building of a hierarchy of factors that influence this goal, and ending with a set of basic parameters and their interactions. The second step of the process identifies the relevance of the basic parameters through a pairwise comparison process of those parameters, either quantitatively or qualitatively. The final step uses these relevance measures to compute a priority ranking score for each parameter. The process includes contingency steps for resolving inconsistencies in the pairwise comparison. The advantage of such an approach is that it provides a structured and systematic process for the experts to evaluate the TH parameters and their relationships. In a comparison against a 2000 study of the same passive system, the authors identified several differences in the identification of key parameters, though they reconciled the differences to show that both studies capture all of the relevant factors.

An application of the REPAS approach by another set of researchers, as described in “Reliability Evaluation of a Natural Circulation System” [9] to assess and optimize the design of a passive natural circulation system, demonstrates its use. For this analysis, the identification of 29 relevant TH parameters expanded to create 137 distinct system configurations requiring TH code calculations. The calculations averaged 5 hours of computer run time, each on a modern Pentium 4 PC. The authors used expert judgment to assign probabilities for each parameter and calculate an overall TH reliability. This TH reliability represents only the failure of natural circulation as a result of TH uncertainties and does not consider actuation failures or changes in geometry or material characteristics. During the research, the authors identified four main types of parameters: system hardware parameters (for example, total length of the loop), optimal system operation parameters (for example, local pressure-drop coefficients), operating conditions (for example, initial pressure), and inadequate modeling issues (for example, nodalization). This paper also provides a good summary of the REPAS process and identifies limitations encountered by the researchers. The researchers had to limit the number of parameters in order to reduce the number of complex calculations and the significant amount of time necessary to perform them. The research concluded that a single-phase, natural-convection cooling loop would be more reliable than a two-phase loop as a result of the avoidance of instability phenomena associated with the boiling/condensing process. Shortcomings in the overall process included the need for engineering judgment at multiple steps in the process, the need to consider the uncertainty in the TH codes, the large number of calculations necessary, the need for a more complete expert judgment procedure, and the possible dependence of important input parameters.

Recent contact with one of the researchers involved in the RMPS project reveals that they are continuing their research by examining the reliability of the decay-heat-removal system for a gas-cooled fast reactor. This is a natural circulation passive system, and they expect to publish their results in early 2008.

Massachusetts Institute of Technology

The MIT research on the reliability of passive safety systems has taken a similar approach but has focused on a different set of reactor technologies. Their research has examined TH uncertainties in passive cooling systems for Generation IV gas-cooled reactors, as described in "The Impact of Uncertainties on the Performance of Passive Systems" [16] and "Incorporating Reliability Analysis into the Design of Passive Cooling System with an Application to a Gas-Cooled Reactor" [17]. Instead of post-design probabilistic risk analysis for regulatory purposes, the MIT research seeks to leverage the capabilities of PRA to improve the design of the reactor systems early in their development life cycle.

The earlier stages of the research, as described in "The Impact of Uncertainties on the Performance of Passive Systems" [16], assessed the reliability of the passive cooling system for a gas-cooled fast reactor design. This passive cooling system consists of a number of identical loops driven by either natural circulation or active blowers to remove decay heat during a loss-of-coolant accident. For the natural circulation version, a high-pressure containment is necessary to maintain sufficient driving force for the natural circulation. In either case, the coolant flows from the reactor core through an inner coaxial duct to an emergency cooling heat exchanger. It then transfers the decay heat to an external cooling source and returns to the core through a check valve via the outer coaxial duct. The check valves prevent back-flow through the emergency cooling heat exchanger during normal operation.

The researchers recognized that traditional PRA approaches captured the safety benefits of redundancy and diversity but failed to account for the role of functional margins on risk. That is, PRAs typically quantify functional failures of systems in a coarse manner, by assuming that their probability of failure is zero whenever they meet the success criteria. This is appropriate when analyzing active safety systems because the functional margins can be sufficiently large to guarantee successful operation. However, this is not necessarily the case for passive safety systems. The functional margins in passive systems should also deal with uncertainties related to the functional aspects of a system—that is, the ability of a system to perform its function. In the case of thermal-hydraulically driven passive systems, this margin may be a large contributor to the reliability of the PSS. Particularly for helium-cooled reactors such as those discussed in the MIT research, the relatively poor heat-transfer characteristics of helium can significantly reduce this margin.

This research employed an importance-sampling Monte-Carlo technique to identify and propagate the key uncertainties that affect PSS reliability. In addition to parameter uncertainties, the MIT model also captures uncertainties in the correlations within the TH computer models and assigns prediction errors to each correlation. Using 10,000 Monte Carlo simulations on various active and passive design options, the research showed failure probabilities that would be

high enough to require additional attention. One important conclusion from this research determined that the amount of functional margin in a system might not be as important as the ability of the uncertainties to degrade that margin. In other words, a system with greater functional margin, but also greater uncertainty, may prove to be less reliable than a design with fewer margins but more certainty. The research also noted that key uncertainties or assumptions that affect all loops can significantly reduce the benefits of redundancy, such as may be the case for passive safety systems. As a result, analysts must carefully assess redundancy in passive systems to account for the possibility of common mode failures. For these reasons, the research cautions that passive systems may not be more reliable than similar active safety systems.

Continued research published in 2007, "Incorporating Reliability Analysis into the Design of Passive Cooling System with an Application to a Gas-Cooled Reactor" [17], focused more specifically on estimation of the reliability of a two-loop passive decay heat removal system for a helium-cooled fast reactor. The authors describe the reliability-evaluation process in six tasks:

1. Identification of potential failure points. Standard FMEA and/or HAZOP methods may be helpful in accomplishing this task.
2. Definition of component failure criteria—either deterministic or probabilistic.
3. Selection of parameters that affect system performance—a structured approach such as the AHP may be helpful to achieve this objective.
4. Development of probability distributions for parameters—based on experiments and/or expert opinion.
5. Propagation of uncertainty distributions—using Monte Carlo or other related options.
6. Calculation of system reliability.

This process is similar to the approaches described in many of the European research papers. It also includes tasks to help improve the quality and efficiency of the process, such as early sensitivity analyses and iteration among tasks.

During the modeling, the researchers discovered situations in which failure of check valves in the cooling loops could cause the flow to bypass the core and instead circulate only through the cooling loops. This situation prompts a warning against simplified modeling of otherwise redundant loops for which small operating margins may cause undesired effects, though it also points out the continued importance of the reliability of traditional components. The researchers also identified the need to explicitly model the heat capacities of structures. Although such modeling details may be unnecessary for water-cooled reactors, they may become quite important in gas-cooled reactors in which the heat capacities of the structures can significantly exceed those of the helium coolant. Sensitivity analyses on parameter uncertainties were able to identify failure thresholds for some parameters in which failures became very unlikely.

Regulatory Experience

A key source of information for this report is the actual experience of regulators in dealing with the issue of PSS reliability. At this time, the NRC has completed the formal design-certification

review of the AP600 and AP1000 plant designs that incorporate passive safety systems. Based on the early work on the AP600, a paper by NRC staff and a contractor, as described in "A Risk-Based Margins Approach for Passive System Performance Reliability Analysis" [18], presents a basic "risk-based margins approach" to PSS reliability. This approach uses four basic steps:

1. Perform accident-sequence grouping and selection of bounding sequences.
2. Identify sources of uncertainty.
3. Identify "large impact" variables.
4. Explore available margin-to-core damage.

A similar approach is evident in the review of the AP1000 design certification. Although the design control documents "Westinghouse AP1000 Design Control Document Revision 15 Errata" [19], and the NRC safety evaluation report "Final Safety Evaluation Report for AP1000 Design" [20] provide the basis for the final design approval, perhaps the best discussion of the approach to PSS reliability appears in the transcript of an Advisory Committee on Reactor Safeguards (ACRS) meeting and as described in the *Official Transcript of Proceedings: Advisory Committee on Reactor Safeguards Subcommittees on Reliability and Probabilistic Risk Assessment* [21] on the topic. In their design-certification submittals, Westinghouse used a "risk-based bounding approach" that reanalyzed scenarios using conservative assumptions for key TH parameters. They first used expanded event trees to identify potentially risk-important scenarios that had low TH margins. They then used design-basis-approved computer codes to perform bounding TH calculations to determine any increase in risk as a result of PSS reliability issues. For their purposes, they defined low-margin scenarios as accident scenarios that potentially uncover the reactor core but do not lead to core damage. Risk-important scenarios were successful scenarios in the PRA with a frequency equal at least 1% of the total core-damage frequency. They analyzed these scenarios again to verify their success under conservative TH assumptions. Because these scenarios remained successful, they concluded that the effect of PSS reliability on overall risk was negligible.

The ESBWR design from GE is currently in the design-certification process. In response to a request for additional information from the NRC, GE is performing an analysis of TH uncertainty for their passive safety systems. Their official response to the NRC as described in "Response to Portion of NRC Request for Additional Information Letter No. 3 Related to ESBWR Design Certification Application, RAI Number 19.1.0-1" [22] indicates that they are using a somewhat similar approach as Westinghouse by performing an analysis of the sensitivity of the PRA results to changes in the success criteria of passive systems. GE examined three of the ESBWR's four passive safety systems: the gravity driven cooling system (GDCS), passive containment cooling system (PCCS), and automatic depressurization system (ADS). Because of the "extensive experience" with isolation condenser systems (ICS) in operating plants, they did not include the ICS in the review. Assuming design-basis success criteria instead of PRA success criteria for those three passive safety systems, the core damage frequency increased by a factor of approximately 10, from 1.07E-8 to 1.97E-7. Although this may represent a substantial increase, the overall risk remains low. From additional sensitivity calculations of lesser

combinations of success criteria changes, GE claims that the risk results show little to no sensitivity to changes of success criteria by one GDCS injection valve, one depressurization valve, or one PCCS heat exchanger. From this, they conclude that an adequate margin exists in the success criteria and the PRA results as a result of uncertainties in the performance of the passive safety systems. As of the drafting of this report, a response from the NRC is not yet available.

3
ADVANCED MODELING TECHNIQUES

The purpose of this task is to evaluate innovative or advanced techniques for PSS reliability modeling. In particular, this section describes advanced techniques for quantitatively addressing the TH reliability of a passive safety system.

TH code uncertainties can come from uncertainties in the imperfect modeling of the physical geometry of the system, uncertainties in the value and/or precision of input parameters, and uncertainties in the modeling of the physical processes as a result of solution methods that use imperfect correlations or numerical-solution techniques. Potential TH effects include one-dimensional versus multi-dimensional effects, physical asymmetries, two-phase flow instabilities, TH oscillations, and the effects of noncondensible gases.

In short, the advanced techniques described in the literature take similar, straightforward approaches to estimating passive system reliability.

The previously described RMPS approach addresses two types of uncertainties. The first type of uncertainty relates to correlations and the other inputs and models contained in the codes used to model TH systems. The second type of uncertainty relates to the more fundamental physical processes that directly affect natural circulation. The approach addresses both types of uncertainty using qualitative techniques adopted from FMEA and HAZOP methods. RMPS evaluates the significance of these uncertainties with code calculations and, in some cases, supplements the calculations with response surfaces fit to the code results. Application of these techniques leads to the identification of disturbances that might upset natural circulation, such as noncondensible gas buildup where condensation is occurring, fouling of heat exchanger surfaces, the presence of foreign material, and stratification. In some systems studied, the overall failure probability of passive systems is comparable to those in active systems (see, for example, “The Impact of Uncertainties on the Performance of Passive Systems” [16]). The major difference is that, in passive systems, the failure of natural circulation itself dominates the failure probability, whereas in the active systems, mechanical failures of active components dominate.

Jafari’s application of REPAS as described in “Reliability Evaluation of a Natural Circulation System” [9] uses a somewhat more quantitative approach, in that a complete exercise of a TH model follows the identification of the key inputs and their associated probability distributions. This TH model is a simplified version of a detailed model, purpose-built to support Monte Carlo or other analyses that propagate the uncertainty distributions. They demonstrate a version of this methodology, applied to an experimental version of a passive heat removal (PHR) system. The process involves performing steps to identify key parameters, assign probability distributions, create a TH model, determine the required “mission” of the system, define failure criteria, select

parameters for uncertainty analysis, perform uncertainty analyses, and assess the analysis results to determine the reliability of natural circulation.

As noted previously, considerable work exists regarding general methodologies for addressing the reliability of passive safety systems. The remainder of this section focuses instead on identifying and addressing specific characteristics and challenges posed by the passive systems planned for near-term advanced light-water reactor designs and Generation IV advanced reactor designs. Specifically, this task considers:

- How well uncertainties in passive system performance are understood for each of these broad classes of systems.
- Whether an analysis can treat each type of system in a relatively isolated fashion, such as by parameterizing the boundary conditions applied to the individual system. For some safety systems, a relatively complex coupled analysis may be necessary, and such systems will require more careful treatment than the others will. In this regard, it is probably not surprising that most of the assessments of passive safety systems published to date in the open literature have assessed relatively easy-to-treat "isolated" systems such as PHR and isolation condenser system (ICS) rather than, for example, the PCCS.
- To what degree existing, commonly available tools such as RELAP are considered suitable for assessing the performance of passive safety systems within the context of a methodology such as REPAS or RMPS. Are there situations where the limitations of the usual safety-analysis tools require computational fluid dynamics (CFD) or special "outside the box" considerations?

This is a very broad issue, so in this research effort, the following simplifying assumptions were made to make this effort tractable.

This task neglects failure of piping or welds, except for corrosion of thin-walled heat exchanger tubing. Based on previous work, the former types of failures should not be limiting. Gosselin et al., as detailed in *Probabilities of Failure and Uncertainty Estimate Information for Passive Components—A Literature Review* [23], provide an extensive recent review of work in this area.

This task focuses on the pre-core damage (prevention) phase of accidents. Use of passive safety systems to mitigate core damage will generally involve complex phenomena such as aerosol behavior, noncondensible gas generation and transport, issues associated with very high heat transfer rates, and debris crusting. For example, operation of systems that cool core debris in the containment (for example, ESBWR basemat-internal melt arrest and coolability device [BiMAC]) or in the lower head of the reactor pressure vessel (RPV) (for example, AP1000 in-vessel retention) can be sensitive to such uncertainties as material interactions and properties at high temperatures, heat transfer correlations under extreme conditions, and the behavior of submerged reactor-vessel insulation. Although past and ongoing experiments address these issues, assessments of the reliability of such systems under severe accident conditions will require an in-depth investigation of the special considerations involved in each particular case. Thus, making general conclusions about the types of analyses necessary in these cases is particularly difficult.

Many passive systems are subject, at least in principle, to the possibility of two-phase flow instabilities. D'Auria, et al., in a paper titled Insights into Natural Circulation Stability [24] and IAEA TECDOC-1281, *Natural Circulation Data and Methods for Advanced Water Cooled Nuclear Power Plant Designs: Proceedings of a Technical Committee Meeting Held in Vienna, 18–21 July 2000* [25], provide a review of this subject in the context of passive safety systems. These reviews suggest that analysis using the usual qualified codes can often determine the onset of instabilities that could affect the operation of systems that depend on natural circulation unless the solution algorithms introduce so much artificial damping that they inappropriately suppress the instabilities.

General Comments on Analytical Tools

To assess the impact of uncertainties, most published analyses of passive safety systems employ one-dimensional codes such as RELAP, TRACG, or their European counterparts. Some researchers have stated that these codes may not have sufficient detail for large passive safety systems for which three-dimensional effects may be important. Wichers, et al., as described in "Testing and Enhanced Modeling of Passive Evolutionary Systems Technology for Containment Cooling (TEMPEST)" [26], demonstrate a hybrid approach using CFD to provide insights on stratification that conventional safety codes can then use. Researchers also use CFD to study whether there are conditions in advanced boiling water reactors (BWRs) in which steam discharged into a subcooled suppression pool could fail to condense (for example, through strong stratification of the pool). This has also been the subject of considerable experimental work.

Interest is growing in using CFD for specialized studies, but it does not appear that this is the technique of choice for most applications, due to limitations in the state-of-the-art (for example, two-phase flow) modeling or simply because their use would be unwieldy when a large number of sensitivity calculations is necessary. For the foreseeable future it is likely that analysts will continue to rely on more traditional codes. Fortunately, experience to date has generally demonstrated that the predictions of these codes compare favorably to scale-model simulations of passive safety systems as described in "TEPSS—Technology Enhancement for Passive Safety Systems" [27], especially considering the reduced need for absolute fidelity in the context of a PRA. Nevertheless, modelers of a particular passive safety system should ensure that they could demonstrate good code fidelity for the situation of interest.

Assessment of Potential Passive Safety Systems

This section discusses the challenges posed in evaluating various passive safety systems planned for advanced reactors by focusing on the key phenomenological features on which their operation depends.

Systems Using Continuous Natural Circulation of Water Through a Heat Exchanger in a Closed Loop

The prime example of such a system is the passive residual heat removal (PRHR) system in the AP1000 and other PWRs. Issues that may affect the operation of such systems include:

- Successful valve operation to initiate operation
- Successful long-term cooling of the ultimate heat sink
- Fouling and foreign material
- Undetected tube corrosion and the potential for tube failures
- Two-phase flow during loss-of-coolant accidents (LOCAs)

The PRA may normally credit such systems for accidents involving a subcooled reactor coolant system, such as loss of feedwater, feedwater line breaks, or steam line breaks. If the PRA needs credit during LOCAs, it should include additional uncertainties associated with two-phase flow modeling. However, the existing tools developed for treating small-break LOCAs would be applicable.

Such systems should be readily analyzable, either by modeling them in isolation by changing the boundary conditions applied to the system or by including the PRHR loop in the overall primary system model. The level of uncertainty appears to be quite low, especially if two-phase flow conditions do not occur.

Marques, et al., in "Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment" [12], demonstrated an analysis of a PRHR system in a station blackout accident using the RMPS methodology. The authors used FMEA to identify critical system parameters and expert judgment to quantify uncertainties in these parameters. They used response surfaces based on detailed code results (in this case, CATHARE) to quantitatively evaluate the impact of the assessed range of uncertainties. The authors concluded that unless tube failure occurs, the pool level and the decay-heat curve represent the largest uncertainties. They also found that their conclusion that the system would operate successfully was relatively robust.

Systems Using Continuous Natural Circulation of Gas for Core Cooling

Similar considerations apply to passive cooling systems involving natural convection of pressurized gas. Pagani, et al., in "The Impact of Uncertainties on the Performance of Passive Systems" [16], modeled such a system for a gas-cooled fast reactor. The authors developed a purpose-built lumped parameter model and then exercised the model over a range of reactor powers, pressures, correlation parameters, and wall temperatures. As mentioned earlier, a particular focus of their study was to use this example system to illuminate the difficulties of defining success criteria for passive systems that can "fail," not because the systems do not work (which might be the case if a component actually failed), but because they may not fully fulfill their design objectives.

Issues associated with successful operation of these systems are essentially the same as for their single-phase water counterparts:

- Successful valve operation to initiate operation
- Successful cooling of tube walls
- Fouling and foreign material
- Undetected tube corrosion and the potential for tube failures

Such systems should be relatively easy to model, and the conclusions of the study should be fairly robust. Unlike their all-water counterparts (for example, PRHR) and cooling systems that depend on condensing steam (for example, isolation condensers), the system performance should be strongly dependent on pressure/gas density on physical grounds. This is a rather stark example of a "functional failure" because the system will not remove decay heat if the system pressure and, thus, the gas density drop too low. Further, they demonstrated that the existence of substantial functional margin under nominal conditions does not provide a measure of the susceptibility of the system to functional failures under other conditions.

As in the case of PRHR systems, gas-cooling loops should be readily analyzable, either by modeling them in isolation by changing the boundary conditions applied to the system or by including the loop in a comprehensive primary-system model. The level of uncertainty in such analyses for a given set of defined boundary conditions appears to be fairly low, albeit higher than that of an all-liquid system operating at lower temperatures.

Systems Using Drainage of Water as a Result of Hydrostatic Head Imbalances Without Depressurization

The prime example of such a system is the core makeup tank incorporated in the AP1000 and similar designs. Issues that may affect the successful operation of such systems are valve reliability and loss of stratification in the pool.

When steam is present at the inlet to the pressure balance line (PBL), some researchers, as described in "Inherent Failure Modes of Passive Safety Systems" [1], have stated that achieving the required flow rate can be dependent on maintaining stratification in the pool in the face of a strong flow of steam through the PBL. When two-phase flow exists in the reactor coolant system, uncertainties such as the branching fraction at the inlet will impact operation. However, use of standard reactor safety codes such as RELAP developed and qualified for small-break LOCAs appears appropriate.

As in the case of PRHR systems, core makeup tank (CMT) systems should be readily analyzable, either by modeling them in isolation with parameterized inlet and outlet boundary conditions or by including the system in the overall primary system model. The level of uncertainty in the modeling appears to be relatively low.

Test data for qualification of models and assessing uncertainties are available from the Oregon State University Advanced Plant Experiment (APEX), as described in *Natural Circulation in Water Cooled Nuclear Power Plants: Phenomena, Models, and Methodology for System Reliability Assessments* [28].

Systems Using Accumulators

Virtually all advanced PWR designs use accumulators. Their successful operation depends on the following:

- Check valve operation
- Loss of water from a break in large-break LOCAs
- Heat transfer to the fuel pins under conditions of low pressure and high surface temperatures in large-break LOCAs

Modeling accumulators in advanced light-water reactors poses the same difficulties as in the current generation of reactor designs, and the results of the analysis should be relatively robust. However, some of the considerations mentioned previously may not apply for advanced reactor designs such as AP1000 that have a dedicated reactor vessel injection line that eliminates the loss of injection water during a large-break LOCA.

Systems Using Drainage of Water from an Unpressurized Tank for Core Cooling

Advanced PWRs and BWRs typically employ systems such as GDCSs that allow an elevated tank in the containment to drain into the primary system following depressurization to provide long-term cooling. The issues involved in successful operation include:

- Success of the ADS
- Successful isolation-valve operation

The details of the time-dependent operation of GDCS-type systems, especially in BWRs, will depend on the operation of wetwell/ RPV equalization lines and vacuum breakers. Nevertheless, success in terms of a PRA is primarily dependent simply on the adequacy of primary system depressurization, which is fairly straightforward to model and to account for uncertainties.

Systems Using Condensation of Steam for Core Cooling

An example of such a system is the isolation condenser in various current-generation and advanced BWR designs. In advanced BWR designs, isolation condensers provide core cooling in high-pressure accident sequences, while depressurization valves and GDCSs provide core cooling in low-pressure accidents. The advanced PWR design IRIS may use a similar emergency heat removal system (EHRS) for secondary cooling.

The issues that can complicate analysis of these types of systems include the following:

- Collection of noncondensible gases
- Fouling
- Blocking of the inlet pipe due to severe heat losses (for example, as a result of damaged insulation)
- Plugging as a result of foreign material
- Tube failure under elevated temperature accident conditions as a result of undetected corrosion

Although operation should be robust when no noncondensibles are present, performance can degrade as a result of collection of noncondensible gasses, both from radiolytic decomposition and (eventually) hydrogen production during severe accidents. Sweep-out lines prevent excessive buildup of such gases.

Even though condensation rates are strongly dependent on the amount of noncondensible gases present in the tubes, extensive experimental data and correlations are available to estimate the degradation in performance. Data sources available for qualifying models include PANDA and PUMA test facilities, as described in *Natural Circulation in Water Cooled Nuclear Power Plants: Phenomena, Models, and Methodology for System Reliability Assessments* [28]. Although an analysis could model the systems in an isolated fashion if desired, the feedback of ICS operation on the other parts of the system is sufficiently strong that it is probably better to model them in an integrated fashion.

Systems Using Condensation of Steam for Containment Cooling

This category includes passive containment cooling systems with rather diverse designs. The AP600 and AP1000 designs use ambient air circulation through a shroud over the exterior of a steel containment shell. A supply of water that drains over the surface of the shell from an elevated tank supplements the cooling effect of the air. Advanced BWR designs include a set of explicit condensers submerged in an external pool through which gas in the drywell circulates and condenses.

Issues affecting successful operation include:

- Effect of noncondensible gas on condensation heat transfer
- Fouling of heat transfer surface
- Tube failure in BWR PCCS
- Limitations on heat transfer at high cooling rates as a result of gravity drainage of condensate film and external heat transfer coefficient in the AP600/1000

Of all the passive safety systems, accurate modeling of the BWR PCCS may require the most complex analysis. A complete representation of the behavior of these systems requires the representation of the distribution of noncondensible gases in the containment, the potential for stratification in the suppression pool, and the interaction between GDCS and the core. It is, therefore, difficult to confine attention to a discrete set of boundary conditions. Nevertheless, conventional one-dimensional safety codes appear to do a good job in analyzing this behavior, as outlined in "TEPSS—Technology Enhancement for Passive Safety Systems" [27].

Analysis of the AP600/1000-type system does not appear to be as difficult and, except for the need to model heat transfer to the external water film and flowing air, poses difficulties comparable to modeling condensation on passive heat sinks in conventional PWR safety analysis. The NRC review of the AP1000 as described in *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design* [29] identifies other concerns regarding functional failures of the PCCS as a result of wind-dependent pressure fluctuations and non-uniform distribution of the water film on the outside of the containment shell. Although the NRC resolved these issues for the AP1000, they represent the types of subtle issues that designers should consider for other plant designs that implement similar containment cooling techniques. Generally, for these types of systems, there is both a sufficient level of margin and an adequate experimental basis to support the analysis.

4
RESEARCH AND DEVELOPMENT ISSUES

The purpose of this task is to consolidate the key issues related to PRA requirements for passive safety systems. This section evaluates the state of each issue to describe the practicality and maturity of the existing research.

Categorization of Passive Systems

Though the IAEA has had a classification system for passive systems since 1991, the classification system may need modification. The existing classification system provides one good set of criteria for passive systems. However, for the purposes of PRA, a different approach may be necessary. In fact, the research literature does not strictly conform to the IAEA classification. For example, many passive systems in new plant designs may fall under Category B or Category D, depending upon how an analyst chooses to treat features such as the actuation of the system. Passive systems may need active actuation, though the actuation signal may use dedicated batteries and/or the actuation action may use stored energy (for example, a squib valve that requires a dc-powered actuation signal).

Just as with active systems, different passive systems will have different impacts on the overall risk at a nuclear power plant. Passive systems that have minimal or no risk importance should not receive the same level of analysis as a passive system with a larger impact on risk. Because the existing IAEA classification does not address this issue, it does not help to determine the level of analysis needed for a given passive system.

Analysis Challenges

The literature review identifies a number of analysis challenges. The documented analyses all take a fairly straightforward approach to the assessment of PSS reliability. Beginning with a definition of the system of interest, each method attempts to model the important phenomena and identify the likelihood that system parameters or the system environment will cause the system to fail to perform its intended function. All of the methods seem to encounter a similar set of challenges, many of which relate to each other:

- More or different potentially important failure mechanisms
- Scarcity of data sources for unique component failures or different phenomenology
- Reliance on expert judgment for identification of key phenomena

- Reliance on a large number of Monte-Carlo computer calculations requiring significant computation time
- Consideration of both the level of uncertainty in important phenomena and the sensitivity of system behavior to that uncertainty

The approaches to these issues result in increased levels of effort for the analysis. Analyses may require more work to examine the potential failure mechanisms of the system. Because data are sparse for some or all aspects of the analysis, expert judgment often provides the only approach to estimate performance characteristics. Expert judgment may also be necessary during the identification of key phenomena to reduce the scope of the analysis to a manageable level. Even after that, the analysis will likely require a large number of complex computer simulations of system behavior in order to estimate its failure probability. The relationship between the uncertainty in the phenomena and the system's sensitivity to those phenomena is not always straightforward and, therefore, magnifies the challenges in the expert-judgment process. Ultimately, each of these issues requires an increased level of effort—more expert judgment, more computer simulations, and more overall analyst effort. The documented analysis examples involve significant overall effort to analyze one system. For the analysis of an entire plant with multiple, possibly interactive passive systems for regulatory purposes (for example, to support a reactor license submittal), the level of effort may be even greater.

Additional Issues

A few other issues exist that do not directly relate to the PSS reliability approaches in the literature.

Synergistic Effects

Similar to some other types of analyses for nuclear power plants, the documented experience with PSS reliability seems to focus on the analysis of one passive system at a time. In many cases, this may be sufficient, but for some advanced designs with multiple passive systems, modeling of the synergistic effects among the systems may be important. For example, modeling of a passive containment cooling system may require simultaneous modeling of the distribution of noncondensible gases in the containment, the potential for stratification in the suppression pool, and interactions between the passive core cooling system and the core. Analysis of each of these systems independently may not fully capture the important boundary conditions of each system. The literature search did not identify any work regarding this issue.

Post-Core-Damage Mitigation Strategies

As discussed earlier, there are many different types of passive system designs. The focus during most of this research has been on core damage prevention and containment protection systems, as has been the focus of research reported in the available literature. However, many new plant designs also incorporate passive systems into the post-core-damage mitigation strategy, such as devices to contain and cool molten corium following a core-damage accident. The analysis of

these processes includes different phenomenologies that may create other challenging issues. Further work regarding PRA requirements for these types of systems might be necessary, particularly if the plant licensing basis, safety analysis, or PRA credits operation of these systems.

Gas-Cooled Reactors

Finally, it is important to note that the research described in this report has focused on water-cooled reactors because the next generation of plants to be deployed in the United States is anticipated to employ this technology. Advanced gas-cooled reactors have very different TH phenomenology and may operate under a different (and yet unspecified) regulatory regime. (See the EPRI report *Technical Elements of a Risk-Informed, Technology-Neutral Design and Licensing Framework for New Nuclear Plants* [30] for a summary of the currently proposed alternative frameworks.) The available functional margins in gas-cooled passive systems are likely to be much more sensitive to changes in operating parameters, boundary conditions, and the surrounding environment than for water-cooled passive systems. In addition, because there is far less operating experience with gas-cooled power reactors, fewer data exist and further research may be necessary to build up a comparable database of knowledge. If the regulatory structure uses a more risk-based approach to license and regulate future gas-cooled reactors, the importance of accurately assessing PSS reliability may gain much more importance. For water-cooled reactors in the current regulatory structure, much margin may exist as a result of the parts of the regulatory process that are still largely deterministic. If a new regulatory structure reduces or eliminates these deterministic aspects, PSS reliability for gas-cooled reactors might require significantly more attention.

Because of these issues, it would be beneficial to develop a graded approach to analyzing the safety risk impact of PSS. The next section proposes a research plan to accomplish this objective.

5
PROPOSED RESEARCH AND DEVELOPMENT PLAN

Conclusions

Based on the observations and issues identified previously, this research effort can draw a number of conclusions that lead to several recommendations for an R&D plan. These conclusions and recommendations focus on the best solutions to the most significant issues associated with PRA requirements for PSS reliability. It is important that the solutions developed are practical, cost-efficient, and timely, and that they address both qualitative and quantitative aspects of reliability.

- Passive system reliability is not necessarily better or worse than active system reliability. Reliability will depend on the overall design and operation of the system, regardless of whether the system is active or passive. A good overall plant design may include active systems, passive systems, or a combination of both types of systems to meet performance and safety objectives.
- A system that has greater functional margin, but also greater uncertainty, may prove to be less reliable than a system with less functional margin but less uncertainty.
- Because passive systems are likely to be more sensitive to variations in TH parameters, analysis of their reliability should include consideration of a broader range of failure mechanisms, including mechanisms that may provide a significant impact on the phenomenology and functional margins.
- Although uncertainties exist in computational codes, a high-quality code benchmarked on experimental data should be adequate to calculate the important phenomena expected for passive system operation.
- In a risk-informed environment (for advanced light-water reactor designs), regulators will continue to use conservative deterministic calculations, along with results and insights from probabilistic risk assessment, to ensure safety. This provides additional assurance of a reliable system, particularly for advanced light-water reactor designs operated under the current regulations.
- Because liquid systems are less sensitive to variations in operating conditions such as system pressure, a high-quality design of a liquid-driven system usually yields high confidence in the ability of the system to perform its function under a broad range of conditions. Systems that rely on condensing steam to remove decay heat should also function in a robust fashion as long as the means provided for purging noncondensible gases functions as designed.

- Best engineering practices under the current risk-informed regulatory regime create a requirement for a high-quality analysis with a good understanding of natural convection. Passive systems may require more care in this regard than active systems, but it is within the capabilities of the current state of the art.
- Full modeling capabilities may be necessary to capture the effects of any potential interactions among systems that may not be evident in independent system analyses. This is also within the state of the art.
- Existing PRA approaches and approved TH analysis codes can address many issues related to PSS functions in advanced light-water reactor designs.
- More attention may be necessary during plant operation to monitor for passive system characteristics that can affect performance (for example, pipe fouling). Thus, these insights and requirements should appear in the reliability, availability, and maintainability program.
- Gas-cooled reactors may have several unique issues requiring further R&D. These include:
  - Differences between the TH behavior of gases and liquids
  - Unique recovery strategies (for example, quasi-steady states and recriticality)
  - Reduced redundancy as a result of fewer or no active systems
- A more risk-based regulatory regime in the future might require a more accurate accounting of functional margin.
- Other complex TH questions (for example, dynamic instabilities) might exist, but designers and analysts should be able to solve these as TH design questions rather than PRA issues.

Passive components or systems are always part of a larger system and contribute to the overall safety of the reactor. Therefore, it is important to view the analysis of PSS reliability within the context of the overall risk. This view provides an opportunity for the analyst to make intelligent simplifications to the process. For many systems and/or scenarios, it may be possible to show that PSS reliability is an insignificant contributor to system failure or overall risk.

Because passive systems eliminate some of the dominant failure mechanisms seen in active systems, more and different failure mechanisms are likely to dominate passive system reliability. Such mechanisms may include structural failures, physical degradation of components, blocking of flow paths, actuation signal failures, reduced heat-transfer capability, and unexpected changes in boundary conditions. Such failure mechanisms, though rare, do appear in operating experience (for example, events that include the failure of control rods to fall under gravity, breaking of natural circulation loops as a result of stratification, and decreased radiation heat transfer as a result of environmental phenomena, as described in “Screening of Probabilistic Safety Evaluations for Different Advanced Reactor Concepts” [2]). Where the system architecture permits and adequate data exist, the analyst may be able to estimate the functional reliability aspects of the passive system based on active components that lead to these types of failure mechanisms. Only when these functional reliability aspects become negligible must the reliability focus on the TH performance of the passive system in detail.

The reliability of a PSS depends upon the integrity of its components and its ability to function under all required conditions. Therefore, the assessment must consist of both classical reliability analysis of its components and evaluation of the passive function, which may involve classical reliability analysis of other components designed to ensure conditions conducive to success of the passive system. However, direct application of a straightforward approach to deductively calculate PSS reliability may involve a prohibitively large number of complex TH calculations. Therefore, a more practical approach to the issue must provide a systematic method to focus the necessary calculations on the most important characteristics. The approach must link the PSS reliability analysis to the regulatory purpose, which is usually defined by the assessment of risk (for example, core damage frequency or large early-release frequency).

Anticipating the Unknown

As discussed in the introduction, the objective of this research was to take an initial step toward characterizing the issues and limitations that currently exist in the application of PRA technologies to the evaluation of the reliability of passive safety systems and to recommend an R&D program to address these issues and limitations. Although the list of conclusions listed previously summarizes a number of identified issues, it is important to recognize that existing research in this area is not all-inclusive.

The research to date, represented by both the extant literature and the work supporting this report, shows several limitations. In general, much of the research has understandably used a narrow scope that is specifically focused on achievable issues. The existing research typically addresses easily anticipated issues and uses relatively straightforward approaches to their solutions. The approaches often use separate effects calculations to examine specific design issues in isolation rather than fully integrated models of the reactor and its environment.

Yet it appears likely that passive safety systems may have many unique characteristics that the existing research has only begun to address. For example, PSSs appear to have a wide range of susceptibilities that may produce unique failure mechanisms unlike the standard failure mechanisms seen in the literature. As advanced light-water reactor designs and gas-cooled reactor designs increase their dependence on passive safety systems, the greater importance these unique and possibly unknown issues will become evident. Therefore, a broader, more comprehensive research perspective may be necessary to address the wide range of issues related to risk analysis of nuclear power plants with passive safety systems.

For example, the use of passive safety systems could introduce unique potential issues as a result of the specifics of their construction, operation, or environment. Some hypothetical examples include the following:

- For a passive containment cooling system, rapid weather changes could affect the driving pressure differentials, heat transfer characteristics, or other factors via rapid atmospheric pressure changes or temperature fluctuations.

- For a passive containment cooling system that uses external airflow located near a salt-water body, fouling of the containment surface via salt-entrainment in the air could alter important cooling characteristics such as the heat transfer properties or the distribution of air or water over the containment shell.

- For passive safety systems with infrequently used, low-flow heat exchangers, current testing and maintenance plans may not capture problems such as long-term corrosion or biofouling that could reduce heat transfer characteristics and increase friction factors.

- For passive safety systems using treated water (for example, boric acid), chemical deposits could degrade the performance of either the passive system itself or other interfacing systems. Such effects may be particularly likely at interface points and discontinuities in the system such as valve locations.

These types of atypical effects (and others discussed throughout the report) demonstrate the need to expand the traditional state of knowledge for PSS failure mechanisms. In addition, combinations of both recognized and emergent effects have a greater potential to lead to unknown interactions that negatively influence the operation of passive safety systems. It is these types of "unknowns" and interactive effects that should be thoroughly explored in order to provide the most complete assessment of the effects of PSS reliability on the overall risk at a nuclear facility.

The value of identifying and addressing issues such as these is greatest before construction and operation of any advanced reactor design. Although the research tasks discussed in the next section do not specifically address these types of issues, the tasks should recognize and integrate these types of concepts. The demonstration application tasks would be appropriate places to revisit the unique aspects of passive safety systems and highlight any specific research needs to address them. Such an approach would better enable the outcomes of the research to positively affect the reliability, availability, and maintainability programs for new reactors.

Recommended R&D Tasks

Based on the research summarized here, this report recommends the development of a phased approach to the assessment of PSS reliability. Such an approach will combine regulatory PRA needs with identification of the leading failure mechanisms to categorize and screen passive systems. A detailed TH uncertainty analysis would be necessary only for some systems. For situations in which the reliability of passive systems is a key contributor to overall risk, it may prove wiser (and less expensive) to modify the design of the system in order to provide additional margin or reduce the risk-significance of the system rather than attempt to prove PSS reliability to a fine degree. Alternatively, in particularly critical applications for which the PSS may not provide adequate margins, it may be more appropriate to use conventional active systems to achieve the safety-function objective. (See "The Impact of Uncertainties on the Performance of Passive Systems" [16] for an example gas-reactor application.)

In the end, the evaluation of PSS reliability for PRA is likely to remain a risk-informed activity for the near future. Large uncertainties may be unavoidable when dealing with newly deployed reactors with passive safety systems. Therefore, more traditional, deterministic analyses and experimental testing (when appropriate) to ensure the overall safety of the passive system and, ultimately, the overall safety of the reactor should support any PSS reliability evaluation.

The following tasks provide specific recommendations for future research based on the conclusions of this study. Each recommendation provides the purpose of the proposed task, its potential impact, estimated schedule, and estimated resource needs. The potential impact of a task relates to both its potential effect on near-term new reactor licensing activities and the ability to achieve the task in a timeframe to support such activities. The schedule estimates range from less than a year (short) to a few years or more (long). The resource estimates generally correspond to the schedule estimates, ranging from approximately a half staff-year of effort (low) to multiple staff-years of effort (high), as shown in Table 5-1.

Table 5-1
Impact, Schedule, and Resource Estimates

Potential Impact on New Reactors		Estimated Schedule		Estimated Resources	
High	Immediate and achievable	Short	6–12 mo	Low	< 6 staff-mo
Medium	Some impact and achievable	Medium	1–2 yr	Medium	6-12 staff-mo
Low	Gen-IV issue or long-term	Long	> 2 yr	High	>1 staff-yr

The first six recommendations focus on the analysis of passive system reliability for core damage prevention in advanced light-water reactors. The last two recommendations deal with the unique issues associated with passive safety system reliability for post-core-damage functions (Level 2 PRA) and revolutionary gas-cooled reactors.

Task 1: Categorization and Screening Process

The purpose of this task is to develop a formal categorization and screening process for passive systems to determine whether a passive system necessitates a formal reliability analysis for PRA and what level of analysis is required for those that require assessment. Considerations for categorizing passive systems include the working fluid involved (such as water or helium), the availability of data for similar systems (such as an isolation condenser), and whether the system requires actuation by other components. Existing PRA techniques such as sensitivity analysis and importance measures may be useful in determining the potential risk importance of a system and therefore indicate whether a passive system demands a basic analysis process or a more comprehensive approach. The decision criteria may consider a combination of the risk significance of the passive system, the available functional margin to accomplish its safety function, and the level of uncertainty regarding performance of the passive system. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: high
- Estimated schedule: short
- Estimated resources: low

Task 2: Database Development

The purpose of this task is twofold—to collect applicable historical data and to prepare for the collection of data for new nuclear power plants. The database development would collect two different types of data. An event-description portion of the database would capture the details of failures of passive systems or components with the goal of identifying unique failure mechanisms. This collection of identified failure mechanisms would then serve to ensure that all subsequent analyses of passive systems properly considered the full range of potential failure mechanisms. The second type of data gathering would collect traditional failure-probability data for components that are unique to passive systems or that have increased importance in passive systems. For this portion, the database should include both system/component demands and failures. Once collected, these data would provide an improved basis for failure probabilities in future PSS reliability evaluations. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: high
- Estimated schedule: medium (ongoing)
- Estimated resources: low

Task 3: Basic Analysis Approach

The purpose of this task is to develop a formalized basic analysis approach for passive systems that have low risk-significance or low TH complexity based on the categorization and screening process developed in Task 1. The approach would use risk-sensitivity analyses and conservative approaches similar to those used during the design certification of the AP1000. This approach

should be a sequence-based analysis rather than a system-based analysis, in that accident scenarios are the focus of the analysis rather than individual passive systems. The basic process would consist of steps to identify potentially risk-significant scenarios, identify conservative or bounding calculations if possible for those scenarios, and calculate the effect on risk by using those conservative or bounding calculations. For scenarios where such calculations are not available, the process should describe a simple procedure for identifying key variables and performing limited TH analyses to estimate the probability of PSS failure and its effect on overall plant risk.

Because PRA uses a binary analysis approach that defines each scenario as failure or success, the effect of PSS unreliability would be to convert a successful scenario to a failure scenario. If the total frequency of the potentially risk-important scenarios is already low enough, it will remain risk-insignificant even if the passive system does not possess high reliability. Where necessary, identification of key variables should make use of a broad range of available information, including expert judgment, TH sensitivity analyses, and all available experimental data. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: high
- Estimated schedule: medium
- Estimated resources: low

Task 4: Demonstration Application of the Categorization Process and Basic Analysis Approach

The purpose of this task is to perform a demonstration application of the developed categorization process and basic analysis approach on actual passive systems. The demonstration should include one or more passive systems in advanced light-water reactor designs. The demonstration would serve to both demonstrate the concepts of the approach and to refine the approach to allow broader implementation. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: high
- Estimated schedule: medium
- Estimated resources: medium

Task 5: Advanced Analysis Approach

The purpose of this task is to develop a formalized advanced analysis approach for passive systems that have a high risk-significance and high TH complexity based on the categorization and screening process of Task 1. The approach would build upon the previous research in the literature in order to develop a process optimized for advanced light-water reactor designs under the current U.S. regulatory regime. Similar to the basic analysis approach, the advanced analysis approach would also inductively identify scenarios in which a passive system would be most susceptible to a failure that would increase the overall risk of the plant. The goal of the approach

would be to develop a structured search process to identify scenario deviations that challenge the design assumptions of the passive system(s). This search process may draw upon existing techniques such as FMEA and HAZOP to develop a tailored search process for passive system failures. Such a process would expect to use expert judgment as an integral part of the search process, and these aspects could draw upon existing expert elicitation techniques common in fields such as seismic PRA and second-generation human reliability analysis.

Ultimately, the goal of the advanced analysis approach is to estimate the failure probability for the passive system. This probability could result from a combination of different scenarios that present different challenges to the passive system. Where necessary, the analyst would subdivide scenarios defined by the PRA into subscenarios to allow for a more detailed analysis. For scenarios in which the boundary conditions and environment are within the design envelope of the passive system, the probability of failure would be nearly zero. For scenarios outside the design envelope, the analysis could either assume a conservative failure probability of 1.0 or conduct further analysis to refine the scenario and/or passive system performance. The overall failure probability of the passive safety system is the sum over all scenarios of the probability of each scenario times the probability of PSS failure given each scenario. Impact, schedule, and resources for this task are outlined as follows:

$$\Pr(PSSfailure) = \sum_{allscenarios} \Pr(scenario)\, x\, \Pr(PSSfailure \mid scenario)$$

- Potential impact: medium
- Estimated schedule: long
- Estimated resources: high

Task 6: Demonstration Application of the Advanced Analysis Approach

The purpose of this task is to perform a demonstration application of the advanced analysis approach on one or more passive systems in advanced light-water reactor and/or gas reactor plant designs. The demonstration would serve to both demonstrate the concepts of the approach and to refine the approach to allow broader implementation. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: medium
- Estimated schedule: medium
- Estimated resources: high

Task 7: Level 2 PRA Issues and Approaches

The purpose of this task is to investigate the unique needs for the analysis of passive systems for Level 2 PRA. The first six recommended tasks focus on the analysis of passive systems for core-damage prevention systems. As discussed in Section 4 and Section 5, the phenomenology for post-core-damage passive functions may be significantly different from core-damage prevention functions. However, given the reduced attention that these types of systems often receive in PRA and the sometimes reduced risk significance of these types of systems, they will be of lower priority for R&D. The unique analysis needs for post-core-damage mitigation systems may result in modifications to the basic and advanced analysis approaches. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: low
- Estimated schedule: medium
- Estimated resources: medium

Task 8: Gas-Cooled Reactor Issues and Approaches

The purpose of this task is to investigate the unique needs for the analysis of gas-cooled reactors. The first seven recommended tasks focus on the analysis of advanced light-water reactors (although they are likely to be applicable to advanced gas-cooled reactors as well). As discussed in Section 4 and Section 5, the TH behavior of gas-cooled systems may be significantly different from water-cooled systems. Because the licensing and construction of gas-cooled reactors are unlikely in the immediate future, issues specific to these reactor designs will be of much lower priority for R&D. This task is intended to examine unique issues associated with gas reactor design (for example, issues associated with potential recovery strategies that permit the reactor to remain in long-term, quasi-steady states or permit recriticality) and the effects of a possible risk-based licensing process. The output of this task would be a longer term R&D plan to address the unique aspects of gas-cooled reactors. Impact, schedule, and resources for this task are outlined as follows:

- Potential impact: low
- Estimated schedule: long
- Estimated resources: medium

Table 5-2 summarizes these recommendations and their classifications.

Table 5-2
R&D Recommendations

Task	Title	Impact	Schedule	Resources
1	Categorization and screening process	High	Short	Low
2	Database development	High	Medium	Low
3	Basic analysis approach	High	Medium	Low
4	Demonstration application of the categorization process and basic analysis approach	High	Medium	Medium
5	Advanced analysis approach	Medium	Long	High
6	Demonstration application of the advanced analysis approach	Medium	Medium	High
7	Level 2 PRA issues and approaches	Low	Medium	Medium
8	Gas-cooled reactor issues and approaches	Low	Long	Medium

Table 5-3 presents a potential schedule for these R&D tasks.

Table 5-3
Potential R&D Schedule

Task	Topic	Year 1	Year 2	Year 3	Year 4	Year 5
1	Categorization					
2	Database					
3	Basic approach					
4	Demo—basic					
5	Advanced approach					
6	Demo—advanced					
7	Level 2 issues					
8	Gas reactors					

6
REFERENCES

1. Päivi Maaranen and Juhani Hyvärinen. “Inherent Failure Modes of Passive Safety Systems,” *Passive System Reliability—A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants: Proceedings of an International Workshop Hosted by the Commissariat à l’Energie Atomique (CEA)*. NEA/CSNI/R(2002)10, Cadarache, France (June 26, 2002).
2. C. Kirchsteiger and R. Bolado-Lavin. “Screening of Probabilistic Safety Evaluations for Different Advanced Reactor Concepts,” *Proceedings of the Eighth International Conference on Probabilistic Safety Assessment and Management*, New Orleans, LA (May 14–18, 2006).
3. U.S. Nuclear Regulatory Commission. Office of Nuclear Regulatory Research. *Review of Findings for Human Error Contribution to Risk in Operating Events*. NUREG/CR-6753. Washington, D.C. (August 2001).
4. L. Burgazzi. “State of the Art in Reliability of Thermal-Hydraulic Passive Systems,” *Reliability Engineering and System Safety*. Vol. 92, p. 671–675 (2007).
5. International Atomic Energy Agency. *Safety Related Terms for Advanced Nuclear Plants*. IAEA-TECDOC-626. Vienna, Austria (September 1991).
6. Organization for Economic Co-operation and Development. *Passive System Reliability—A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants: Proceedings of an International Workshop Hosted by the Commissariat à l’Energie Atomique (CEA)*. NEA/CSNI/R(2002)10, Cadarache, France (June 26, 2002).
7. International Atomic Energy Agency. *Description of Natural Circulation and Passive Safety Systems in Water Cooled Nuclear Power Plants*. IAEA-TECDOC-DRAFT, presented at the 3rd Research Coordination Meeting on the CRP on Natural Circulation Phenomena, Modeling, and Reliability of Passive Systems that Utilize Natural Circulation, Cadarache, France (September 11, 2006).
8. F. Bianchi, et al., “The REPAS Approach to the Evaluation of Passive Safety Systems Reliability,” *Passive System Reliability—A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants: Proceedings of an International Workshop Hosted by the Commissariat à l’Energie Atomique (CEA)*. NEA/CSNI/R(2002)10, Cadarache, France (June 26, 2002).
9. J. Jafari, et al., “Reliability Evaluation of a Natural Circulation System,” *Nuclear Engineering and Design*, Vol. 224, p. 79–104 (2003).

10. E. Zio, et al., "The Analytical Hierarchy Process as a Systematic Approach to the Identification of Important Parameters for the Reliability Assessment of Passive Systems," *Nuclear Engineering and Design*, Vol. 226, p. 311–336 (2003).
11. M. E. Ricotti, et al., "Reliability Methods for Passive Systems (RMPS) Study—Strategy and Results," *Passive System Reliability—A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants: Proceedings of an International Workshop Hosted by the Commissariat à l'Energie Atomique (CEA)*. NEA/CSNI/R(2002)10, Cadarache, France (June 26, 2002).
12. M. Marques, et al., "Methodology for the Reliability Evaluation of a Passive System and Its Integration into a Probabilistic Safety Assessment," *Nuclear Engineering and Design*, Vol. 235, p. 2612–2631 (2005).
13. L. Burgazzi, "Passive System Reliability Analysis: A Study on the Isolation Condenser," *Nuclear Technology*, Vol. 139, p. 3–9 (2002).
14. L. Burgazzi, "Evaluation of Uncertainties Related to Passive Systems Performance," *Nuclear Engineering and Design*, Vol. 230, p. 93–106 (2004).
15. L. Burgazzi, "Addressing the Uncertainties Related to Passive System Reliability," *Progress in Nuclear Energy*, Vol. 49, p. 93–102 (2007).
16. L. Pagani, G. Apostolakis, and P. Hejzlar, "The Impact of Uncertainties on the Performance of Passive Systems," *Nuclear Technology*, Vol. 149, p. 129–140 (2005).
17. F. Mackay, G. Apostolakis, and P. Hejzlar, "Incorporating Reliability Analysis into the Design of Passive Cooling System with an Application to a Gas-Cooled Reactor," accepted for publication in *Nuclear Engineering & Design*, available online May 29, 2007, http://dx.doi.org/10.1016/j.nucengdes.2007.04.006.
18. N. Saltos, et al., "A Risk-Based Margins Approach for Passive System Performance Reliability Analysis," *Progress in Design, Research, and Development and Testing of Safety Systems for Advanced Water Cooled Reactors: Proceedings of a Technical Committee Meeting*, IAEA-TECDOC-872, Piacenza, Italy (May 1995).
19. R. Vijuk, Letter to U.S. NRC Document Control Desk dated December 8, 2005, "Westinghouse AP1000 Design Control Document Revision 15 Errata." U.S. Nuclear Regulatory Commission ADAMS Accession Number ML053460400.
20. W. Beckner, Letter to W. Cummins dated September 13, 2004, "Final Safety Evaluation Report for AP1000 Design." U.S. Nuclear Regulatory Commission ADAMS Accession Number ML042540268.
21. U.S. Nuclear Regulatory Commission. *Official Transcript of Proceedings: Advisory Committee on Reactor Safeguards Subcommittees on Reliability and Probabilistic Risk Assessment*. Washington, D.C. (January 23, 2003). U.S. Nuclear Regulatory Commission ADAMS Accession Number ML030370746.
22. J. Kinsey, Letter to U.S. Nuclear Regulatory Commission Document Control Desk dated June 14, 2007, "Response to Portion of NRC Request for Additional Information Letter No. 3 Related to ESBWR Design Certification Application, RAI Number 19.1.0-1." U.S. Nuclear Regulatory Commission ADAMS Accession Number ML071920091.

23. U.S. Nuclear Regulatory Commission. *Probabilities of Failure and Uncertainty Estimate Information for Passive Components—A Literature Review*. NUREG/CR-6936. Washington, D. C. (May 2007). U.S. Nuclear Regulatory Commission ADAMS Accession Number ML071430371.

24. F. D'Auria, A. Del Nevo, and N. Muellner, Insights into Natural Circulation Stability, undated paper available on http://www.iaea.org/OurWork/ST/NE/NENP/NPTDS/Downloads/TECDOC_NC_WM/Annexes/Annex_08.doc.

25. International Atomic Energy Agency. *Natural Circulation Data and Methods for Advanced Water Cooled Nuclear Power Plant Designs: Proceedings of a Technical Committee Meeting Held in Vienna, 18–21 July 2000*. IAEA-TECDOC-1281. Vienna, Austria (April 2002).

26. V. A. Wichers, et al., "Testing and Enhanced Modeling of Passive Evolutionary Systems Technology for Containment Cooling (TEMPEST)," Presented at Fission Safety (FISA-2003) EU Research in Reactor Safety, Luxembourg (November 2003).

27. J. Hart, et al., "TEPSS—Technology Enhancement for Passive Safety Systems," *Nuclear Engineering and Design*, Vol. 209, p. 243–252 (2001).

28. J. Reves, *Natural Circulation in Water Cooled Nuclear Power Plants: Phenomena, Models, and Methodology for System Reliability Assessments*. DOE/ID/14550 (February 2005).

29. U.S. Nuclear Regulatory Commission. *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design*. NUREG-1793. Washington, D.C. (September 2004). U.S. Nuclear Regulatory Commission ADAMS Accession Number ML043570339.

30. *Technical Elements of a Risk-Informed, Technology-Neutral Design and Licensing Framework for New Nuclear Plants*. EPRI, Palo Alto, CA: 2006. 1013582.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California; Charlotte, North Carolina; and Knoxville, Tennessee, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together...Shaping the Future of Electricity

Program:

Technology Innovation

Printed on recycled paper in the United States of America

1015101

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com