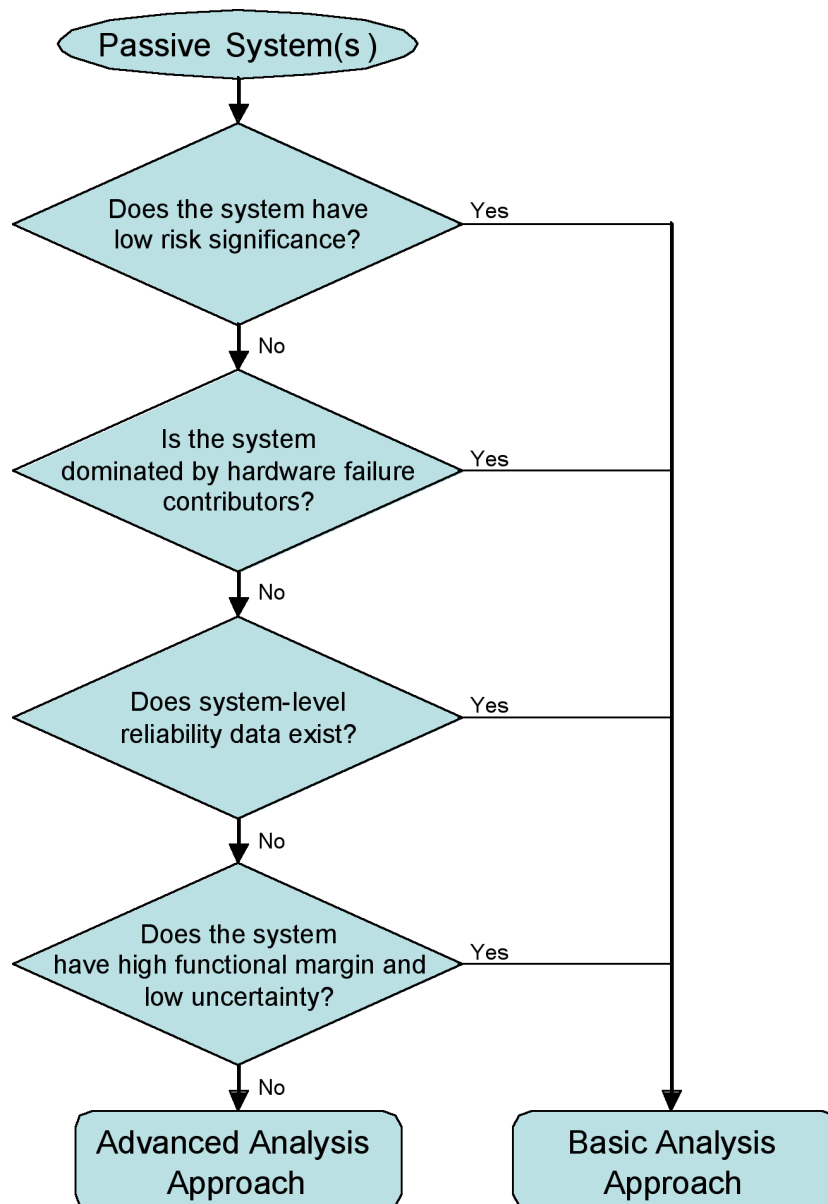


Program on Technology Innovation: Comprehensive Risk Assessment Requirements for Passive Safety Systems



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

1016747

Final Report, December 2008

EPRI Project Manager
S. Hess

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

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.

Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2008 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This report was prepared by

ERIN Engineering and Research, Inc.
158 West Gay Street, Suite 400
West Chester, PA 19380

Principal Investigator
E. Thornsberry

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

This publication is a corporate document that should be cited in the literature in the following manner:

Program on Technology Innovation: Comprehensive Risk Assessment Requirements for Passive Safety Systems. EPRI, Palo Alto, CA; 2008. 1016747.

PRODUCT DESCRIPTION

A key feature of the forthcoming generation of nuclear power reactors will be reliance on passive safety systems (PSSs)—those that rely on natural physical laws and require minimal or no intervention by plant operators. In 2007, preliminary findings summarized the current state of research into tools and methods that are capable of supporting probabilistic risk assessments (PRAs) for PSSs. These results and a recommended research plan for addressing the identified issues are presented in the Electric Power Research Institute (EPRI) report *Program on Technology Innovation: Probabilistic Risk Assessment Requirements for Passive Safety Systems* (1015101). The present report describes follow-on research that developed an approach to address the most complex and challenging of these issues—PSSs that are characterized by both high levels of safety significance and complex physical phenomenology.

Results and Findings

This report describes an approach to evaluate the reliability of PSSs that are characterized by high risk significance and high phenomenological complexity. This approach is designed to obtain estimates of PSS reliability that can be integrated into a plant PRA in a manner that is technically sound and resource-efficient. Follow-up research planned for 2009 will include a pilot demonstration of the approach on one or more PSSs likely to be deployed in the next generation of advanced light water nuclear reactors.

Challenges and Objectives

Because of the narrow operating margins associated with some PSS designs, uncertainty in system parameters can result in significant uncertainty as to the capability of the system to achieve its intended function. As a result of this uncertainty, situations have occurred where application of PSSs would not necessarily result in improved reliability compared with conventional active systems. Although methods exist to evaluate the phenomenological uncertainties, they constitute a brute force approach; they are labor-intensive, time-consuming, and expensive to perform. Although these techniques can be used to evaluate PSS reliability, at the design stage, they could significantly increase the expense and time required to perform required evaluations and thus impact proposed licensing schedules. During the plant operational phase, application of these methods will not address operational or emerging regulatory issues.

Applications, Value, and Use

This research is needed in order to support the deployment of advanced nuclear reactor technology that uses safety systems that are passive in nature. The approach described in this report will give plants the capability to perform an evaluation of PSS reliability and its impact on nuclear safety risk in a manner that is both resource-efficient and technically sound.

EPRI Perspective

The deployment of advanced nuclear generating technology is a critical element in ensuring a sustainable, cost-competitive, carbon-emission-free energy source. Because advanced nuclear technologies—including the next generation of light water reactors that are anticipated to be deployed over the next decade—use passive safety features as a cornerstone to enhance plant safety, it is essential that an adequate analytical framework exist to assess the risk impact of these systems. The research described in this report advances the state of the art in PRA technology by prescribing an approach to efficiently evaluate the reliability of PSSs that are characterized by high risk significance and high phenomenological complexity. It is anticipated that these methods will be important in demonstrating the high levels of safety inherent in advanced nuclear reactor technology. Also, it is anticipated that these methods will be a necessary component to support a risk-informed regulatory environment and decision making for these plants.

Approach

This project developed a formal, comprehensive analysis for PSSs that are characterized as possessing high risk significance and high phenomenological complexity. The approach builds upon research described in the literature to develop a process optimized for advanced light water reactor designs. The analysis framework consists of a structured search process to identify risk-significant scenarios that could challenge the design assumptions of plant PSSs. The process then assesses these scenarios for their effects on the functionality of the PSS. The likelihood of each scenario is then combined with the conditional failure probability of the PSS in order to determine the overall reliability of the PSS.

Keywords

Passive safety system (PSS)

Probabilistic risk assessment (PRA)

Thermal hydraulic analysis

ABSTRACT

A key feature of the next generation of nuclear power reactors is a reliance on safety systems that are passive; i.e. those that rely on natural physical laws and require minimal or no intervention by plant operators. However, due to the small operating margins associated with some PSS designs, uncertainty in system parameters may result in significant uncertainty in the capability of the system to achieve its intended function. Although methods exist to evaluate the phenomenological uncertainties, they constitute a “brute force” approach and, thus, are labor intensive, time consuming and expensive to perform. This project developed a formal comprehensive analysis approach to address the most challenging class of PSS; one that is characterized as possessing high risk-significance and high phenomenological complexity. The approach builds upon the previous research described in the literature to develop a process optimized for advanced light-water reactor designs. The analysis framework consists of a structured search process to identify risk significant scenarios that could challenge the design assumptions of plant PSSs. The process then assesses these scenarios for their effects on the functionality of the PSS. The likelihood of each scenario is then combined with the conditional failure probability of the PSS to determine overall reliability of the PSS. It is anticipated that these methods will serve as an important element to demonstrate the high levels of safety inherent in advanced nuclear reactor technology. It also is anticipated that these methods will be a necessary component to support a risk-informed regulatory environment and decision-making for these plants.

ACRONYMS

AHP	Analytical Hierarchy Process
ALWR	Advanced Light Water Reactor
ATHEANA	A Technique for Human Event Analysis
CATHARE	Code Avancé de Thermodynamique Appliqué aux Réacteurs à eau sous pression (Nuclear Safety Analysis Code for PWR)
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
ECCS	Emergency Core Cooling System
FMEA	Failure Modes and Effects Analysis
F-V	Fussell-Vesely
HAZOP	Hazard and Operability Analysis
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
I&C	Instrumentation & Control
ICS	Isolation Condenser System
LERF	Large-Early Release Frequency
LOCA	Loss of Coolant Accident
MAAP	Modular Accident Analysis Program
MSIV	Main Steam Isolation Valve
PRA	Probabilistic Risk Assessment
PSS	Passive Safety System
RAW	Risk Achievement Worth
RELAP	Reactor Excursion and Leak Analysis Program

RG	Regulatory Guide
SSHAC	Senior Seismic Hazard Analysis Committee
TH	Thermal-hydraulic
TRACE	TRAC/RELAP Advanced Computational Engine
TRACG	Transient Reactor Analysis Code – GE version

CONTENTS

1 INTRODUCTION	1-1
Purpose and Objectives	1-1
Background	1-2
General Approach	1-2
Ensure All Relevant Data Are Captured	1-4
Identify Potentially Important Scenarios	1-4
Identify Additional Calculations to Demonstrate Reliability	1-5
Quantification.....	1-5
2 ENTRY CONDITIONS FOR THE COMPREHENSIVE ANALYSIS APPROACH	2-1
Related Conclusions	2-1
Entry Conditions for Comprehensive Analysis	2-2
3 GUIDANCE FOR COLLECTION OF IMPORTANT INFORMATION	3-1
Related Conclusions	3-1
Approach for Collection of Important Information.....	3-2
System-Level Performance Data.....	3-3
Hardware Component Data (Including Multiple/Dependent/Common Cause Failures).....	3-4
Maintenance Data/Schedules.....	3-4
Support System Data	3-4
Phenomenological Calculations	3-5
Experimental Data	3-5
Expert Opinions	3-5
Unique Plant-Specific Conditions (Weather, Ultimate Heat Sink)	3-6
Potential Information Sources	3-6
4 GUIDANCE FOR IDENTIFICATION OF ACCIDENT SCENARIOS.....	4-1
Related Conclusions	4-1

Approach for Identification of Accident Scenarios.....	4-2
Identify the Objectives of the Analysis.....	4-3
Identify the Boundaries of the Analysis	4-4
Identify Potential Interactions with Other Systems	4-5
Define the Important Safety Function(s) for the Analysis	4-6
Define "Normal" Operation of the Passive System.....	4-6
Identify Potential PSS Failure Modes	4-8
Identify Traditional Failure Mechanisms That Could Cause a PSS Failure Mode to Occur	4-9
Identify Phenomenological Conditions That Could Cause a PSS Failure Mode to Occur	4-9
Identify PRA Scenarios That Deviate from "Normal" PSS Operational Assumptions.....	4-13
Identify Additional Deviations That the PRA Model Does Not Explicitly Represent.....	4-15
Sort PRA Scenarios by Risk.....	4-16
Identify the Important Scenarios That Can Challenge the Operation of the PSS	4-17
5 GUIDANCE FOR TARGETED PHENOMENOLOGICAL ANALYSES	5-1
Related Conclusions	5-1
Approach for Targeted Phenomenological Analyses	5-2
Identify and Categorize Gaps in Existing Information.....	5-2
Identify Approach to Close Each Gap	5-5
Define and Perform Necessary Phenomenological Calculations	5-6
6 GUIDANCE FOR QUANTIFICATION OF PSS RELIABILITY	6-1
Related Conclusions	6-1
Approach for Quantification.....	6-1
7 SUMMARY	7-1
8 REFERENCES	8-1

LIST OF FIGURES

Figure 1-1 Summary of comprehensive risk assessment process.....	1-6
Figure 2-1 Important issues for PSS reliability	2-3
Figure 2-2 Comprehensive analysis entry conditions flowchart	2-8
Figure 4-1 Schematic of generic isolation condenser	4-4
Figure 4-2 Conceptual fault tree for PSS failure	4-8
Figure 5-1 Categorizing gaps in the information	5-4
Figure 5-2 Successive analyses to reduce uncertainty.....	5-7
Figure 6-1 Conceptual fault tree for PSS failure	6-2
Figure 7-1 Summary of comprehensive risk assessment process.....	7-2

LIST OF TABLES

Table 4-1 Example of the guide word approach to identification of PSS failures	4-13
Table 4-2 Example PRA scenarios and failure conditions	4-18
Table 5-1 Classification of potential failure scenarios	5-3
Table 5-2 Examples of potential code parameters for phenomenological failures	5-9
Table 6-1 Example of quantification calculation	6-3
Table 6-2 Guidance for rough probability estimates	6-5

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. These systems typically rely on natural forces to achieve their designed safety objectives, resulting in smaller margins between system operating conditions and required success criteria. This is in contrast to many of the safety systems in current nuclear power plants that rely on electrical or pneumatic support systems. This combination of potentially reduced design margin coupled with the increasing use of probabilistic risk assessment (PRA) in the operation and regulation of nuclear power plants raises the issue of specifying appropriate PRA requirements for these passive safety systems (PSSs).

For many plant designs or systems that incorporate passive safety features, sufficient data often are not available to support obtaining detailed quantitative conclusions regarding the reliability of the passive safety systems. Additionally, the limited operating, testing, and experimental experience contains instances in which deviations from anticipated operation have occurred for some existing passive-type systems. Operating experience provides examples of foreign material obstructions [1], failure of control rods to fall under gravity [2], breaking of natural circulation due to stratification [2], and various latent human errors that disable or degrade nuclear systems [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.

A common belief related to advanced nuclear power plant designs is that reliance on passive safety systems will result in several advantages including 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. Due to 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.

During research conducted during 2007, we reviewed the state of the art associated with reliability analysis of PSSs, characterized issues related to performing these analysis and integrating them into a plant PRA, and developed a research plan to address these issues [4].

That plan proposed a graded approach to specify appropriate methods to analyze the PSS based on its characteristics:

1. Systems with Low Risk Significance AND Low Phenomenological Complexity
2. Systems with High Risk Significance OR High Phenomenological Complexity
3. Systems with High Risk Significance AND High Phenomenological Complexity

This research project will address the systems in category (3) for which innovative research is required to address the issue and meet industry needs. This report presents the initial development of a comprehensive analysis approach for passive safety systems in U.S. nuclear power plants. Follow-up research planned for 2009 will perform a demonstration of the process on one or more passive safety systems likely to deploy in the next generation of nuclear reactor construction in the United States. Based on results of the planned trial application, insights from the demonstration will be used to refine the comprehensive analysis approach for passive safety systems (if necessary).

Background

In the last several years, researchers have placed increased attention on the issues and techniques associated with PSS reliability. During 2007, preliminary research summarized the current state of research into tools and methods that are capable of supporting PRA analyses for passive safety systems [4]. The research culminated in a research plan to address issues associated with passive system PRA in a technically justifiable and cost-effective manner.

During 2007, initial research characterized the current state of tools and methods that are capable of supporting PRA analyses for passive safety systems. Due to the small margins associated with some PSS designs, uncertainty in system parameters may result in significant uncertainty in the capability of the system to achieve its intended function. As a result of this uncertainty, situations have occurred where application of PSSs would not necessarily result in improved reliability compared with use of conventional active systems. Although methods exist to evaluate the phenomenological uncertainties, they are a “brute force” approach and are very labor intensive, time consuming and expensive to perform. Although analysts can use these techniques to evaluate PSS reliability, at the design stage they could significantly increase the expense and time required to perform required evaluations and thus impact proposed licensing schedules. During the operational phase, application of the current technology most likely would not be sufficient to address operational or emerging regulatory issues.

General Approach

This project developed a formalized, comprehensive analysis approach for passive systems that our process characterizes as possessing high risk-significance and high thermal-hydraulic complexity. The approach builds 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. Previous research summarized in the 2007 report EPRI 1015101 [4], as well as recent

research performed in India [5, 6], has many aspects in common with the general approach developed here. However, due to differences in the types of systems, plant design, and regulatory environment, the research described in this report develops a comprehensive analysis approach intended to support PRAs of advanced light-water reactor (ALWR) designs under the current U.S. nuclear regulatory regime.

The comprehensive analysis approach will inductively identify scenarios where a passive system would be most susceptible to a failure that would increase the overall risk of the plant. The goal of the approach is 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 utilize 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 comprehensive analysis approach is to estimate the failure probability for passive systems. This probability could result from a combination of different scenarios that present different challenges to the passive system under evaluation. Where necessary, the analyst would subdivide scenarios defined by the PRA to allow for a more detailed analysis. For scenarios where the boundary conditions and environment are within the design envelope of the passive system, the probability of failure would be very low (and even negligible when other dominant failure scenarios exist). For scenarios that could exceed the boundaries of the design envelope, the analysis could either assume a conservative system failure probability of 1.0, or perform further analysis to refine the scenario and/or reevaluate passive system performance. The overall failure probability of the passive safety system then is obtained as the sum over all scenarios of the probability of each scenario multiplied by the conditional probability of PSS failure given each scenario.

Such an approach requires a more subjective view of probability and reliability. Because a passive system cannot be exhaustively tested for all possible operating conditions and accident scenarios (both within its design assumptions and beyond those assumptions), it is not possible to utilize a purely objective approach to probability. That is, one would not employ the objective frequency definition of probability in which m failures in n trials produces an estimated failure probability of m/n . Instead, a more subjective, or “degree of belief,” approach will be used. In this approach, the analyst can incorporate non-numerical information such as isolated failures, partial failures, near-failures, and expert opinion into the reliability assessment process. This approach is not unusual in the field of PRA, but it is important to recognize its use in applications such as this.

The general concept of the comprehensive analysis framework will consist of a structured search process to identify scenario deviations that challenge the design assumptions of the passive system(s). The process will then assess these scenarios for their effects on the functionality of the passive system. The analyst then combines the likelihood of each scenario with the conditional failure probability of the passive system given the scenario to determine the overall PSS reliability.

In addition to failure of the passive system to fulfill its function due to phenomenological failures, the analyst must consider typical component-related failures. Hardware failures that could affect the phenomenological function of the passive system, such as vent valve operation to remove noncondensable gases from a system, could affect both aspects of the analysis.

Thus, the comprehensive analysis approach consists of several high-level steps, which are briefly described below and expanded in the sections that follow. Figure 1-1 depicts the overall flow of the analysis process, which proceeds from top to bottom. However, the analyst must recognize the important interactions between the quantification steps and key identification steps early in the process. Thus, the process is iterative and the analyst will likely need to use initial probability estimates during the early steps of the analysis, and refine them later, as necessary.

Ensure All Relevant Data Are Captured

First, the analyst must obtain any relevant data regarding components of the PSS, its actuation hardware, and its support systems and evaluate it for inclusion in the PRA. If it exists, relevant system-level performance data provides a rough estimate of the failure probability of the system due to phenomenological issues. In addition, data from similar operational systems may help assess the potential for natural circulation failure, even if the systems and applications are not identical. Section 2 discusses how to use the available information to determine whether the passive system meets the “Entry Conditions” to require a comprehensive analysis approach. Section 3 provides further guidance for collecting important forms of information for the comprehensive risk assessment process.

Identify Potentially Important Scenarios

To determine the overall reliability of the passive system, the analyst must know the characteristics of both the passive system and the accident scenarios to which it may need to respond. The characteristics of the passive system follow from the important parameters that govern its operation. The PRA defines the accident scenarios in which the passive system must function. The search process will examine these characteristics in order to identify scenarios that may challenge the design parameters and any other assumptions inherent to the operation of the passive system. Once these scenarios are identified, they can be examined to determine both the likelihood of the scenario occurring and the likelihood that the passive system can perform its function under the specific conditions of the scenario. For most scenarios within the design basis of the plant and the passive system, the probability of failure should be very low. However, for beyond-design-basis scenarios within a PRA, the passive system may or may not be able to function adequately to achieve its safety function. In some of these cases, information from the design, testing, or operation of the passive system or similar systems may be necessary to provide sufficient evidence to estimate the failure probability of the passive system. Section 4 provides further guidance for identifying potentially important scenarios.

Identify Additional Calculations to Demonstrate Reliability

If available design-basis calculations and other information do not provide an adequate basis for evaluating all the potential scenarios, additional phenomenological calculations may be required to determine the behavior of the passive system during unusual situations. Though some approaches to PSS reliability utilize a large number of complex calculations, this process will guide the analyst to develop a limited number of “targeted” phenomenological calculations to fill gaps in the existing information base. If needed, these calculations should use best-estimate assumptions and computer codes to ensure high confidence in their results. Section 5 provides further guidance for identifying and performing additional phenomenological calculations.

Quantification

As stated previously, the overall failure probability of the passive safety system is the sum over all scenarios of the probability of each scenario multiplied by the conditional probability of PSS failure given each scenario occurs.

$$\Pr(PSSfailure) = \sum_{allscenarios} \Pr(scenario) \times \Pr(PSSfailure | scenario)$$

The analyst may assign the failure probability for each scenario through the use of operational data, experimental data, phenomenological calculations, expert opinion, and/or conservative assumptions. Section 6 provides further guidance for the quantification process.

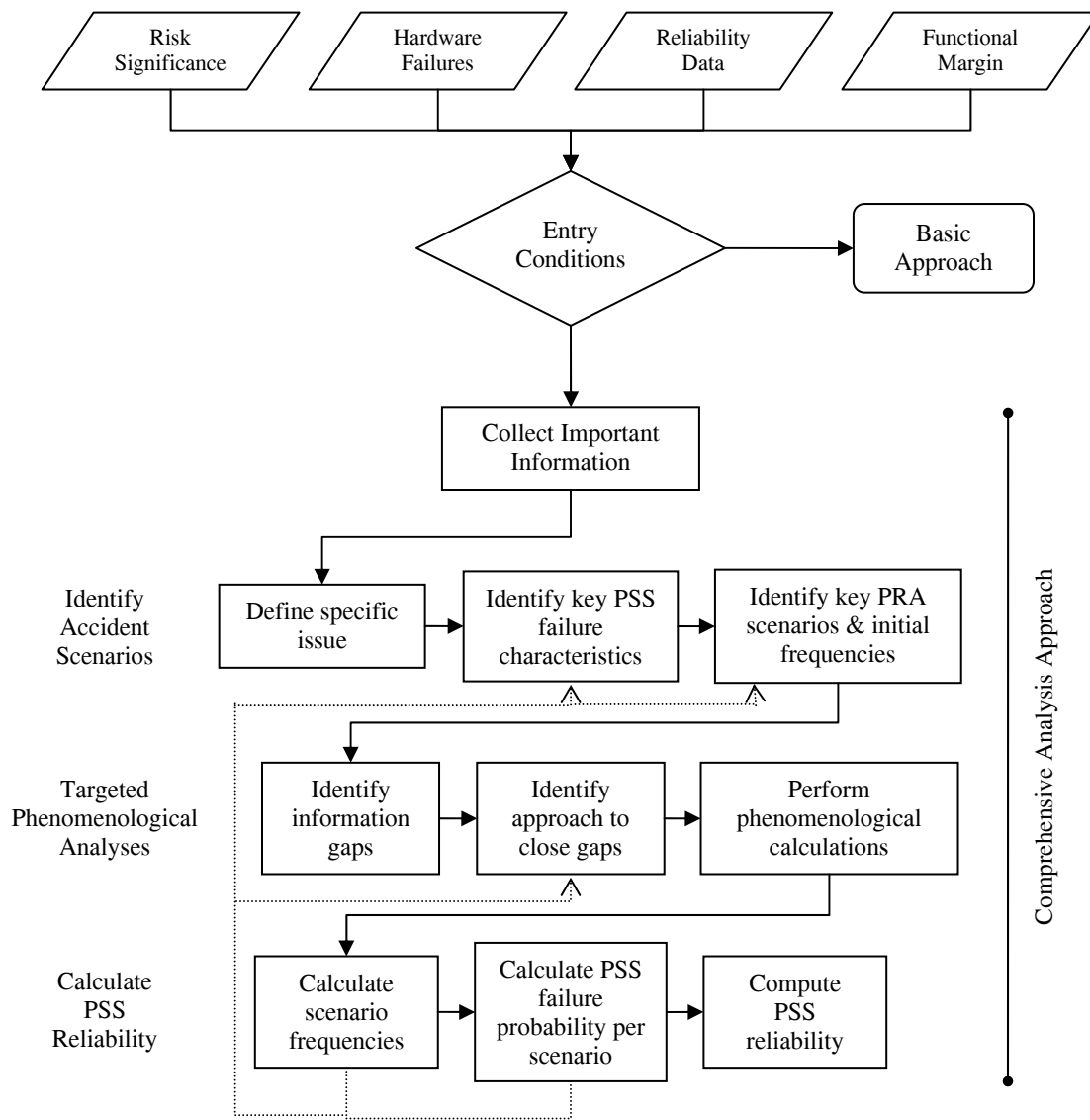


Figure 1-1
Summary of comprehensive risk assessment process

2

ENTRY CONDITIONS FOR THE COMPREHENSIVE ANALYSIS APPROACH

The purpose of this task is to describe the characteristics of passive systems that indicate that the system may require a more comprehensive approach to evaluating system reliability. This task fulfills part of Task 1 described in EPRI 1015101 [4], which identified the need to develop a formal categorization and screening process for all passive systems to determine (1) whether a passive system requires a formal reliability analysis and (2) for those that do, what level of analysis it requires. For passive systems of concern (i.e. IAEA Category B systems [7]), considerations for categorizing these passive systems include the working fluid involved (i.e. water, helium, etc.), the availability of failure data for similar systems (such as an isolation condenser), and whether the system requires actuation by other (active) 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 requires a basic analysis process or a more comprehensive approach. The decision criteria should 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.

Related Conclusions

A number of the conclusions from the EPRI 1015101 [4] report relate to this task.

- 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 thermal-hydraulic parameters, analysis of their reliability should include consideration of a broader range of failure mechanisms, including mechanisms that may provide significant impact on the phenomenology and functional margins.
- 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 are also likely to function in a robust fashion so long as the means provided for purging noncondensable gases function as designed.
- 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 current state-of-the-art.

Passive components or systems are always part of a larger context to 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; for applications to ALWRs this can be represented by the conventional measures of nuclear safety risk (e.g., core damage frequency [CDF] and large early release frequency [LERF]). 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. For these cases, a straightforward process should be sufficient to evaluate the system's impact on safety.

The reliability of a PSS depends upon both the integrity of its components and its ability to function under all required conditions. Though modern passive safety systems greatly reduce the number and complexity of components such as valves and pumps, some components may still exist depending on the system design. Therefore, the assessment must consist of both the classical reliability analysis of any components and the evaluation of the passive function. The evaluation of the passive function may itself involve classical reliability analysis of other systems designed to ensure conditions conducive to success of the passive system. In addition, an integrated modeling approach that crosses normal system boundaries may be necessary to characterize the complete phenomenological spectrum. Such capability is achievable within the current state-of-the-art.

Because passive systems eliminate some of the dominant failure mechanisms seen in active systems, different failure mechanisms likely will 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. 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 solely on active components that lead to these types of failure mechanisms, though this may be rare. Only when these functional reliability aspects decrease to levels comparable to or below the phenomenological reliability, must the reliability analysis focus on the phenomenological performance of the passive system in detail.

Entry Conditions for Comprehensive Analysis

The entry conditions necessary to specify the performance of a comprehensive analysis should follow from these conclusions. If a passive system, or set of passive systems, is insignificant to risk or existing analysis techniques capture the dominant contributors to its reliability, then the use of a more traditional, straightforward approach is justified. However, if the system or systems appear to be susceptible to one or more of the larger concerns expressed above, a more comprehensive reliability analysis method is necessary.

The issues of concern for the reliability of passive systems all relate to three overarching issues: risk significance, functional margin, and uncertainty. Figure 2-1 shows the interaction of these three attributes depicted as a Venn diagram. This representation provides a useful visualization to show the concept of the graded approach to the reliability analysis/risk assessment of PSSs described in EPRI 1015101 [4] and summarized in Section 1 of this report. Thus, a

comprehensive analysis should only be required for those systems whose characterization causes them to fall within the intersection of all three attributes (i.e. each attribute is significant for the evaluation of system reliability).

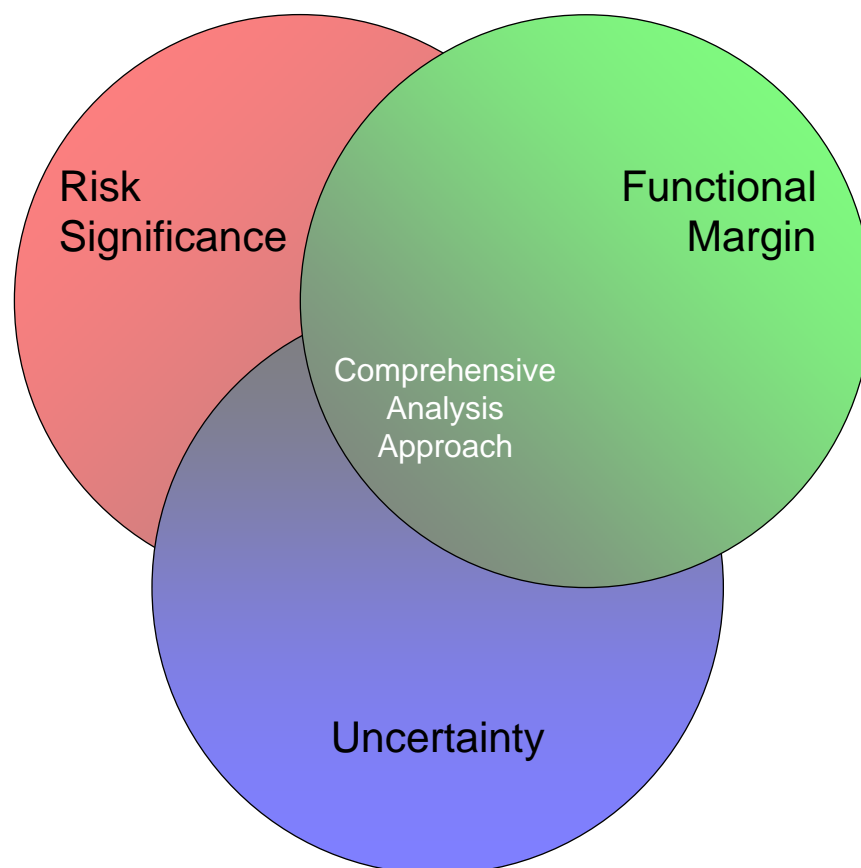


Figure 2-1
Important issues for PSS reliability

In this scheme, the risk significance issue precedes the other factors, such that if a passive system or component would not significantly affect the overall plant risk (as measured by CDF and LERF), the other questions are irrelevant. However, if the passive system does not screen out solely on the basis of risk significance, the importance of functional margin becomes the primary concern. The 2007 report (EPRI 1015101 [4]) identified three contributors to functional margin: PSS capabilities, scenario characteristics, and modeling capabilities. The combination of these three contributors will define the level of functional margin that exists in the passive system, and thus the importance of the reliability of the system to plant safety risk. If the functional margin is low relative to the uncertainty in the functional margin, the analyst should utilize the comprehensive analysis approach. Uncertainty has the capability to affect both functional margin and risk significance, such that sufficient uncertainty in both factors may be able to create the need for an in-depth analysis of reliability, even though the best estimate based on these factors indicates sufficient functional margin.

The entry conditions for the comprehensive analysis utilizes these overarching issues as well as the specific contributing factors to identify when a passive system would require a comprehensive reliability assessment. A number of questions will guide the determination of the required analysis level. The following outline and the flowchart in Figure 2-2 depict the general structure of the process.

- Risk Significance
 - Low risk-significant systems or components will not require in-depth analysis of reliability.
- Functional Margin
 - PSS Capabilities
 - New failure modes or failure modes that may increase in likelihood compared with an active system increase the need for a comprehensive evaluation approach.
 - Reliance of the system on traditional (well-understood) components for actuation or continued operation decreases the importance of the uniquely passive aspects of the system.
 - Modeling Capabilities
 - Industry experience in the modeling and operation of similar systems or phenomenological processes reduces the need for a comprehensive evaluation.
 - Availability of system-wide and component failure data also reduce the need for a comprehensive evaluation.
 - Scenario Characteristics
 - Unique scenarios that may present considerable challenges to the passive system will require comprehensive evaluation.
- Uncertainty
 - Interaction of other active and passive systems may affect the operational conditions of the passive system.
 - Large or unknown uncertainties may degrade the amount of functional margin and require a more comprehensive assessment of reliability.

The examination process can begin with a single passive system or a group of related passive systems. If multiple passive systems have a high level of interaction, they should initially undergo analysis as a group, though it may be possible to analyze them separately later.

Four high-level questions capture the important issues that identify systems that require the comprehensive analysis approach.

Does the system have low risk significance?

Risk significance has several different types of measures in use in other applications that we could adopt for use in screening passive systems. For relatively well-understood passive systems that use water as the heat transfer medium, the criterion for low risk significance should coincide with low-risk indicators from these other existing applications. For less-well-understood gas-based systems that may have higher uncertainties, the criterion for low risk significance may need to be set at a lower level than for water-based systems.

With the increased use of risk-informed applications during recent years, the definition of risk significance has been an important issue. Applications such as Regulatory Guide 1.174, Special Treatment Requirements (10CFR50.69/RG 1.201), and the Maintenance Rule (10CFR50.65/RG 1.160) provide accepted approaches for determining risk significance for specific purposes. These applications should provide good models for the definition of passive system risk significance.

The Maintenance Rule's risk significance criteria could be one example adapted to determine the risk significance of passive systems. For an initial screen at the system level, we recommend the use of relative criteria with values similar to the Maintenance Rule: Risk Achievement Worth (RAW) > 2, Fussell-Vesely (F-V) > 0.5%, and cutsets in top 90%. Because these measures provide a relative ranking, their application does not depend on the specifics of the reactor design. Thus, these metrics remain a valid measure of the system's risk importance for both current and advanced light water reactor designs.

With such measures, the same cautions apply as with their current use. For example, if the reliability of the PSS is overestimated (or highly uncertain), the F-V importance measure criterion and top 90% cutset criterion may not accurately account for the PSS and its components. Thus, these measures may not be adequate for determining the risk significance of the PSS. However, use of RAW to determine the risk significance does not mask the uncertainty in the reliability of the passive systems. In these cases, the analyst should calculate RAW explicitly (i.e., set system failure to 1.0 or TRUE) since RAWs for very reliable systems can be underestimated significantly if the analyst just evaluates cutsets. The analyst should also be sure to account for any common cause effects among passive systems during the risk screening process.

Do hardware failure contributors dominate the system?

Many types of passive systems retain some limited amount of physical hardware or actuation subsystems, such as various types of valves or actuation circuitry that must function in order for the passive system to achieve its mission. Particularly if multiple components must function, the failure rates of these components may dominate the failure probability of the passive system under many or all circumstances. These components may screen out of traditional PRAs due to their low contribution relative to more common active system failures, but they may take on greater importance in passive systems. The analyst should pay particular attention to the potential for new or different failure mechanisms within the passive system that could affect the functionality of these components or of the overall passive system. The criterion for this question should be set such that there is high confidence that the phenomenological uncertainties would not create a failure probability greater than the criterion.

The overall reliability of the passive system will be the combination of the reliability due to any traditional hardware failures and the reliability due to phenomenological reasons (captured by functional margin). If non-negligible traditional hardware failures exist in the passive system and the system meets common high-quality design standards, the traditional hardware failures likely would dominate the reliability, and a comprehensive analysis approach would not be necessary. In other words, if any phenomenological failures are likely to be negligible in comparison to hardware failures, only a simple analysis should be necessary.

Does system-level reliability data exist?

Some passive systems, such as isolation condensers, may have sufficient similarity to existing passive systems that existing operational data may be suitable to estimate the system's overall failure probability. However, the analyst should pay careful attention to potentially different scenario characteristics that the new system could encounter to ensure that the data from the existing systems is appropriate for the application under consideration. If existing operational data is appropriate, only a simple analysis should be necessary.

Does the system have high functional margin and low uncertainty?

The exact criterion for this question may be difficult to define explicitly. The purpose of this question is to capture those more complex systems where the design, while strictly acceptable, may be susceptible to failures that could occur due to small changes in its operating environment. This contrasts with the large majority of active systems, which typically have such high functional margin that the effect of most small uncertainties is negligible. However, if the passive system performance has significant uncertainties that can degrade its functional margin, the system should be subject to the more detailed analysis method.

Here, we use lessons from the 2007 EPRI 1015101 report [4] to guide the judgment for addressing this question. For example, 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; so such a system may not require the comprehensive analysis method. On the other hand, water-based designs with innovative features or gas-based systems may have less functional margin or more uncertainty regarding the amount of such margin; in which case the comprehensive analysis approach may be required.

Characteristics that indicate phenomenological complexity include:

- Use of natural circulation with small driving forces (i.e., small pressure differences, low temperature differences, etc.),
- Use of gas as the working fluid (due to, for example, their lower thermal conductivities),
- Low driving pressure for the working fluid,
- Susceptibility to blockage, including by external debris, noncondensable gases, or internal pipe fouling/corrosion,
- Susceptibility to decreased heat transfer by pipe fouling/corrosion,

- Susceptibility to minor failures that could compromise system integrity (e.g., leakage from the system that could divert or negate required flow),
- Potential for changes to the expected flow phase (e.g., transition to two-phase flow when single-phase flow is expected),
- Dependence on stratification within a pool, and
- Dependence on phenomenological conditions influenced by other systems (e.g., passive containment cooling system dependencies or containment conditions that may be affected by other systems located within containment).

Note that none of these characteristics, by themselves, necessarily indicates a high level of phenomenological complexity. Such characteristics are an integrated part of determining whether the system has enough phenomenological complexity or phenomenological uncertainty such that the analyst must use the comprehensive analysis approach to obtain a robust estimate of the reliability of the passive system.

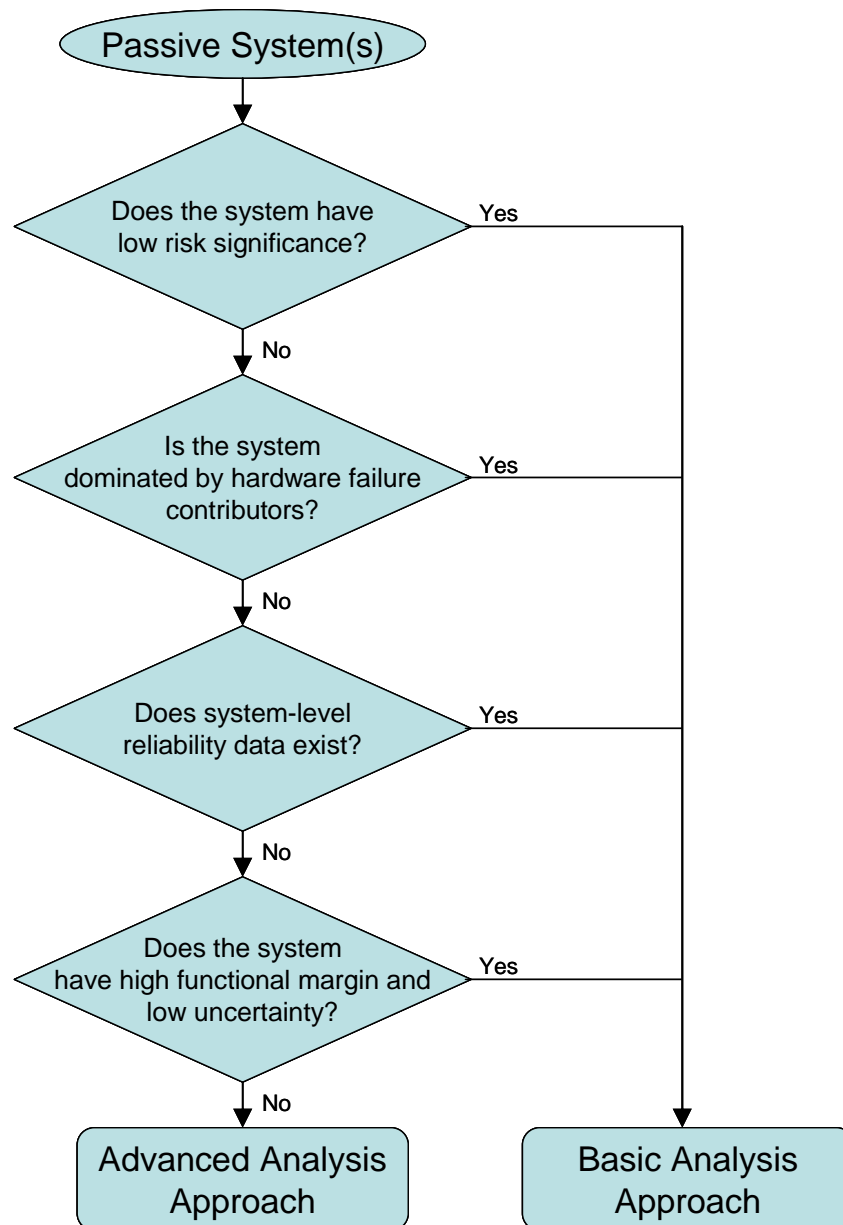


Figure 2-2
Comprehensive analysis entry conditions flowchart

3

GUIDANCE FOR COLLECTION OF IMPORTANT INFORMATION

The purpose of this task is to provide guidance regarding the initial collection of important and useful information from various sources for the comprehensive analysis approach. Because passive systems can vary in design and available information, it is difficult to define a list of “necessary” information. While some minimum set of information is required, there is no one piece of data that is absolutely necessary. Logically, the availability and quality of information will directly affect the quality and uncertainty of the resulting analysis. It will also affect the effectiveness and efficiency of the analysis, as the analyst will need to remedy any critical gaps in the available information later in the process.

All relevant data regarding components of the PSS, its actuation hardware, and its support systems should be included in the assessment of passive system reliability. If it exists, relevant system-level performance data may provide an estimate of the failure probability of the system due to phenomenological issues. For example, the analyst may examine data from similar operational systems to determine potential causes of natural circulation failure that do not appear in other component-related data. Other sources of data, such as from mockup system testing, also will play an important role in estimating PSS reliability. The sections below discuss the various types of information that may be available and how each type of data may be useful. Note that in addition to obtaining an estimate of the PSS reliability, an important additional element in the analysis will be to provide some measure of confidence in the estimate obtained; this will be determined, to a great extent, by the amount and quality of available data.

Related Conclusions

A number of the conclusions from EPRI 1015101 [4] relate to this task.

- 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 thermal-hydraulic parameters, analysis of their reliability should include consideration of a broader range of failure mechanisms, including mechanisms that may provide significant impact on the phenomenology and functional margins.
- While 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 assure safety. This provides additional assurance of a reliable system, particularly for advanced light-water reactor designs operated under the current regulations.
- Existing PRA approaches and approved TH analysis codes can address many issues related to PSS functions in advanced light-water reactor designs.

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, and such information will be important to an analysis of PSS reliability. Depending on the system design and availability of data, the analyst may be able to identify traditional (active) component failures that lead to or contribute to these types of failure mechanisms. For example, if operation of a valve is necessary to purge noncondensable gases from a system, failure of that valve (an active component) should appear in the analysis, since its failure would increase the likelihood of functional failure of the PSS.

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 system components and evaluation of the passive function itself. This evaluation of the passive function may involve classical reliability analysis of other components designed to ensure conditions conducive to success of the passive system and/or evaluation of the fundamental physics of the processes (e.g. heat transfer mechanisms or fluid flow regimes) to identify conditions under which the system would not be capable of successfully performing its intended function. Therefore, all information related to classic reliability estimates of system components and information related to the phenomenological operation of the passive system or similar systems will be important to this analysis.

Approach for Collection of Important Information

The initial collection of important information for the comprehensive analysis should follow from these conclusions. That is, it will be important to gather not only system-specific information, but also general plant performance information in order to assess the system in the proper operational context. The information gathering task will not differ greatly from that performed for typical PRA applications, but some of the special characteristics of passive systems could modify the focus of some of the information needs. This task outlines the initial information collection process; later in the analysis process, the analyst may need to identify additional analysis-specific data to evaluate PSS reliability. It is important to note that the information collection process should incorporate both success and failure information for the operation of the passive system(s), as the information will provide the basis for defining both the expected operation of the system and potential deviations from normal operation.

In general, the analysts should collect two different types of data. Event descriptions would capture the details of failures of passive systems or components with the goal of identifying failure mechanisms that are unique to the passive system. This collection of identified failure mechanisms would ensure that the passive systems analysis properly considers 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 for the successful operation of PSSs. Once collected, this data would provide an improved basis for estimating failure probabilities in the PSS reliability evaluations.

The specific types of useful information should include those listed below. For some passive system applications, some categories of information may not exist. When this is the case, the analyst will need to evaluate the impact of the lack of this information. In those situations where the information is necessary to perform an adequate assessment of PSS reliability, Section 5 provides additional guidance regarding appropriate alternative methods to obtain the data (e.g. expert elicitation). As a general rule, the greater the breadth and depth of available information, the more efficiently the comprehensive analysis approach will be able to determine the reliability of the passive system.

System-Level Performance Data

Obviously, system-level performance data will be the most directly applicable to the estimate of passive system reliability. The information gathering process should collect direct operational data from similar systems in other nuclear power plants and assess the applicability to the system under assessment. In some cases, data from non-nuclear or non-commercial nuclear applications may also be useful. The applicability of the data will depend on a number of factors, including operating environment, specific system design parameters, operational parameters, and operational philosophy. At best, operational data from similar systems may be able to provide a direct estimate of PSS reliability. In many cases, though, system design and operational differences may not allow a direct estimate, but the data should still provide a general estimate of overall reliability, important components, and important phenomenological conditions. The analyst then can use such operational data from similar systems to develop a starting point for the analysis. In addition to collecting direct objective failure data, this task should include obtaining other subjective information regarding system operation, tendencies for failures or unexpected operation, and the basis for any changes to the system or its operation since its installation.

One example of a system that may be amenable to this type of information collection is the isolation condenser system. Some nuclear power plants have used similar systems for many years. Important information may include actual operation during potential emergencies (if any), thermal-hydraulic operational characteristics, changes in those characteristics over years of operation, regulatory issues related to the system, and maintenance records that could indicate unexpected changes in the assumptions necessary for system operation.

Hardware Component Data (Including Multiple/Dependent/Common Cause Failures)

The gathering of hardware component data should be the most straightforward information-gathering task. A plant PRA should already include failure data for many of the hardware components that may be present in a passive system, including check valves, relief valves, heat exchanger failure/plugging, battery failure, and electrical circuit failures. However, it is essential to note that an important part of this data collection activity is to evaluate the relevance of the data for application to the particular PSS under evaluation. One such element of this evaluation is the identification of any important differences between the assumptions/conditions under which the data were obtained and the operational characteristics of the system being studied. As an example, in the evaluation of the likelihood of heat exchanger failure/plugging, one should consider the potential differences between the conditions applicable to the component failure data and the conditions in the passive system (such as potentially lower system flowrates or differential pressures). Another example involves solenoid valves that need to de-energize in order to function within a passive system, though the available data may include both “failure to energize” and “failure to de-energize,” therefore overestimating the failure probability. For components that are new to nuclear power plants or that take on increased importance by their use in passive systems, hardware failure data may be more difficult to acquire. Explosive squib valves are one example where the analyst may need to search other sources of hardware component data or obtain an estimate via other methods (e.g., expert elicitation).

Maintenance Data/Schedules

Due to the potential sensitivity of passive systems to minor variations in their operational environments, information from maintenance activities may provide a valuable source of data to identify potential failure mechanisms and their frequency. Important maintenance information could include such activities as valve maintenance, pipe cleaning, chemistry adjustments, and other expected or unexpected activities that affect the assumptions and conditions necessary for proper system operation. For example, if maintenance logs indicate that debris must be cleaned from a pool regularly, this could indicate the potential for changes in natural circulation or heat transfer characteristics. If the design and operational assumptions for the system do not adequately address these changes, they could adversely affect the reliability of the passive system.

Support System Data

The most common support systems for passive safety systems include electrical power (usually DC), air/nitrogen supply (for pressure differential), and instrumentation and control systems. Within the PRA, application of modern methods should be able to address any contribution by support systems and incorporating these elements into the passive system reliability analysis should be straightforward. However, information regarding any support systems will be important to the analyst to help determine potential failure modes and the importance of the passive system functional reliability. That is, if failure due to one or more support systems is sufficiently high, it may reduce the effort required for analysis of the passive system function since failures of the support systems may dominate the reliability of the passive system.

Phenomenological Calculations

Information and data from phenomenological calculations will provide the backbone for the comprehensive analysis approach for passive safety system reliability. Three general types of phenomenological calculations will be useful. First, design-basis calculations for regulatory purposes will provide an indication of the effects of many types of calculational and operational uncertainty. Because these calculations use conservative assumptions and calculation methods, they provide confidence in the operation of the PSS over a wide range of conditions. For example, these conservative design-basis calculations typically eliminate the need to consider many of the parameter variations that may create uncertainty in a best-estimate calculation. Second, best-estimate calculations for design and operational purposes will provide important information to identify key variables, key assumptions, and the sensitivity of PSS operation to those characteristics. Third, best-estimate phenomenological calculations that push the PSS to failure will provide important insights into any vulnerabilities of the passive system. This third set of calculations may not exist or may be more difficult to produce. Note that the definition of these three groups is not mutually exclusive – some calculations may fit into more than one category. The important aspect for collecting information from phenomenological calculations is to capture operational characteristics, sensitivity to variations, limitations of the design, and the means by which the system could fail to adequately perform its intended function.

Experimental Data

Closely related to phenomenological calculations is experimental data. The scope of applicable experimental data should be as broad as possible. The most obvious source of experimental data will be from the design and licensing process. The challenge regarding experimental data for modern nuclear power plant designs is the decreased availability of such information. Even during a full design and licensing process, the amount of experimental data may not be as great as desired due to the increased use of computational techniques and the high cost of experimentation. However, other sources of experimental data may be useful, particularly for the purposes of examining PSS behavior under unexpected conditions. The analyst also could collect experimental data from similar, but not necessarily identical systems (if available) to aid in the analysis.

Expert Opinions

Despite the capabilities of computational tools and analysis techniques, expert judgment also may be required to aid in the assessment of PSS reliability, particularly if large gaps exist in the other categories of information. The gathering of expert opinion should include both the gathering of documented expertise (e.g., previous, related analyses) and the gathering of available experts to assist with the analysis. Because passive system performance may include state-of-the-art technologies, a multi-disciplinary approach may be necessary for the analysis. Expertise in thermal-hydraulics, risk analysis, instrumentation and control, electrical engineering, and related disciplines may be necessary.

Unique Plant-Specific Conditions (Weather, Ultimate Heat Sink)

As discussed in EPRI 1015101 [4], it appears likely that passive safety systems may have a wide range of susceptibilities that may produce unique failure mechanisms. For example, the use of passive safety systems could introduce unique issues due to the specifics of their construction, operation, or environment. Some examples include rapid weather changes, the effects of salt-water environments, biofouling of heat exchangers, or chemistry management. These types of atypical effects may only occur on a plant-specific basis, so any unique plant-specific design, operational, or environmental conditions should appear in the analysis. The analyst should identify information related to unusual weather conditions, unusual geological conditions, unusual environmental conditions, unique plant and animal life, and unique design or operational conditions for analysis later in the process.

Potential Information Sources

The types of information discussed above may or may not be readily available depending on the system under review and the state of the system in its design/licensing/operational life cycle. When the comprehensive analysis is conducted early in the life cycle, less directly applicable information will be available, and the analyst must expand the search for useful information. In these cases, it is important to remember that information from similar systems in other plants or in non-nuclear applications would be valuable. Though not an exhaustive list, information may occur in sources such as:

- Plant reports (i.e., incident reports, maintenance reports, etc.)
- Industry reporting systems (including precursor reports)
- Design calculations (from vendor and/or architect-engineer)
- Licensing calculations (e.g., design certification)
- Experimental reports (from vendors, research institutions, etc)
- Manufacturer data (particularly for component-level data)
- Non-nuclear application data (via manufacturer or other industry organizations)

4

GUIDANCE FOR IDENTIFICATION OF ACCIDENT SCENARIOS

The purpose of this task is to provide guidance regarding the identification of important accident scenarios for the passive system. To determine the overall reliability of the passive system, the analyst must know the characteristics of both the passive system and the accident scenarios for which it must provide mitigation capability. The important characteristics of the PSS follow from the key parameters that govern its operation. The PRA defines the accident scenarios in which the passive system must function. The search process will examine these characteristics in order to identify scenarios that may challenge the design parameters and any other assumptions inherent to the operation of the passive system. Once the scenarios (and their constituent parts) are identified, they can be examined to determine both the likelihood of the scenario occurring and the likelihood that the passive system can perform its function under the specific conditions of the scenario.

The search process provides guidance to identify and examine:

- Key phenomenological parameters affecting the operation of the PSS
- Key environmental/operational conditions important to the PSS
- Key assumptions of the design and operation of the PSS
- Risk-important scenarios within the PRA where the PSS provides important mitigation capability
- PRA scenarios that challenge any of the above bases

The process described in this section provides guidance to the analyst. It is not a strict step-by-step procedure, but requires interaction among some of the steps and iterations between steps in order to produce a complete, but efficient, identification of accident scenarios. The output of the process is a list of accident scenario-failure condition pairs that could challenge the successful operation of the subject passive safety system or systems.

Related Conclusions

A number of the conclusions from EPRI 1015101 [4] relate to this task.

- Because passive systems are likely to be more sensitive to variations in thermal-hydraulic parameters, analysis of their reliability should include consideration of a broader range of failure mechanisms, including mechanisms that may provide significant impact on the phenomenology and functional margins.
- Existing PRA approaches and approved TH analysis codes can address many issues related to PSS functions in advanced light-water reactor designs.

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, and the analyst should consider them for this analysis.

Approach for Identification of Accident Scenarios

The identification of important accident scenarios for the comprehensive analysis should follow from these conclusions. That is, it will be important to identify all of the important phenomenological parameters, environmental and operational conditions, and design assumptions affecting the operation of the PSS. The search process must be very broad in order to capture all potential failure mechanisms

Passive safety systems should have very high reliability under “normal” operating conditions (i.e., within their design envelope with no external disturbances). Therefore, it is important to recognize that the purpose of this approach is not merely to calculate the failure probability of the PSS under “normal” conditions, but rather to identify and analyze those unexpected conditions and situations where the likelihood of PSS functional failure becomes significant.

The search process will utilize the following general outline of tasks:

- Define the specific issue
 - Identify the objectives of the analysis
 - Identify the boundaries of the analysis
 - Identify potential interactions with other systems
 - Define the important safety function(s) for the analysis
 - Define “normal” operation of the passive system
- Identify key PSS failure characteristics
 - Identify potential PSS failure modes
 - Identify traditional failure mechanisms that could cause a PSS failure mode to occur
 - Identify phenomenological conditions that could cause a PSS failure mode to occur
 - Identify traditional failures in related systems that could lead to the phenomenological failure condition
 - Identify abnormal conditions that could lead to the phenomenological failure condition

- Identify key PRA scenarios with potentially unexpected conditions that can affect the likelihood of PSS failure
 - Identify PRA scenarios that deviate from “normal” PSS operational assumptions
 - Identify additional deviations that may not be explicitly represented in the PRA model
 - Sort PRA scenarios by risk importance
 - Identify the important scenarios that can challenge the operation of the PSS

The discussion below provides guidance for each task and subtask. Throughout the discussion, a hypothetical example illustrates how the guidance applies to a specific situation.

Identify the Objectives of the Analysis

To begin the analysis of passive system reliability, the analyst must clearly define the specific objectives of the analysis. As with all applications of PRA, passive system reliability analyses may have different purposes that will require slightly different approaches. The guidance in the following sections should apply broadly, regardless of the specific application, but the analyst should implement it with a thorough understanding of the objectives of the analysis. Potential overall objectives could range from a complete plant PRA (or significant update) to the investigation of a particular PRA-related issue.

In the following sections, we illustrate the approach using a hypothetical example application. In this example, we will assume that a plant wishes to reassess the reliability of their isolation condenser system in order to modify the operational controls (e.g., technical specifications) regarding the system based on a risk-informed approach. The isolation condenser provides a good example due to its use in some currently operational U.S. nuclear power plants, its inclusion in the design for some advanced light water reactor power plants, and its common use as an example in the research literature related to passive systems.

The simplified schematic in Figure 4-1 below shows the design of the hypothetical isolation condenser. The isolation condenser connects to the reactor vessel, drawing steam from the reactor, condensing it in a secondary side tank or pool of water, and returning the condensate to the reactor vessel. During normal operation, the condensate return valves are closed, preventing circulation through the isolation condenser. One of these valves opens to actuate the isolation condenser, allowing the condensate stored in the isolation condenser to enter the reactor vessel and set up a natural-circulation cooling loop. As water on the secondary side boils off, steam releases to the atmosphere and makeup water to the pool ensures long-term operation. A few existing U.S. nuclear plants utilize isolation condensers; for those that do, they typically contain one or two isolation condenser loops. New ALWR designs typically contain up to four loops.

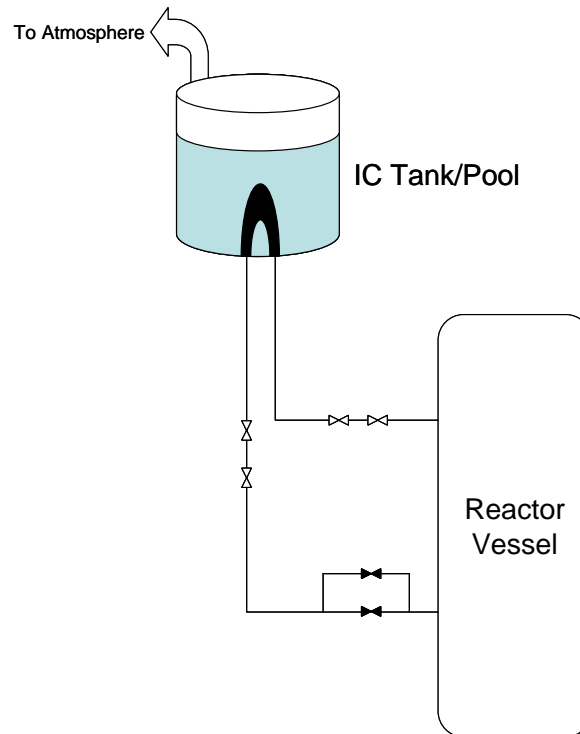


Figure 4-1
Schematic of generic isolation condenser

Identify the Boundaries of the Analysis

Another initial step in the analysis is to identify the boundaries of the analysis. These should include both physical and analytical boundaries.

Identification of the physical boundaries of the analysis is not unique to this process, but it is vitally important for complex reliability analyses such as this. The analyst should clearly define the boundaries of the system or systems under analysis. Particularly where two or more systems are the subject of the analysis, the analyst should clearly allocate components and functions to one system or the other.

The analyst should also define analytical boundaries based on the objectives of the analysis. Depending on the specific objectives, the scope of the analysis may be restricted to limit its extent. For example, some applications may only require the assessment of specific initiating events or specific functional failure modes. Initiating events may be limited by types (LOCAs, transients, external events, etc.) or by mode (e.g., full power vs. shutdown). The desired outputs of the analysis may also limit the analysis scope. That is, the analyst should define which PRA metrics the analysis will address (e.g., passive system reliability/availability, core damage frequency, large early release frequency).

The selection of both the physical and analytical boundaries of the PSS analysis should consider the available information, operational experience, and the available resources for the project. The available resources include the time available for performing the analysis (which will flow directly from the objectives), the availability of personnel (including key personnel with specific expert knowledge), and the allocated funding. Consideration of such items early in the analysis process is important for implementing an efficient analysis process.

For our hypothetical example, the design of the isolation condenser defines the physical boundaries for the analysis. The physical boundaries on the primary side of the isolation condenser are at the connections to the reactor vessel. On the secondary side, the boundary will include the tank/pool, as well as the interface with the potential makeup sources. Also included within the boundary of the system are the vent lines for removing noncondensable gases from the system.

The analytical boundaries for this example will be set to include all events generally represented within the full-power, internal events PRA. It will include all initiating events that credit operation of the isolation condensers. The output of the hypothetical analysis would be a reliability estimate for the isolation condenser system. This estimate may be a single value or a set of values that apply to different scenario conditions, depending on the results of the analysis.

Identify Potential Interactions with Other Systems

Related to the identification of boundaries is the identification of potential interactions with other systems, either passive or active. These interacting systems fall into three general categories.

First are systems that must function in order for the passive system to function. An example would be the relationship between automatic depressurization valves and a gravity-driven cooling system. If the gravity-driven cooling system can only function at low pressure, the automatic depressurization system must first function. The identification of these inter-dependent systems is important not only from a general PRA function perspective, but also as a potential means for degraded operation of the passive system. For example, if the depressurization valves do not fully open, the depressurization may not meet the expectations of the design (e.g., blowdown may not occur sufficiently fast), and so the ability of the PSS to properly function may be more uncertain.

A second general category is dynamically interacting systems. One area where this may be particularly apparent is in the function of passive containment cooling systems. Because the effectiveness of the containment cooling function will depend upon the conditions within containment, system operation is likely to have interactive effects on other in-containment systems. These other systems may or may not serve similar functions, but the analyst should consider their specific operating characteristics for their phenomenological effects on the passive system under analysis.

The third type of interacting system includes support systems. While passive systems may have little to no support system dependencies, the analyst should identify any dependencies that do exist. A typical example that may occur is a support system necessary to actuate the passive system. Potential support systems for passive systems include DC electrical power, instrumentation and control signals (either analog or digital), and control air.

For the isolation condenser example, we consider two main types of interactions. On the primary side of the system, interactions may exist near the steam and condensate connections to the reactor vessel. For example, if the line where the steam supply connects is near systems such as depressurization or relief valves, we consider the operation, failure, or degraded operation of these valves. On the condensate connection, we assess systems whose performance could affect the ability to return condensate to the reactor. For example, on plant designs with recirculation pumps, these pumps may need to be unisolated to allow proper condensate flow back to the core. These types of potential interactions will depend upon plant-specific details.

Define the Important Safety Function(s) for the Analysis

The next step in defining the specific issue for PSS analysis is to define the safety function or functions of interest. This definition will require interaction with the previous steps in order to create a concise, complete definition of the required safety function.

In general, most passive safety systems for which a comprehensive reliability analysis would be required will provide a heat transfer function. This function may occur through circulation of a cooling fluid, injection of coolant, or similar cooling functions. For the purposes of this analysis, the analyst should define the safety function in terms of the phenomenological function. For example, the system should remove a specified amount of heat, transfer a specified amount of heat, provide a specified amount of coolant injection, or establish a specified flow rate. The function should be defined according to measurable phenomenological factors. Because of the typically small operating margins possessed by passive PSSs (compared with active systems), it is important that these factors be as specific as possible.

Note that the definition of the specific factors and applicable success criteria may expand beyond a single variable or single setpoint. For example, the safety function may be the removal of decay heat from the core, which follows the decay heat curve. In such cases, the critical variable and the mathematical representations that define the safety function and its success criteria would be necessary to complete this step.

For our hypothetical example, the safety function of interest is to provide adequate core cooling to prevent core damage. In a real analysis, “adequate core cooling” and “core damage” will require additional definition, such as maintaining the water level in the reactor vessel above the top of the active core. For this example, this simple definition is sufficient. Depending on the objectives of the analysis, we may also consider the function of the isolation condensers to inject their inventory into the reactor core during a loss of coolant accident.

Define "Normal" Operation of the Passive System

The final step in clearly defining the issue is to define what constitutes “normal” operation of the passive system. This should flow directly from the design and expected operational parameters previously identified. The definition of normal operation of the passive system must include the initial and operational boundary conditions expected for the system, important phenomenological variables to measure normal operation, and the expected end state of the system after performing its function (e.g., either transfer of the safety function to another system or establishment of a steady state for the long-term safety function).

Because this definition will provide the basis for the subsequent steps of the analysis, it is important that the normal operation definition contain well-defined operational conditions, well-understood phenomenology, and adequate documentation. The conditions in which the passive system is likely to operate will provide key analysis points to examine for potential failures. The well-understood phenomenology will provide key variables to examine for uncertainties and potential failures. Key documentation sources for this step may include the plant safety analysis report, technical specifications for the system, system design documentation, experimental evidence, and other phenomenological analysis of the system (or similar systems).

The definition of normal PSS operation should include:

- Types of initiating events during which the system must operate
- Sequence of events from each initiating event until system initiation occurs
- Sequence of events for the system to initiate, continue operation, and complete operation, if applicable
- Expected plant phenomenological conditions prior to and during PSS operation
- Expected environmental conditions prior to and during PSS operation
- Expected plant conditions as a result of successful system operation
- Expected indicators of system failure
- Operator actions associated with operation or monitoring of the system

Each characteristic listed above provides both the definition of normal operation and the map of potential failures to examine in subsequent steps of the analysis.

For our hypothetical example, except for medium and large LOCAs, the isolation condensers operate during all initiating events where normal cooling to the main condenser is lost. The system should operate within a few seconds of the loss of the main condenser cooling path, due to either closure of the MSIVs, loss of feedwater, or other failed systems. When initiated, one of the two condensate return valves must open in order to place the isolation condenser system into operation. At that time, any condensate stored in the isolation condenser will drain into the reactor vessel. Steam from the vessel will then naturally circulate to the isolation condenser, reject heat to the secondary side, and return to the vessel as condensate. The system will remain in operation until the reactor is depressurized or other cooling means are established. The reactor power is likely to be at high decay heat levels (up to 5-6%) at initiation, decreasing along the decay heat curve with time. During operation, the water on the secondary side of the isolation condenser will boil and escape to the atmosphere. Successful isolation condenser operation removes decay heat from the core and reactor pressure will decrease. Failures of the isolation condenser will be evident in rising reactor temperatures and pressures, or radiation alarms on the secondary side for tube breaks. System initiation is automatic, though operators can manually initiate the isolation condenser if needed. Noncondensable gases will need to be removed from the system both before and during operation in order to ensure proper flow and heat transfer characteristics.

Identify Potential PSS Failure Modes

This step begins a three-step process to identify the key failure characteristics of the passive safety system. While the terms failure mode and failure mechanism sometimes are used inconsistently across applications, in this instance we will define failure mode as the functional failure of the passive system. In other words, it is the failure to perform one or more safety functions as required by the specific accident scenario (e.g., insufficient heat removal due to insufficient coolant flow). Failure mechanisms, then, are the physical causes of a failure mode (e.g., a blocked tube that inhibits coolant flow).

The definition of failure mode will follow directly from the previous step to identify the important safety function(s). At its most basic level, the potential failure modes are the failure to perform the safety functions identified above. Because the definition of the safety function may vary depending on the specific accident sequence characteristics, so might also the identification of potential failure modes. Because a PRA models a wide range of possible events, the analyst should be sure to consider the operational variations that the passive system may face. Iteration with subsequent steps that identify key PRA scenarios may be required in order to assess the range of potential failure modes comprehensively.

For our hypothetical isolation condenser example, we identify two failure modes. Failure to cool the reactor core could occur due to either failure of flow through the isolation condenser or failure of heat transfer from the primary side to the secondary side of the isolation condenser.

The identification of key passive safety system failures follows the conceptual fault tree depicted in Figure 4-2 below. The next few sections discuss the contributors to each gate.

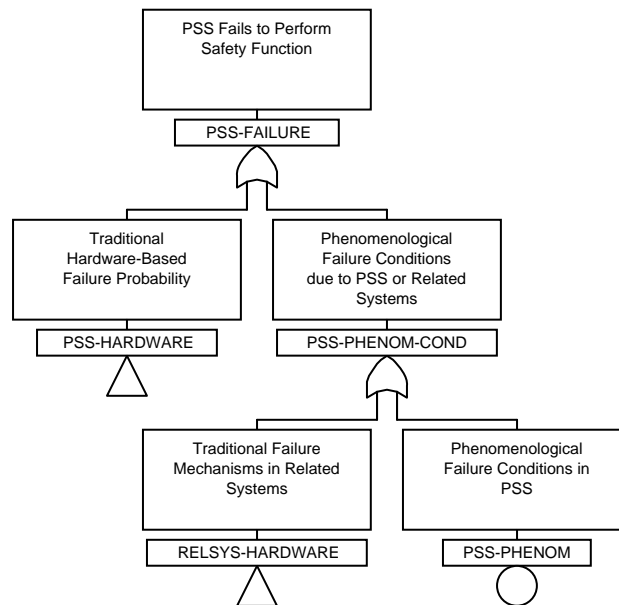


Figure 4-2
Conceptual fault tree for PSS failure

Identify Traditional Failure Mechanisms That Could Cause a PSS Failure Mode to Occur

The next step in identifying the key passive safety system failure characteristics is to link the potential failure modes to potential failure mechanisms from traditional PRA sources. These failure mechanisms may occur due to component performance, latent errors (e.g., maintenance errors), human failures, or other failures that prevent the PSS from performing its safety function. The analyst should identify the failures at the level of a basic event in a PRA, though some of the failures may not have been included in traditional PRAs due to their low likelihood. Other conditions that also may cause a component to fail to operate, such as failed I&C signals or support systems should be included as separate failure causes.

Examples of failure mechanisms to consider may include:

- Failure of check valves to open
- Failure of squib valves to function
- Rupture of tanks, tubes, or piping
- Improper component condition following maintenance
- Plugging of heat exchangers
- Human errors to disable or prevent system actuation
- Human errors to interrupt continued operation

This list of examples is not exhaustive and should not restrict the analyst's brainstorming process. To aid in the identification of failure mechanisms (as well as performance of the next step), the analyst should employ structured analytical techniques such as those used in FMEA [8, 9, 10] and HAZOP [9, 10, 11] type analyses. Table 4-1 following the next section demonstrates the use of a guideword approach in these steps.

For our hypothetical example, traditional failure mechanisms include failure of condensate return valves to open (i.e., physical valve failures), failure of steam supply valves to remain open, failure of the instrumentation and control system to actuate the system, human failure to actuate the system following automatic actuation failure, failure of support systems for the necessary valves (e.g., loss of electrical power or control air), common cause failures of valves, and test/maintenance unavailability of valves.

Identify Phenomenological Conditions That Could Cause a PSS Failure Mode to Occur

The last of the three-step process in identifying the key PSS failure characteristics is to identify any phenomenological conditions that could lead to each failure mode identified above. The analyst should define these conditions at the level of a failed phenomenological function, such as failure of heat transfer through a heat exchanger. Some functions may require additional levels of definition, such as subdividing failure of heat transfer into failure of flow, corrosion of tubes, and

insufficient heat sink. This subdivision can occur at this step, or during the identification of abnormal conditions in the second sub-step below. A good example of such a process is shown in [12], where a fault tree structure models both traditional component failures and phenomenological failures.

To identify phenomenological failure conditions efficiently and effectively, the analyst should consider relevant thermal-hydraulic operating experience. Input from thermal-hydraulic experts familiar with the passive systems is another valuable resource. In general, thermal-hydraulic experience shows that heat transfer characteristics can be one of the most important variables for passive system operation. Fouling, foreign material, and corrosion can affect heat transfer, and are generally more likely on the secondary side of a heat exchanger system. For systems using natural circulation, the thermal-hydraulic effects of two-phase flow can reduce or prevent the capability of the system to achieve its functional requirements. Analysts should consider issues such as pool water levels, decay heat curve uncertainties, and tube failures, but they are not generally significant sources of uncertainty. For systems with pressure-driven drainage of a tank (e.g., accumulators, core makeup tanks), issues related to stratification, introduction of nitrogen into the system, human actions to disable or isolate the system, and the interactive effects on other natural circulation systems should be considered. For any system using condensation of steam as the primary heat transfer mechanism, the analyst should address the impact of accumulation of noncondensable gases. Because system designers also are aware of the issue with noncondensable gases, the system is likely to contain compensating measures, which may reduce the importance of this issue. Systems using gas flow (either as a coolant or in a containment cooling system) should consider phenomena that can inhibit the low-differential-pressure flow, such as tube fouling, small amounts of leakage, or debris. Plant-specific environmental effects such as weather fluctuations, bio- or chemical fouling, and salt-water effects should be considered for inclusion in any plant-specific analysis.

For our hypothetical example, failure of the isolation condenser could occur due to inadvertent system isolation, loss of sufficient primary flow, loss of heat transfer to the secondary side, loss of the secondary side heat sink, flow diversion away from the isolation condenser, or loss of isolation condenser integrity. Note that there is some flexibility regarding where to categorize a failure condition. The analyst may categorize some conditions located under this process step as “traditional” failure mechanisms. The important issue is that the analyst identifies and evaluates the full range of potential failure causes so that all significant mechanisms that could prevent successful PSS operation are addressed.

Identify traditional failures in related systems that could lead to the phenomenological failure conditions

While passive systems do not have the same requirements for electrical power and other support systems that are necessary for the functioning of active systems, they can still possess dependencies on the operation of other systems. These systems may include support systems (such as instrumentation and control) that are not commonly included in current generation PRAs. Performance of this step also should include systems that do not directly support the operation of the subject passive system, but can influence its operation. Examples may appear in the design assumptions for the PSS, which may assume either that certain other systems are

available or that there are limited failures (i.e., the single failure criteria) in other systems. The analyst should include conditions that violate these design assumptions, such as multiple failures in other systems that create unexpected phenomenological conditions.

Examples of such failures include:

- Unexpected I&C signals
- I&C component failures (analog or digital)
- Multiple failures in emergency core cooling systems that affect containment cooling assumptions

For the hypothetical isolation condenser example, inadvertent system isolation could occur due to failed sensors or other instrumentation and control components that prevent initiation or incorrectly cause an automatic or manual isolation of the system (e.g., occurrence of a spurious secondary side radiation signal). Loss of the secondary side heat sink could occur due to valve failures and other traditional component failures in the makeup systems. Flow diversion could occur due to inadvertent valve openings or leakthrough, or due to failures of valves in other systems to properly close (e.g., failure of MSIVs). Loss of isolation condenser integrity could occur due to tube failures or other structural failures of the piping or heat exchanger.

Identify abnormal conditions that could lead to the phenomenological failure conditions

The other set of phenomenological conditions that could cause a PSS failure come from abnormal conditions that directly affect the passive system itself. This step should provide an additional level of detail to the phenomenological conditions identified above, if needed. For example, the previously mentioned insufficient flow conditions could occur due to debris in the piping or insufficient driving pressure due to various factors. Potential sources of abnormal conditions include extreme environmental conditions, unexpected thermal-hydraulic conditions, or violation of design assumptions for the passive system.

Examples of failure conditions may include the following issues discussed in many references [e.g., 1, 2, 5, 13, 14, 15]:

- Blockage of tubes/piping by corrosion products or foreign debris
- Key parameters outside the design and operational limits of the PSS
 - Temperature
 - Pressure
 - Fluid level
 - Volume
 - Flow rate
 - Heat transfer rate
 - Radiation
 - Reactivity

- Chemical deposits on heat exchanger tubes
- Diversion of working fluids
- Depletion of working fluids
- Flow instabilities
- Flow stratification
- Excessive levels of noncondensable gases
- Rapidly changing meteorological conditions
- External environmental events (e.g., fire/flood/seismic)

As with all the lists of failure mechanisms, this list should aid the analyst and provide seeds for the brainstorming process. Table 4-1 below shows how these processes work together to identify potential failure mechanisms and failure-causing abnormal conditions.

For our hypothetical example, several abnormal conditions could lead to the phenomenological failure conditions identified above. Decreased driving pressure for natural circulation could decrease the flow through the isolation condenser. Decreased heat transfer through the isolation condenser tubes could occur due to corrosion, foreign debris, or noncondensable gases. Increased secondary side pressure (e.g., due to failure to vent the secondary side steam to the atmosphere) also could decrease heat transfer. Isolation condenser tube leakage or failure could also fit under this category due to their direct effect on heat transfer in addition to potentially causing system isolation. Obstructions or noncondensable gases could block flow through the primary side of the isolation condenser. High temperatures or insufficient inventory on the secondary side of the system prior to the event also could decrease heat transfer capability.

The use of guide words to systematically identify deviations from expected operation is common in many technical fields. In particular, HAZOP techniques common in chemical and industrial engineering follow a prescribed approach to pair guide words with key parameters to identify potentially harmful deviations. References such as [11] provide examples of these HAZOP techniques. Table 4-1 provides an example application of the guide word approach tailored to a passive safety system application. Each guide word is applied to the important PSS parameters or functions to identify potential deviations in PSS operation that may challenge its ability to perform its safety function.

Table 4-1
Example of the guide word approach to identification of PSS failures

Common Guide Words	Example Applications to PSS Failures
Negative	Component does not actuate Component fails to operate
More	Too much flow (e.g., failed downstream piping) Excessive temperature
Less	Insufficient flow (e.g., due to debris or closed valves) Insufficient driving pressure (e.g., due to insufficient fluid level)
Timing (early/late)	Valves open/close early (e.g., due to I&C failure) Valves open/close late (e.g., due to I&C failure)
Timing (quickly/slowly)	Timed events happen too close together Water drains from tank too slowly
Timing (short/long)	I&C signal is not maintained long enough I&C signal does not clear when function has been accomplished
Spurious operation	Extra components actuate System operates when not needed
Partial operation	Not enough depressurization valves operate Check valve partially opens
Reverse operation	Flow leaks through a closed check valve Component opens when it should close
Repetitive operation	I&C signal repeats Valve cycles when it should stay in place

Identify PRA Scenarios That Deviate from "Normal" PSS Operational Assumptions

Because a PRA represents a broad range of accident sequences, including many that are beyond the traditional design-basis accident scope, there exists the possibility for PRA scenarios to present conditions that deviate from the “normal” PSS operational assumptions. To identify these scenarios, the analyst will need information from the plant-specific PRA model. In particular, the event trees and success criteria that define the accident sequences will provide the foundation for identifying situations that can challenge the functions of the passive system.

Along with information from the PRA, the failure modes and their causes identified in the previous sections will provide important direction for the identification of PRA scenarios. That is, where phenomenological conditions that can cause a failure of the PSS exist, the analyst should search for these specific conditions in the PRA model. In order to improve the completeness of the search, the process should iterate between examining PRA scenarios and revisiting the failure modes and abnormal conditions. For each abnormal phenomenological condition identified, the analyst should search for matching PRA sequences; for each PRA scenario that potentially deviates from the design and operational assumptions of the PSS, the analyst should revisit the failure modes to see if a failure condition already matches or if the analysis needs to define a new failure condition.

The previous steps in the analysis to define the system, its boundaries, and its normal operation will provide the basis for the identification of deviating PRA scenarios. Performing the process as specified to this point should have identified any scenario that contains a violation of the factors needed for normal operation in this step. Examples of such deviations include scenarios with:

- Initiating events that the system is not specifically designed to address (e.g., loss of support system initiators)
- Variations in an initiating event that deviate from the assumed accident progression
- Multiple failures
- Support system failures that affect multiple dependent systems
- Abnormal environmental conditions
- Human errors (especially multiple human errors)
- External events (e.g., fire, seismic) that affect multiple systems

Note that the analyst should examine the PRA at different levels of detail in order to identify deviant scenarios. At the highest level, the PRA generally represents a series of key functions (e.g., reactivity control, inventory control, and heat removal) that occur in order to protect the reactor core. The event trees show the progression of systems called upon to maintain safety. At the lowest level, cutsets represent the components, human actions, and configuration conditions that lead to core damage. The search for challenging PRA scenarios should examine all three of these levels, since different deviations may occur at different levels. For example, initiating event variations may appear at the functional or system level, while human errors likely only will appear at the cutset level.

The identification activity will be an iterative process, where the analyst identifies a deviation scenario and matches its characteristics against the operation of the PSS. If the deviant scenario lies within the design of the PSS or the analyst can show that the PSS is highly likely to function successfully, the scenario can be discarded. If the scenario is able to challenge the successful operation of the PSS, it continues for further analysis. The process then repeats with each identified scenario.

The hypothetical isolation condenser example becomes more difficult to follow at this point without a real system to examine and a real plant PRA into which to integrate the PSS reliability analysis. Using the types of deviations proposed above, we can postulate some example deviations that would be applicable for an isolation condenser. For example, the isolation condenser is designed to provide an alternate core cooling method when the main condenser is not available. It may not be designed to deal with scenarios where coolant is also being lost due to a stuck-open valve or small leak. These events may represent deviations for the isolation condenser. The PRA structure may already capture the effects of multiple failures and support system failures, but they may also create deviation scenarios for an isolation condenser system. Abnormal environmental conditions could affect the secondary side of the isolation condenser, particularly if external events are included in the scope of the analysis.

Identify Additional Deviations That the PRA Model Does Not Explicitly Represent

Like all models, a PRA is an imperfect indicator of the plant response to potential adverse events. Since all organizations have limited resources and time, simplifications are necessary to enable development of the PRA model and ensure that it evaluates and captures the most important aspects of plant operation. As such, examination of the modeled PRA scenarios may not be sufficient to identify operational deviations that challenge the function of the passive system. Further comparison of the PRA with other documentation should identify such plant conditions that the PRA may not specifically model.

The plant conditions of interest include unusual plant configurations; component availability due to testing and maintenance, instrumentation and control availability and reliability; and other factors (e.g., off-normal or dynamic conditions) that could result in unusual plant conditions and behavior. Examples include:

- Operational modes other than full-power (i.e., low-power or shutdown conditions)
- Operational data indicating frequent component unavailability or I&C failures
- Unusual maintenance or testing configurations
- Latent human errors (e.g., from maintenance activities)
- Degraded, though technically successful, system performance

Like the search for explicit PRA scenario deviations, this more detailed search may occur at either the functional, system, or cutset level, though it is more likely to require the more detailed information in the lower levels of the PRA. Where matching phenomenological failure conditions do not already exist, iteration with that task should occur to add those failure conditions to the analysis.

Following our hypothetical example further, latent human errors and instrumentation & control failures are additional deviations that could affect an isolation condenser system. Since a PRA does not always explicitly model either of these factors, they may not show up in a search of formal PRA scenarios. Instrumentation and control failures could not only affect system actuation, but could also lead to unexpected initial conditions due to improper valve alignments

or incorrect secondary side water levels. Latent human actions may or may not explicitly appear in the PRA for activities such as maintenance errors that leave one or more valves in incorrect positions or without actuation signals.

Sort PRA Scenarios by Risk

Once the analyst has developed a list of PRA scenarios that potentially challenge the successful function of the PSS, a sorting process will identify those scenarios that will have the greatest effect on PSS reliability. This process can utilize both qualitative and quantitative arguments for identifying important scenarios, with the best approach being to consider both. Note that this step should be a rough sort, and not a definitive ranking. The goal of this step is to “screen-in” scenarios, so any scenario that meets either the qualitative or the quantitative guidance should be retained for analysis.

Qualitative approach

In the qualitative approach, any identified PRA scenario that shows characteristics typical of important scenarios should be retained. These characteristics of high-importance scenarios include:

- Rapid accident progression (i.e., a short time to core damage)
- Operation outside the traditional design-basis accident definitions
- Single-failure susceptibilities/lack of redundancy
- Support system susceptibilities among different systems (e.g., loss of component cooling water to multiple ECCS systems)
- External events (e.g., internal fires and seismic events)
- High-frequency events

In addition to the characteristics that indicate high importance for a scenario, the analyst should also consider compensating characteristics that tend to decrease the importance of a scenario. While this guidance cannot provide a formula that provides instruction on how a compensating characteristic can “cancel out” a high-importance characteristic, the analysts should be conservative in including scenarios for further consideration. That is, scenarios with one or more high-importance characteristic should be retained. Scenarios with no high-importance characteristics or that possess significant compensating characteristics can be discarded (assuming they are not identified for inclusion by the quantitative guidance).

Characteristics of decreased-importance scenarios include:

- Recovery available and likely (via automatic or manual actions)
- Multiple, independent failures that typically produce negligible probability of event occurrence
- Well-defined, design-basis type accident sequence
- Long-time frame available before core damage

Quantitative approach

The analyst also should use quantitative risk metrics to identify scenarios to retain for further analysis. The quantitative approach will specifically apply to accident scenarios with detailed definition, such as at the cutset level. Any scenario represented by a cutset in or near the top 90% of core damage frequency or large early release frequency should be retained for analysis.

Identify the Important Scenarios That Can Challenge the Operation of the PSS

The last step in the identification process is to consolidate the results of the previous steps into a final list of important scenarios.

First, all the surviving PRA scenarios must be matched with the corresponding failure conditions that threaten the success of the PSS. This process may require iteration of the failure identification and scenario identification steps in order to ensure that all scenarios and failure conditions have matches. Note that there is not necessarily a one-to-one correspondence between the scenarios and failure conditions. That is, more than one scenario could result in a specific failure condition. Likewise, one specific scenario could result in multiple failure conditions. The result of this matching process will be a list of scenario-condition pairs that define an accident sequence that creates conditions that could lead to failure of the passive system function.

The resulting list may include scenarios that are similar to each other with respect to the plant conditions created. Where possible, the analyst should group similar scenarios together in order to increase the efficiency of the later analysis. When combining scenarios, it is important to maintain a description that includes the details of the combined scenarios so that the resulting quantification (in a later step) will capture all of the contributing scenarios.

The last aspect of this step is to provide detailed descriptions for each scenario (or group of scenarios) in order to facilitate the later steps in the PSS reliability evaluation. This should provide a detailed description of the accident scenarios that can lead to potential PSS failure conditions. The description also should describe the failure conditions and an explanation of why these failure conditions may prevent the PSS from performing its safety function. If known, the description also should include a qualitative assessment of the effects of the failure condition on the PSS – whether failure is certain, likely, or merely possible under the defined conditions.

Many of the failures and scenarios identified in this process will be amenable to modeling with existing PRA techniques. Component failures, support system failures, plugging of heat exchanger tubes, and structural failures of tanks are just some examples of traditional failure mechanisms that may contribute to passive safety system reliability. It is those failures that do not fit into traditional PRA techniques that gain a greater importance for some passive systems and that need additional attention throughout this analysis. These phenomenologically-driven scenarios will be the focus of the remaining passive system analysis, though any traditional failures are just as important to track in order to provide perspective to the importance of the phenomenological failures.

Using our hypothetical example, we can identify many traditional failures, including valve failures, valve motive power failures, inadvertent valve operations, I&C actuation failures, and human failures. The table below lists potential phenomenological failures.

Table 4-2
Example PRA scenarios and failure conditions

PRA Scenarios	Phenomenological Failure Conditions
All or most PRA scenarios	Reduced heat transfer due to corrosion
	Reduced heat transfer due to foreign debris
	Reduced heat transfer due to secondary side atmospheric vent failure
	Reduced heat transfer due to high initial secondary side temperature due to I&C failure
	Reduced heat transfer due to high initial secondary side temperature due to latent human error
	System isolation due to I&C or sensor failures
	System isolation due to failed tubes
	Reduced primary flow due to obstructions or noncondensable gases
High-pressure (non-LOCA) scenarios	Stuck-open valves divert flow from isolation condenser
Small LOCA scenarios	Reduced driving pressure for natural circulation
Medium/Large LOCA scenarios	System not credited

5

GUIDANCE FOR TARGETED PHENOMENOLOGICAL ANALYSES

The purpose of this task is to provide guidance regarding the identification of additional phenomenological calculations related to the passive system. To determine the overall reliability of the passive system, it may be necessary to create information regarding the effects of potentially important accident sequences on the passive system(s) being analyzed. The purpose of this part of the analysis is to develop a limited number of “targeted” phenomenological analyses that will provide useful information to fill gaps in the existing information base. The process will examine the failure mechanisms and accident scenarios identified in the previous step in order to identify gaps to address through phenomenological calculations.

Related Conclusions

A number of the conclusions from EPRI 1015101 [4] relate to this task.

- Because passive systems are likely to be more sensitive to variations in thermal-hydraulic parameters, analysis of their reliability should include consideration of a broader range of failure mechanisms, including mechanisms that may provide significant impact on the phenomenology and functional margins.
- While 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 assure 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 so long as the means provided for purging noncondensable gases function as designed.
- 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.

Phenomenological failures of passive systems are most likely to occur when the passive system encounters operating conditions outside its design basis. Some of these beyond-design situations may be covered by existing analyses or can be addressed by conservative analysis for rare (i.e., non-risk-significant) conditions. That is, the analyst may be able to use conservative or bounding analyses for very unlikely situations without affecting the end result. However, for more likely situations, additional, more realistic calculations may be required to address passive system reliability adequately.

Approach for Targeted Phenomenological Analyses

The identification of additional phenomenological conditions for the comprehensive analysis should follow from these conclusions. That is, it will be important to address all of the previously identified phenomenological parameters, environmental and operational conditions, and design assumptions that affect the operation of the PSS.

Identify and Categorize Gaps in Existing Information

The first step in this part of the analysis process is to map the potential failure scenarios to the available information. This mapping will help to identify which scenarios can be categorized as successful operation, failed operation, or unknown operation. Unknown outcomes represent gaps in the knowledge base that the analyst needs to address in order to estimate PSS reliability. Note that the categorization of successful or failed operation links to the purposes of the PRA. In this categorization, conservative assumptions or probabilistically negligible arguments may be useful. Categorization should follow the guidance in Table 5-1.

Table 5-1
Classification of potential failure scenarios

No Further Analysis Needed	Further Analysis Needed (Gaps)
Scenario lies within the design basis or is addressed via other available information AND Data indicates a very high likelihood of successful PSS function	Scenario lies within the design basis or addressed via other available information AND Data indicate the PSS function may not succeed AND Likelihood of the scenario is non-negligible
Scenario lies within the design basis or is addressed via other available information AND Likelihood of the scenario is negligible	Scenario lies beyond the design basis and is not addressed via other available information AND Likelihood of the scenario is non-negligible
Scenario lies beyond the design basis and is not addressed via other available information AND Likelihood of the scenario is negligible	Scenario contains special phenomenological concerns or inter-system interactions that the design basis or other information does not adequately address
Scenario lies beyond the design basis and is not addressed via other available information AND Scenario characteristics indicate the PSS function is unlikely to succeed	

For scenarios that fall into the left-hand column, no further analysis is necessary. These scenarios are unlikely to affect the estimate of PSS reliability significantly, since they have either a negligible likelihood of occurrence or a likelihood of failure that is close to zero or one.

For scenarios that fall into the right-hand column, the analyst must acquire additional information and perform phenomenological analysis to address the effects of this scenario on PSS reliability.

Note that the categories above include a rough (i.e. qualitative) estimation of scenario probability. During the initial process, only a determination of non-negligible probability is necessary. However, guidance for estimating the probability of important scenarios that is discussed later in this report may be useful to incorporate during this step.

Figure 5-1 below shows a graphical depiction of the potential operational envelope for a passive system. In the center of the figure, a well-defined area represents the known design basis of the passive system. Within this area, the passive system exhibits well-understood behavior that

supports the determination of success or failure of the passive system for each scenario. Outside the well-defined center, the extreme boundaries of parameters and environmental conditions are more vague. Within this area, scenarios may fall into one of four categories. For some scenarios outside the known design basis, other available information may support a high confidence in the likelihood of success, as in the first box on the left side of Table 5-1. Another set of scenarios may be so unlikely that their probability is negligible, as the second and third boxes on the left side of Table 5-1. For scenarios outside the known design basis with conditions that are likely to prevent the PSS from performing its safety function as in the last box on the left side of Table 5-1, the analyst may assume failure of the PSS in order to focus the analysis on more important scenarios. For all the remaining scenarios on the right side of Table 5-1, the analyst must determine the performance of the PSS and estimate a probability of failure. The next section discusses the potential approaches to evaluate these scenarios.

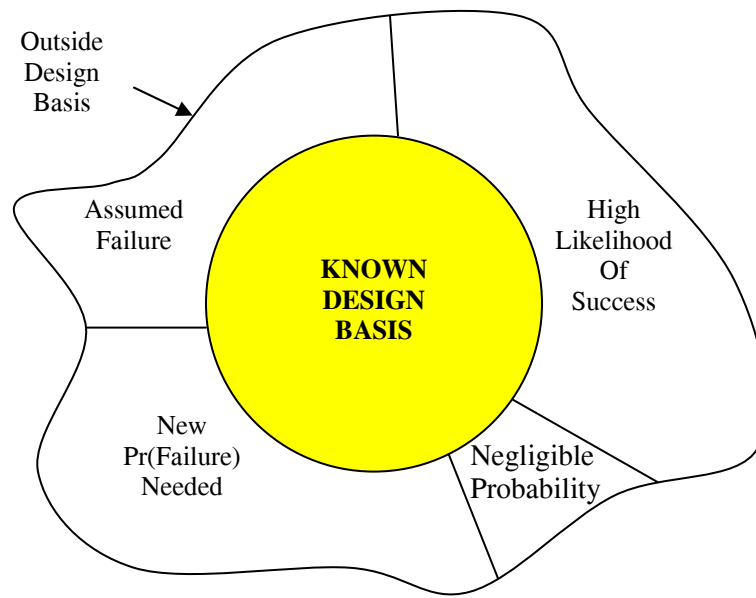


Figure 5-1
Categorizing gaps in the information

Identify Approach to Close Each Gap

Next, the analyst will identify an approach to close each identified gap. Depending on the specific circumstances of each scenario and its reason for appearing as a gap, different approaches may be possible for resolution. The listing below presents possible approaches for the analyst to use.

- **Phenomenological calculation** – Additional phenomenological calculations may provide the information necessary to determine success or failure of the PSS under the given scenario. Depending on the exact scenario parameters, phenomenological calculations can provide the most useful information with an efficient use of resources. Calculations should only be necessary for those applications that possess the highest risk and greatest complexity. Because this approach provides a good balance between cost, resource commitment, completeness, and usefulness of results, it will be discussed in more detail in the next section.
- **Experimentation** – Additional phenomenological experiments can often provide the most realistic information; however, they often apply to only a very few scenarios. Experiments are also typically the most expensive approach in terms of resources and time, and may not be a realistic solution to support near-term decisions.
- **Expert opinion** – The use of expert opinion in PRA is not limited to passive system phenomenology. Despite some negative connotations, expert opinion elicitation can be a valuable source of information to inform the estimate of PSS reliability. Formal techniques for expert opinion elicitation provide a structured process that, if followed, can provide sufficient confidence in the results. Though not discussed further in this document, generic guidance for the development and use of expert opinion in PRA to address issues with characteristics similar to those associated with the analysis of PSSs can be found in resources related to seismic analysis [16] and accident progression analysis [17]. Additional references provide examples of the use of FMEA [8, 9, 10], HAZOP [9, 10, 11], and AHP [8, 18] to guide the analysis process.
- **Conservative assumptions** – In some cases, it may be sufficient to utilize conservative assumptions to cover gaps in information. In cases where the frequency of the scenario is relatively low, or where the effects on the overall safety of the reactor are minimal, the analyst may assume a conservative estimate of PSS failure. The analyst should exercise caution when applying conservative assumptions for a particular application, and consider the effects of such assumptions on other PRA applications that may occur later.
- **Design change** – When the analysis of PSS reliability is part of the design process, it may be possible to modify the plant design, the PSS system design, or the design of related/interfaces systems in order to eliminate or modify the potential failure scenario. Examples may include the incorporation of parallel process paths, diverse and/or redundant components, or modifications to component specifications (e.g., pipe diameter) that affect the phenomenological behavior of the passive system.

Define and Perform Necessary Phenomenological Calculations

As discussed throughout both EPRI 1015101 [4] and this report, one of the most important characteristics that affects the reliability of passive systems is their potential susceptibilities to phenomenological uncertainties. The purpose of the process laid out in this guidance document is to identify the important scenarios where those uncertainties can appear, identify the characteristics and potential phenomenological failure mechanisms that are likely to occur in those scenarios, and identify those scenarios where insufficient information exists to support assessment of the success of the passive safety system functions. The guidance in this step of the analysis supports the definition of key phenomenological calculations that will fill those information gaps efficiently and effectively.

The potential failure scenarios that remain in this step of the analysis are sufficiently complex that straightforward methods cannot address them in a time frame to support efficient operational decisions. They occur with a non-negligible frequency and contain phenomenology that pushes the edges of the operational envelope. The likelihood of PSS failure during these challenging scenarios needs to be estimated in an efficient manner that meets the goals of the PRA application.

Efficiency in the selection and execution of phenomenological calculations is one of the driving purposes for this research. With limited available resources, the ability to compute a high number of complex scenario variations is limited. The primary alternative, use of expert opinion, can be insufficient to assess some of the complex phenomenological interactions in sufficient detail to obtain a realistic estimate of PSS performance during these challenging scenarios. The proposed solution, therefore, is to use available expertise in order to define and perform only those phenomenological calculations necessary to arrive at an acceptable estimate of PSS reliability that is sufficient to support the objectives of the PRA application (including any associated regulatory review).

The process recommended here is a successive parsing of the potential failure scenarios. That is, given a potential failure scenario for a given passive safety system, the ability of the system to successfully perform its intended function is uncertain. If the analyst identifies portions of that scenario as highly likely to succeed or fail, these portions can be “broken off” so that the uncertain areas are assessed separately. Therefore, the goal of the phenomenological calculations is to identify these success/failure bifurcations to successively narrow the degree of uncertainty in PSS behavior and effectively use limited resources. Figure 5-2 schematically shows this concept. In this proposed framework, successive iterations of the process reduce uncertainty until it becomes sufficiently small to adequately support the intended PRA application or decision. The analyst should remember to keep the analysis of the passive system in proper context during this process, as uncertainties will always exist in any PRA application. The effort devoted to the reduction of uncertainty related to the PSS should be commensurate with its importance in the overall PRA application and proportionate to uncertainties in other aspects of the PRA such as initiating event analysis, component reliability, success criteria definition, and human reliability analysis.

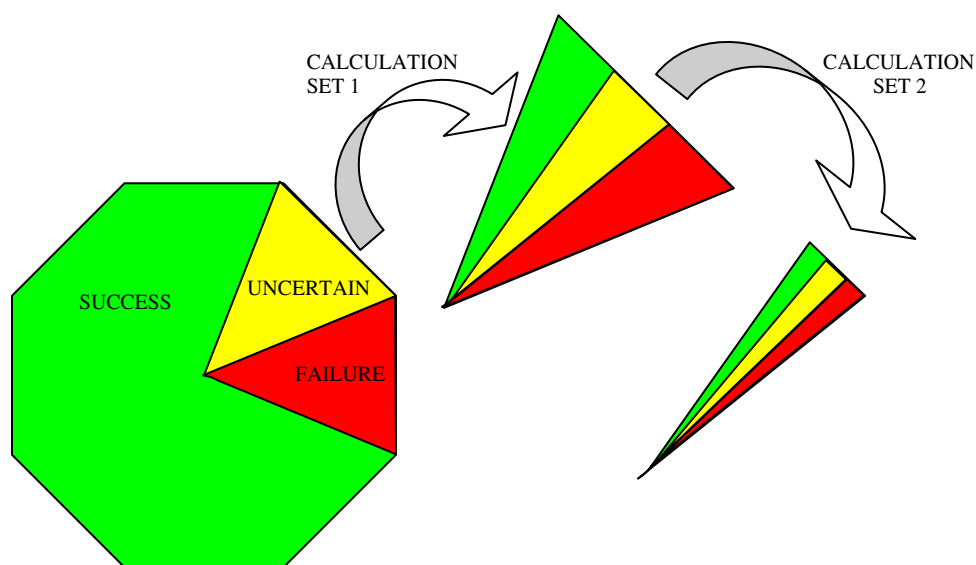


Figure 5-2
Successive analyses to reduce uncertainty

In addressing the phenomenological uncertainties surrounding passive system behavior, we will generally divide the uncertainties into two types, parameter uncertainties and code (calculation) uncertainties. In the sections below, we provide guidance for addressing each type.

Addressing parameter uncertainties

For our purposes, parameter uncertainties represent uncertainties in inputs into phenomenological calculations, including input parameters from the end user and parameters embedded in the code's physics-based models. The uncertainties in these parameters are the most commonly understood and their effects are usually evident by slightly varying parameter values through repeated calculations. The purpose of this guidance is to provide a process to identify a small number of key calculations to address these uncertainties in an efficient manner.

Though the same concepts apply regardless of the phenomenological code being used (e.g., RELAP, TRACE, CATHARE, TRACG), in this report we will discuss the types of parameters based on the general approach employed in the MAAP4 code [19]. Three specific types of parameters are discussed here: model parameters, control parameters, and plant parameters.

Model parameters include both the inputs to a given physics-based model and the selection of a particular model among different physics-based models. For example, a given physical model may require inputs for material properties (e.g., concrete and steel), fluid flow limiting characteristics (e.g., void fraction limits, flow area limits, and critical velocities), friction coefficients, and other parameters. Different physics-based models represent differences in plant configuration, simplifying modeling assumptions, and/or phenomenological correlations.

Different computational codes also may include different maximum and minimum possible values for model parameters. The analyst should investigate these maximum and minimum values to ensure they do not unrealistically constrain the behavior of the PSS and influence the analysis results.

Control parameters include designators for the type of plant, various configuration parameters, and selection of specific model and integration options. Control parameters do not generally affect phenomenological uncertainty, but the analyst should review them against potential failure scenarios to ensure that all control parameters are appropriate for the particular analysis objectives.

Plant parameters define the plant-specific features necessary to perform the phenomenological calculation. Plant parameters include reactor core characteristics, system characteristics (e.g., reactor coolant system pressure/flow/temperature or emergency cooling system flowrate), and physical plant characteristics (e.g., containment building characteristics).

In order to gain efficiency in the handling of parameter uncertainties, the process must use some expert input. Without such input, one must rely on a more-or-less random exploration of the parameter space. Due to the significant calculation time required to perform calculations using the phenomenological models/codes identified previously, use of an inefficient process (such as random exploration requiring a significant number of Monte Carlo simulations) would not support near-term risk-informed operational decisions. The key to an efficient, realistic assessment is to balance expert input with calculational or experimental evidence to address those phenomenological issues that are most significant to successful PSS operation. The successive parsing of the scenarios (as defined by the appropriate parameters) achieves this balance by maximizing the benefit of the expert input.

For each potential PSS failure scenario (or group of scenarios with similar characteristics), the analysis should use personnel with expertise in the particular phenomenologies of importance in order to follow these general steps:

- Define the failure envelope for the passive safety system – that is, define the values at which parameters indicate potential failure of the safety function.
- Identify the key parameters in the phenomenological computer codes that affect the function. The potential failure scenario may already define the parameters or the analyst may need to translate them into one or more code parameters. In addition to phenomenological parameters, the analyst should consider threshold parameters that define actuation setpoints or failure setpoints for their effects.
- Identify values for the key parameters that parse the input space. When more than one parameter affects the phenomenological uncertainty, the analysis should consider varying parameters singly, doubly, or more if parameter behavior is correlated. The analyst must remember to account for interactions among variables and other systems when selecting parameters and their values. The analysts should consider any inflection points in parameter behavior and examine their causes for insights on parsing the input space.

- Perform additional phenomenological calculations to assess passive safety system function with the varied parameter inputs.
- Assess the likelihood of any residual uncertain areas. If the likelihood of the remaining inputs is non-negligible, repeat the parsing and calculation process.
- If necessary, repeat the process of identifying new values for key parameters for new calculations. In selecting additional values, the analyst and phenomenological experts should aim to select values that either represent areas likely to produce non-linear responses or efficiently parse the parameter space such the residual space is of very low likelihood.

EPRI report 1015101 [4] discusses the most important issues for each type of passive system. In general, heat transfer coefficients tend to show up as important parameters for almost all passive system designs. The effects of noncondensable gases, corrosion/fouling, and clogging by foreign debris on fluid flow and heat transfer also are potentially important for many types of systems. Since most passive systems are driven by (relatively small) pressure differences, the analyst should be sure to consider parameters that affect pressure or depressurization rates, such as relief valve area and pressure loss through piping. The particular code parameters that represent these issues will vary from code to code, and may appear under more than one parameter within a code.

Following our hypothetical isolation condenser example developed earlier, Table 5-2 below illustrates some ways to link potential failures to parameter values in a phenomenological code.

Table 5-2
Examples of potential code parameters for phenomenological failures

Phenomenological Failure Conditions	Code Parameters (MAAP parameter)
Reduced heat transfer due to corrosion	Thermal conductivity of tube wall (KTIC) Density of tube wall (DTIC)
Reduced heat transfer due to foreign debris	Thermal conductivity of tube wall (KTIC)
Reduced heat transfer due to high initial secondary side temperature	Initial water temperature of secondary side (TWICI)
Reduced primary flow due to obstructions or noncondensable gases	Number of tubes (NTIC/NIC) Inside diameter of a single tube (XIDTIC)

Addressing code uncertainties

The issue of code (or model) uncertainties is not unique to the issue of passive safety system reliability. It is not the purpose of this research to provide definitive guidance regarding the resolution of the code uncertainty issue. Instead, the general guidance listed below addresses some of the important effects of code and model uncertainty to consider during the conduct of passive system reliability analysis.

- The analysis should utilize different phenomenological calculation methods or codes when possible to determine if code uncertainties affect any of the key conclusions. The specific strengths and limitations of the codes should be recognized and considered for their effect on uncertainty. The analysts should use comparisons among codes and against experimental data when possible; an example of such a comparison is presented in [20]. Important parameters may include the timing for key events and mass distribution for key parameters (e.g., coolant, fuel).
- The particular methods selected for the analysis should utilize high-quality, state-of-the-art analytical models and codes. Traditional systems analysis codes, computational fluid dynamics approaches, and hybrid approaches using both suites of tools may all be useful. Because a significant degree of uncertainty already exists in the analysis of passive system reliability, this guidance does not recommend use of overly-simplified codes or failure surfaces when determining PSS functional performance, particularly when this performance is being evaluated under unusual/unexpected conditions. For the same reasons, simplified models (e.g., with a small number of nodes) are not recommended. However, these types of simplified codes and models can be useful for initial exploration of the parameter space.
- Known issues with a computational method or code should be recognized and examined for any effect on the passive system function. If the issues would produce a significant effect, the analyst should use other methods or codes or apply conservative assumptions.
- The goal of most PRA applications is to obtain realistic estimates of reliability. However, intentionally conservative calculations and codes can be useful. They can play a role in verifying the adequacy of best-estimate calculations and codes, they can provide information regarding the effects of uncertain parameters up to the conservative values used in the code, and they can provide an efficient way to address low-probability scenarios unlikely to affect the overall results. However, whenever analysts use such conservative calculations, they should explicitly recognize and document the calculations as conservative.
- The analyst should consider the likelihood of scenarios and scenario variations when examining code uncertainties. That is, if the code uncertainty only affects an input space with negligible probability, it should not produce a significant effect on the estimation of PSS reliability.

6

GUIDANCE FOR QUANTIFICATION OF PSS RELIABILITY

The purpose of this task is to provide guidance regarding the quantification of PSS reliability. The quantification process will use the information created in the previous steps to estimate the likelihood that the passive safety system fails to perform its designated safety functions.

Related Conclusions

- Because passive systems are likely to be more sensitive to variations in thermal-hydraulic parameters, analysis of their reliability should include consideration of a broader range of failure mechanisms, including mechanisms that may provide significant impact on the phenomenology and functional margins.
- 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 assure safety. This provides additional assurance of a reliable system, particularly for advanced light-water reactor designs operated under the current regulations.

When estimating the likelihood of failure for passive systems, the analyst needs to consider the broad range of potential failure mechanisms. For unique, rarely occurring mechanisms, the likelihood of the deviant conditions that cause the failure mechanism will play an important role in determining the reliability of the passive system.

Because this guidance document focuses on advanced light-water reactor designs under the current regulatory environment, the determination of PSS reliability does not need to be perfect. As with all parts of the PRA, uncertainty will exist in the quantification of the PSS failure probability. A best-estimate failure probability, combined with an integrated risk-informed decision-making process, should provide an adequate estimate of PSS reliability for regulatory purposes.

Approach for Quantification

Passive safety systems should have very high reliability under “normal” operating conditions (i.e., within their design envelope with no external disturbances). Therefore, it is important to recognize that the purpose of this comprehensive approach is not to calculate the failure probability of the PSS under “normal” conditions, but rather to identify the unexpected situations for the PSS where failure could become more likely. The likelihood of these unique situations, combined with the (conditional) failure rate under those conditions, yields the overall failure rate for the PSS.

The PRA should model the passive system by considering a combination of traditional failures of its components, failures of traditional components from related systems that create phenomenological failure conditions, and abnormal conditions that create potential phenomenological failure conditions. The quantification process described here focuses on the quantification of failures due to abnormal phenomenological conditions; existing PRA techniques can handle traditional failures within the passive system or in related systems. That is, the quantification process will estimate the failure rate for the phenomenological failure probability represented by the “basic event” in the conceptual fault tree below.

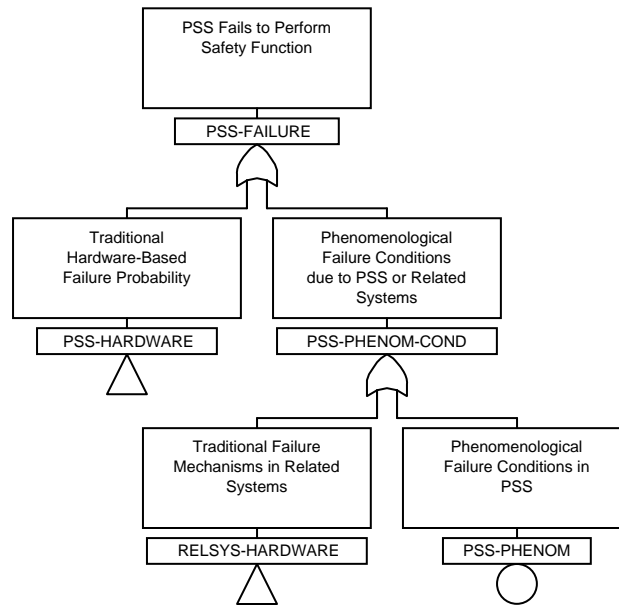


Figure 6-1
Conceptual fault tree for PSS failure

Quantification of passive system failure probabilities may occur at different levels. It may be possible to perform one quantification that covers all PRA sequences that call upon the passive system to perform its safety function. More likely, a small number of calculations will be necessary in order to capture the PSS failure rate under different general operating conditions (e.g., different initiating events). In the most extreme (and rare) cases, each PRA sequence could require an individual calculation for the PSS failure rate. Regardless of the number of phenomenological “basic events” which the analyst will quantify, the process is the same.

Ultimately, the goal of the comprehensive 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 has subdivided scenarios defined by the PRA to allow for a more detailed analysis. For scenarios where the boundary conditions and environment are within the design envelope of the passive system, the probability of failure should be very low. For demanding scenarios outside the design envelope, additional evidence such as phenomenological calculations, experimental data, expert opinion, or engineering assumptions provide a basis to evaluate the ability of the PSS to perform

its safety functions. For the most difficult conditions, the analysis could either assume a conservative failure probability of 1.0 or further analysis could be performed to refine the scenario and/or passive system performance. The failure probability of the passive safety system for the identified PRA sequence(s) is the sum over all scenarios of the probability of each scenario [$\Pr(\text{scenario})$] multiplied by the conditional probability of PSS failure given each scenario [$\Pr(\text{PSSfailure}|\text{scenario})$].

$$\Pr(\text{PSSfailure}) = \sum_{\text{scenarios}} \Pr(\text{scenario}) \times \Pr(\text{PSSfailure} | \text{scenario})$$

The table below shows a general example of the calculation form.

Table 6-1
Example of quantification calculation

Scenario	$\Pr(\text{scenario})$	$\Pr(\text{PSSfailure} \text{scenario})$	$\Pr(\text{PSSfailure})$
1	0.98	0.001	0.00098
2	0.01	0.01	0.0001
3	0.008	0.1	0.0008
4	0.002	1.0	0.002
TOTAL	1.000		0.00388

$\Pr(\text{scenario})$ is not the probability of the scenario from the PRA, but the conditional probability of that scenario occurring that challenges the PSS with the identified failure mechanism. For example, the design basis of the PSS may cover 98% of potential conditions within a PRA scenario, while the remaining 2% presents a unique challenge. In a simple illustration such as this, $\Pr(\text{scenario } 1) = 0.98$ and $\Pr(\text{scenario } 2) = 0.02$. It may be necessary to break the scenario into more than one piece, and end up with, for example, $\Pr(\text{scenario } 2) = 0.01$, $\Pr(\text{scenario } 3) = 0.008$, and $\Pr(\text{scenario } 4) = 0.002$ to reach the total.

$\Pr(\text{scenario})$ represents quantification of the plant and environmental conditions leading to the challenge to the PSS. It should be conditional on reaching that particular branch in the PRA, so those branch probabilities should not be included in this term (though their effects on plant conditions do affect the likelihood of PSS success). It is the quantification of the “deviation” from expected conditions. The sum of all the scenarios should equal 1.0 to account for the full range of potential conditions the PSS may face.

Information identified earlier in the analysis process should provide the basis for the quantification of the deviant accident scenarios. Additional information may be necessary, such as operational data, to determine the likelihood of the deviations. In the absence of specific data, engineering judgments may be necessary, and the use of subject-matter experts is encouraged. In many cases, rough estimates may be sufficient for an initial quantification. The analyst will have an opportunity to revisit the estimates once the initial results identify the dominant contributors.

Examples of data and information that may be necessary for the quantification of $\Pr(\text{scenario})$ include:

- Fraction of the initiating event that leads to the deviation
- Failure probabilities of other components not already included in the event tree prior to the PSS function
- Fraction of time spent in special plant configurations or operating modes
- Failure probabilities for components not normally modeled in the PRA, such as instrumentation
- Testing and maintenance unavailability that affect the PSS function but that are not explicitly modeled in the PRA
- Likelihood of latent human errors, such as during restoration of equipment after testing/maintenance

$\Pr(\text{PSS failure}|\text{scenario})$ may fall into one of several categories. The analyst may assign the failure probability for each scenario through the use of operational data, experimental data, phenomenological calculations, expert opinion, and/or conservative assumptions.

In some cases, a deviation scenario will challenge the function of the PSS to the extent that success is unlikely. In these cases, the failure probability should be set to unity (1.0).

If the scenario is parsed such that one set of deviations is very unlikely to fail the PSS, a low failure probability (e.g., 0.01) may be used for the initial quantification. The analyst should refrain from ignoring the scenario altogether (i.e., assigning a failure probability of zero) to avoid losing potentially useful information. For cases where success is likely, but by no means assured, an initial value of 0.1 may be more appropriate. Even a relatively high value of 0.1 may be sufficient to render some failure scenarios as negligible contributors to overall risk. We note that using a relatively large value (e.g., 0.1) can serve as a useful approach to screen out scenarios for which PSS reliability would not provide a significant impact on PRA results. The specific values to use should be appropriate to the context of the specific PSS and the PRA application. The analyst needs to balance the benefits of underestimating or overestimating these initial values and may need to refine the failure probabilities after the initial results.

If the PSS response is still uncertain but is at neither extreme value (i.e., neither certain nor very unlikely) and the analysis cannot be subdivided further, expert judgment or further phenomenological calculations may be necessary to assign a failure probability. In such cases, the analyst may use a conservative approach for initial quantification, with further calculations or expert judgments used only if the potential accident scenarios contribute appreciably to the overall PSS reliability. In most cases, the analyst should attempt to parse the definition of the scenario such that it falls under one of the first two options, where one part of the scenario is likely to succeed and one part is likely to fail.

Ultimately, some of the most difficult scenario variations may require expert judgment to assign the $\Pr(PSS_{failure|scenario})$. Many previous applications of expert judgment in PRA provide good examples for expert opinion elicitation, such as the SSHAC report [16] and ATHEANA HRA user's guide [21]. However, use of this comprehensive analysis process should limit the need for extensive expert judgment to rare scenarios that may not contribute significantly to the overall PSS reliability. The table below provides general guidance for selection of $\Pr(PSS_{failure|scenario})$ values.

Table 6-2
Guidance for rough probability estimates

Expected PSS Performance	Failure Probability	Notes
The PSS will perform its safety function	0.01 - 0.001	The operating and environmental conditions are within the design assumptions of the PSS or additional information supports successful operation. Lower probabilities may be possible if justified.
The PSS should perform its safety function	0.1	The operating and environmental conditions are outside the design assumptions and other available information, but the system is likely to perform its safety function.
The PSS is not able to perform its safety function	1.0	The operating and environmental conditions are outside the design assumptions and other available information, and there is no basis to expect successful operation. The analyst also may assign this conservative value to very unlikely scenarios to conserve resources.

Different approaches to PRA models exist, but the general approach models accident progression using event trees and/or fault trees. The conceptual fault tree shown in Figure 6-1 earlier in this section provides the general approach for incorporating the PSS failure probability into the PRA. The failure probability calculated according to this guidance will supply the failure probability for the phenomenological failure “basic event.”

When incorporating the results of the quantification task into the PRA, it is important to recognize the conditional nature of the failure of PSS. That is, different failure probabilities may apply to different accident sequences that produce different deviations in plant and environmental conditions. For scenario variations driven by aleatory environmental conditions, the failure probability may be the same across accident sequences, and only one “basic event” is necessary. For example, if an extreme weather condition is the cause of the deviation, the failure probability could be the same across all PRA scenarios. However, if a prior equipment malfunction causes the deviation, this could lead to different failure probabilities across different PRA accident sequences. In such cases, different phenomenological “basic events” would appear under different fault trees that apply to different accident sequences.

The final step in the quantification process is to review the initial results for dominant scenarios and failure probabilities. If dominant failure contributors are the result of conservative assumptions or rough engineering judgments, the analyst should iterate those parts of the comprehensive analysis process. The end goal should be to have a strong technical basis for the dominant failure mechanisms of the passive system, supported by experimental evidence and phenomenological calculations where practical.

7

SUMMARY

This report describes a formalized, comprehensive analysis approach for the analysis of the reliability of passive systems that have a high risk-significance and high thermal-hydraulic complexity. The approach builds upon the previous research in the literature in order to develop a process optimized for advanced light-water reactor designs to be operated under the current U.S. regulatory regime.

The comprehensive analysis approach guides the analyst to identify potentially important PSS failure scenarios inductively. The approach uses a structured search process to identify scenario deviations that could challenge the design assumptions of the passive system(s). This search process draws upon existing techniques such as FMEA and HAZOP to develop a tailored search process for likely passive system failures. It also utilizes limited expert judgment as an integral part of the search process, and draws upon existing expert elicitation techniques common in fields such as seismic PRA and second-generation human reliability analysis.

Ultimately, the goal of the comprehensive analysis approach is to estimate the failure probability for the passive system. This probability results from a combination of different scenarios that present different challenges to the passive system. Where necessary, the analyst parses scenarios defined by the PRA to allow for a more detailed analysis. The overall failure probability of the passive safety system is the sum over all scenarios of the probability of each scenario multiplied by the conditional probability of PSS failure given each scenario.

In addition to failure of the passive system to fulfill its function due to phenomenological failures, the analyst must consider typical component-related failures. Hardware failures that could affect the phenomenological function of the passive system, such as vent valve operation to remove noncondensable gases from a system, could affect both the traditional and phenomenological aspects of the analysis. A full consideration of PSS reliability requires assessment of both the phenomenological and traditional failures, with appropriate attention on the aspects that dominate the overall reliability of the PSS.

The comprehensive analysis approach consists of several high-level steps, described in the corresponding sections and depicted in the overall process flowchart shown in Figure 1-1 and repeated in Figure 7-1. The general flow of the process proceeds from top to bottom, but the analyst must recognize the important interactions between the quantification steps and key identification steps earlier in the process. Thus, the process is iterative and the analyst will likely need to use initial probability estimates during the early steps of the analysis, and refine them as necessary later.

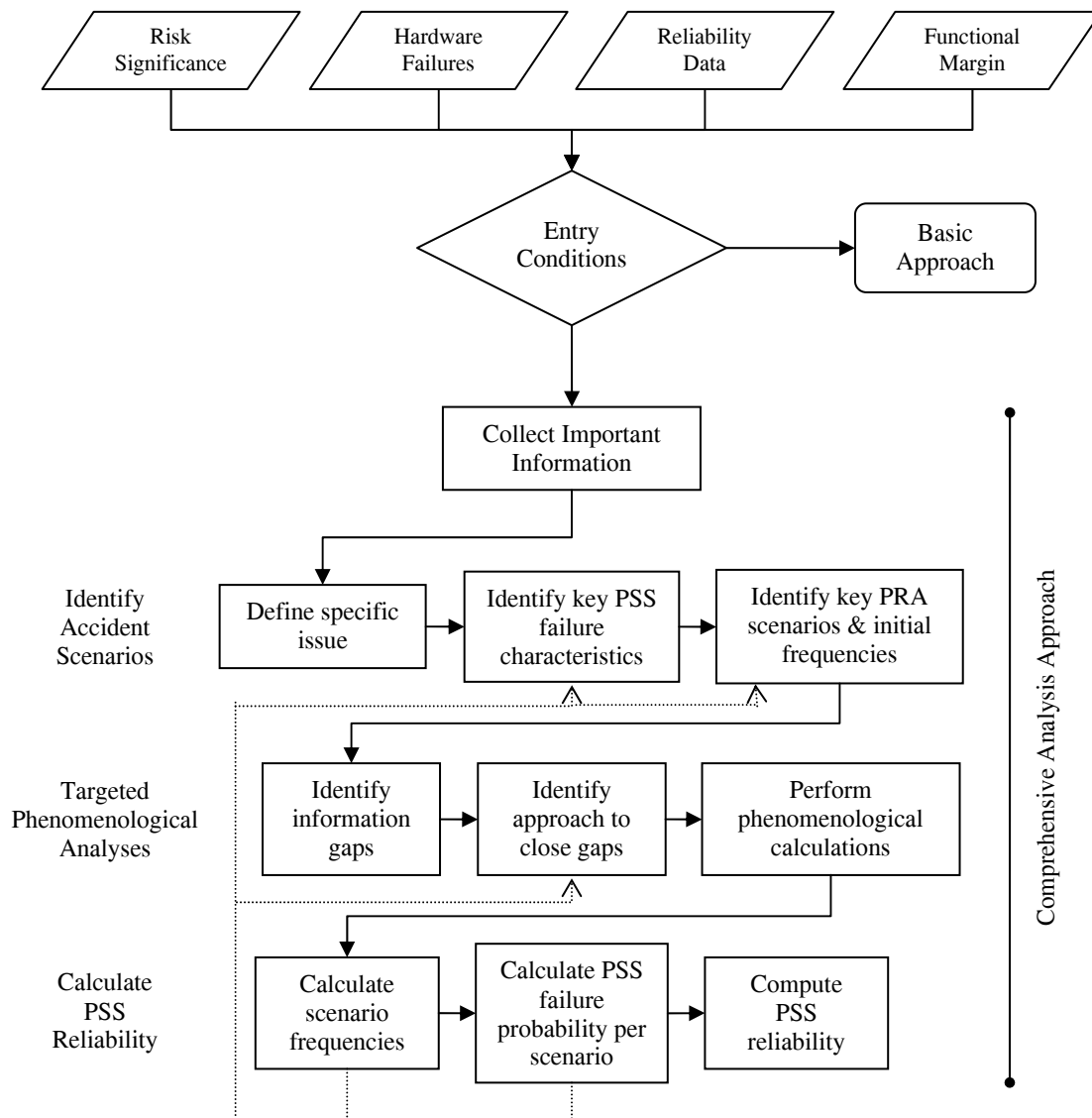


Figure 7-1
Summary of comprehensive risk assessment process

8

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, Louisiana (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. *Probabilistic Risk Assessment Requirements for Passive Safety Systems*. EPRI, Palo Alto, CA: 2007. 1015101.
5. A. K. Nayak and R. K. Sinha, “Role of Passive Systems in Advanced Reactors,” Progress in Nuclear Energy, Vol. 49, pp. 486–498 (2007).
6. A. K. Nayak, et al., “Passive System Reliability Analysis Using the ASPRA Methodology,” Nuclear Engineering and Design, Vol. 238, pp. 1430–1440 (2008).
7. International Atomic Energy Agency. Safety Related Terms for Advanced Nuclear Plants. IAEA-TECDOC-626. Vienna, Austria (September 1991).
8. 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, pp. 2612–2631 (2005).
9. L. Burgazzi, “Evaluation of uncertainties related to passive systems performance,” Nuclear Engineering and Design, Vol. 230, pp. 93–106 (2004).
10. 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,” Nuclear Engineering & Design, Vol. 238, pp. 217–228 (2008).
11. F. Crawley, et al., HAZOP: Guide to Best Practice. Institution of Chemical Engineers, Great Britain 2000.
12. L. Burgazzi, “Passive System Reliability Analysis: A Study on the Isolation Condenser,” Nuclear Technology, Vol. 139, pp. 3–9 (2002).

13. 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.
14. 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).
15. 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.
16. R. J. Budnitz, et al., Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts. NUREG/CR-6372. Livermore, CA (April 1997).
17. U.S. Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants. NUREG-1150. Washington, D.C. (1991).
18. 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, pp. 311–336 (2003).
19. B. J. Schlenger-Faber and J. R. Gabor, "Development of an Applications Guidance Document for the MAAP4 Accident Analysis Code," Presented at PSA 2008 – Challenges to PSA During the Nuclear Renaissance, Knoxville, TN (September 2008).
20. J. Hart, et al., "TEPSS - Technology Enhancement for Passive Safety Systems," Nuclear Engineering and Design, Vol. 209, pp. 243–252 (2001).
21. U.S. Nuclear Regulatory Commission, ATHEANA User's Guide. NUREG-1880. Washington, D.C. (2007).

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

Programs:

Nuclear Power

Technology Innovation

© 2008 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

 Printed on recycled paper in the United States of America

1016747

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