Appendix B

NRC-MIT Cooperative Agreement for

Advanced Nuclear Reactor Technology

Task 2

Reliability of Passive Safety Systems

Dustin Langewisch, Prof. George Apostolakis, and Prof. Michael Golay

Progress Report

September, 2008

I. Introduction

Designers of new and innovative reactors have recently turned to so-called passive cooling systems for performing a variety of functions during both emergency conditions and normal operation. Passive systems, as defined by the IAEA (1991), do not rely upon external power sources or operator actions, or at least do so only to a very limited degree; rather, these systems operate by exploiting various natural phenomena (e.g., conduction, condensation, gravity, buoyancy and/or natural circulation) to accomplish their function.

Due to their reliance on inherent physical laws, passive systems are often thought to be more reliable than traditional active systems (EPRI, 2007). Indeed, considering that the reliability of active systems is often limited by the availability of AC power or successful operator action, it stands to reason that passive systems, relying upon neither, would be more reliable (Mackay et al., 2007). Furthermore, passive systems are often thought to be less expensive than their active brethren, an assumption stemming from the fact that the design of a passive system precludes many of the costly components, such as pumps, that would otherwise be necessary (EPRI, 2007). In addition, the use of passive systems may warrant the elimination of various support systems, such as backup diesel generators, resulting in overall system simplification that benefits both cost and reliability. Thus, it is their potential to achieve enhanced reliability at a low cost that motivates the use of passive systems in innovative reactor designs.

The remainder of this report summarizes the current state-of-the-art in the reliability assessment of passive safety systems. Section II provides examples of passive systems that have been proposed for advanced LWRs. Section III addresses the issue of failure of a passive safety

system, followed by a discussion of various thermal-hydraulic phenomena that are expected to affect the performance of passive systems in Section IV. In Section V, the issue of uncertainty is addressed, including the sources of uncertainty in modeling passive safety systems and the effects of this uncertainty on reliability assessment. Finally, Section VI provides a discussion of existing methodologies and tools for assessing the reliability of passive safety systems.

II. Examples of Passive Systems

The applications of passive systems to reactor safety are numerous. The IAEA currently recognizes four categories of passive safety systems, as listed in Table 1 (IAEA, 1991). Of these, categories B and C have received the most attention of late due to their potential to provide core-cooling without requiring AC power. A quick review of the literature reveals numerous innovative reactor designs that utilize category B and C passive safety systems, the most notable being the latest designs by Westinghouse and GE: the Westinghouse AP1000 and the GE ESBWR (ESBWR 2008, Shultz 2006).

The AP1000 is an advanced PWR that is capable of providing passive core cooling under accident scenarios. This is accomplished through the establishment of various natural circulation cooling loops, including the Passive Residual Heat Removal (PRHR) system and the Passive Containment Cooling System (PCCS). Furthermore, core uncovery is mitigated by various passive injection systems; these systems include the gravity-driven Core Makeup Tank (CMT), accumulators, and the In-containment Refueling Water Storage Tank (IRWST) injection system. In addition, each of these systems injects borated water directly into the core to provide an alternative means of passive shutdown. Reyes (2005) provides a detailed description of the operation of each of these systems.

The ESBWR is an innovative BWR design the employs numerous passive systems to accomplish a variety of safety functions, such as reactivity control, containment heat removal, core depressurization, and inventory control. These functions are achieved through such systems as the Isolation Condenser (IC), Gravity Driven Coolant System (GDCS), and the Passive Containment Cooling System (PCCS). In addition, the ESBWR is notable in that it utilizes natural circulation to provide the main heat transport during normal operation. A brief description of the ESBWR passive systems is provided by Challberg et al. (1998).

Table 1. IAEA Classification for Passive Safety Systems (IAEA, 1991)

Category	Description	Example
A	Physical barriers and static structures	Cladding, piping, containment
B	Moving fluid with no moving parts	Natural circulation cooling systems
C	Moving fluid with moving parts	Gravity-driven make-up tanks and accumulators with check-valves
D	Active Initiation / Passive Execution	Gravity-driven control rods requiring active initiation

III. The Concept of Functional Failure

The increased reliance on passive systems to provide various critical safety functions has not exactly been met with open arms by regulators, who have expressed concerns over designers' capabilities to quantify the reliability of such systems. This is particularly true regarding systems that rely upon thermalhydraulic phenomena such natural circulation (i.e., category B and C passive systems).

It was mentioned above that passive systems are expected to be more reliable than active systems due to decreased reliance on energy sources and intelligent actions; while perhaps true, this assertion remains to be verified. An unfortunate attribute of passive systems is that their driving forces are often weak (Mackay et al., 2007). As a result, the performance of passive systems tends to be sensitive to perturbations in the state of the plant. To illustrate the consequences of this, consider a decay heat removal system operating under natural circulation whose objective is to maintain adequate core cooling to prevent the cladding temperature from exceeding some specified failure limit. In this case, it is helpful to think of the cladding temperature as a load acting on the system, with the failure limit representing the system's capacity to withstand that load. Hence, failure will occur when the load exceeds the capacity. This is the load-capacity failure model, also known as the resistance-stress (R-S) failure model,

familiar to structural reliability (Burgazzi, 2007). For our example, the flow rate, and hence the maximum cladding temperature, may depend strongly on pressure losses in the natural circulation loop; as a result, minor alterations in the total pressure drop, due to corrosion or fouling, for instance, may sufficiently decrease coolant flow to an unacceptable level, resulting in cladding temperature exceeding the failure limit.

In this hypothetical example, no components were assumed to fail, in the traditional sense, yet the passive system was unable to perform its required function due to the degraded condition of the plant. This warrants the consideration of a new type of failure, termed functional failure, applicable to passive systems. The concept of functional failure, as introduced by Burgazzi (2003), refers to the inability of a passive system to perform its intended function when called into operation due to deviations from its expected behavior. Specifically, this concept refers to failures that result from unfavorable initial/boundary conditions or the onset of adverse thermalhydraulic phenomena, rather than traditional active component failures. The term active in the previous statement is important, as the failure of a passive component (e.g., a check valve) would be considered to contribute to functional failure. For instance, a natural circulation system that is initiated by the opening of a check valve may fail if the valve only opens partially, resulting in an increased flow resistance in the system. Pagani et al. (2005) point out that functional failures are generally neglected in actively driven systems because sufficient safety margins exist to preclude their occurrence. Furthermore, the operating point of an active system can usually be easily adjusted to compensate for adverse plant conditions. In the case of passive systems, effective safety margins are reduced due to the uncertainty in predicting system performance. This issue will be discussed at greater detail in the following sections.

IV. Thermalhydraulic Phenomena Affecting Passive System Performance

The previous discussion on functional failure alluded to the possible occurrence of thermalhydraulic phenomena that may impair the performance of category B and C passive systems. Saha (2005) and Vijayan and Nayak (2005) have identified a variety of such phenomena and provide a detailed description of each. The following is a summary of their discussions. It should be noted that, although these phenomena are not necessarily unique to

passive systems, their effects can be more detrimental due to the weak driving forces characteristic of passive systems.

IV.1 Thermal stratification

Thermal stratification refers to a phenomenon wherein horizontal layers of fluid of varying temperature are formed in a large pool. This stratification is the result of a density gradient that forms between the hot and cold fluid; the hotter fluid, being less dense, rises to the top of the pool, and the cooler fluid falls to the bottom. This phenomenon is important for systems with heat exchangers submerged in large pools of water as heat sinks, such as the IRWST. Far from the heat exchanger, the fluid can stagnate in a stable stratified state. Hence, natural circulation will occur only in the vicinity of the heat exchanger, decreasing the overall heat transfer capability of the system (Saha, 2005). In addition, the effective heat capacity of the pool is greatly reduced. As a result, special modeling considerations must be made to determine whether, and under what conditions, thermal stratification will occur, and what effects its occurrence will have on the system.

IV.2 Carryover and Carryunder

Carryover and carryunder are two phenomena of importance in BWRs that operate under natural circulation. In traditional BWRs, separation of the liquid and gaseous phases of the coolant is performed with mechanical steam separators. These mechanical separators introduce a large pressure drop in the system. This pressure drop greatly decreases the performance of natural circulation systems, where the driving head is weak; as a result, many designers have opted to remove the separators, relying instead upon gravity to separate the gaseous and liquid phases (Saha, 2005). Gravity is not as effective a steam separator as traditional mechanical separators, and the possibility exists for entrained liquid to be carried with the steam to the turbine, a process known as carryover. This process is detrimental to the turbine as these entrained water droplets will erode the turbine blades. Similarly, vapor bubbles can become entrained in the liquid as it returns to the core. The result is an overall decrease in density of the recirculation flow, which reduces the driving head leading to reduced flow. Carryover and carryunder depend on a variety of factors such as bubble dynamics, geometry, and interfacial

drag (Saha, 2005). As a result, it is very difficult to accurately model the effects of these phenomena.

IV.3 Condensation in the Presence of Non-condensable Gases

Condensation is known to be greatly impaired in the presence of non-condensable gases. Non-condensable gases tend to be carried with vapor to the walls of the condenser. As the vapor is condensed it is carried away while the non-condensables tend to remain in the vicinity of the condenser. These gases form a barrier to further vapor condensation, as additional vapor must diffuse through the non-condensable gases (Saha, 2005). This effect is particularly important when considering condensation on the walls of the containment, as in the AP1000 PCCS, for example. The containment building contains air, and possibly other non-condensables, that can impede heat transfer through the containment walls. The effect of non-condensable gases may also need to be considered when modeling natural circulation loops in the primary system. In this case, non-condensable gases can enter the primary system through the condenser (in a BWR), which is generally at a vacuum. Fission gases breaching the cladding are another source of non-condensable gases. Although correlations exist to predict the effects of non-condensable gases, accurate modeling of this phenomenon is not a trivial task.

IV.4 Vortex Formation in Pools

This phenomenon refers to the formation of vortices in pools that drain water to the core under the effects of gravity. An example of such a system is the IRWST. The primary concern is that vortices can form near the pool outlet, and under the right conditions, air can become entrained in the fluid as it leaves the pool (Saha, 2005). This results in another source for non-condensable gases in the primary system.

IV.5 Counter-Current Flow Limitation

Counter-Current Flow Limitation (CCFL) is important when considering a two-phase mixture flowing through a pipe, with the liquid phase flowing in the opposite direction as the vapor phase. This situation may arise, for instance, if core makeup water is being injected to the core through the hot leg while, simultaneously, steam is attempting to exit the core. As the two

phases flow against one another, interfacial drag will tend to slow the flow in either direction. This results in a maximum attainable flow rate, and is referred to as CCFL (Saha, 2005). An extreme case would exist when the interfacial drag is sufficient to stop flow in one direction altogether. In the above example, this could result in the inability of the core makeup water to reach the core.

IV.6 Flow Instabilities

Flow instabilities are well recognized phenomena amongst the BWR community. However, due to their rare occurrence in forced-circulation single-phase systems, these phenomena are largely a nonissue to designers of traditional PWRs. On the other hand, natural circulation systems, both single-phase and two-phase, are highly susceptible to flow instabilities. This is a result of the strong coupling that exists between the hydrodynamics and heat transfer in these systems; the flow rate in a natural circulation system is strongly dependent upon the coolant temperature as it exits the core, which, in turn, depends on the flow rate through the core, which is governed by the coolant outlet temperature, and so on. Hence, it is easy to see the potential for flow oscillations in systems that operate under natural circulation. From a safety perspective, flow instabilities are important for a variety of reasons; for instance, flow oscillations can induce mechanical vibrations in system components, potentially subjecting them to fatigue failure (Vijayan and Nayak, 2005). Moreover, flow oscillations may induce premature critical heat flux (CHF), and may further result in power oscillations due to thermalhydraulic-neutronics coupling.

Vijayan and Nayak (2005) provide a very detailed description of various flow instabilities that may be expected to occur in natural circulation systems and provide a discussion on analyzing these phenomena. A particularly important phenomenon in natural circulation systems is the Density Wave Instability (DWI). This is the name given to the type of oscillation described in the previous paragraph. The basic idea is that a natural circulation system will respond to a sudden power increase with an increase in flow due to a decrease in coolant density. This increase in flow will result in a cooler average core outlet temperature, which will, in turn, decrease the flow because of the reduced thermal head. As the flow decreases, the coolant temperature will rise, increasing the flow rate and beginning the cycle anew. Depending on the conditions in the core, the oscillation can either grow indefinitely (unstable), decay (stable), or

converge to a constant amplitude oscillation (limit cycle). If neutronic feedback is sufficient, this phenomenon is classified as a compound dynamic instability (Vijayan and Nayak, 2005).

Additional instabilities that are attributed to boiling inception include flashing and geysering (Vijayan and Nayak, 2005). The former can occur for a single-phase natural circulation system with a tall riser. As the heated fluid rises through the riser, it experiences a decreasing static pressure. If this pressure drops below the vapor pressure of the liquid, the liquid will suddenly flash to vapor, rapidly increasing the buoyancy and flow rate. This will reduce the fluid outlet temperature, as described above, possibly leading to flow oscillations. Geysering is a similar instability that is induced when boiling occurs within the core. In this case, the rising vapor will expand due to decreasing static pressure, leading to a similar behavior. Instabilities of this nature may be an important concern in advanced reactors, namely in situations where boiling is initiated upon system depressurization through the actuation of a series of automatic depressurization valves (ADVs). In such a case, the transition from single-phase to two-phase flow conditions may result in flow oscillations that could challenge the performance of the natural circulation heat removal systems.

V. Uncertainty and the Reliability of Passive Systems

A well posed reliability assessment should address two questions: how likely is the system to fail, and how confident are we in that assessment? Naturally, this is a problem involving uncertainty. The first of these questions addresses the failure probability of the system, which is a product of the inherent variability that exists in the system performance. This randomness, or stochastic variability, is often referred to as aleatory or irreducible uncertainty (Ang and Tang, 2006). The latter terminology arises from the assumption that randomness is inherent to the system, and hence, cannot be removed or reduced. However, this is a bit of a misnomer, as pointed out by Der Kiureghian (2008) who, in quoting Ove Ditlevsen, claims that "[with the exception of] quantum mechanical phenomena inherent variability is reducible by more detailed modeling." The author goes on to claim, "Inherent variability is relative to a level of refinement of the model…. Randomness is not a property of nature but a property of the model" (Der Kiureghian, 2008). For instance, it would, in principle, be possible to precisely model the outcome of a coin toss, but the vast amount of information regarding initial conditions,

as well as the complexity of the model, would render the problem impractical; for most purposes, modeling the coin toss as a 'random' event is good enough. The randomness in this example is inherent to the model, not the system itself. Hence, the claim that aleatory uncertainty is irreducible should be clarified to state that it is irreducible within the current modeling practice or capability.

The second question concerns our confidence that our assessment of the system reliability is accurate. This confidence, or "degree of belief," is represented by epistemic uncertainty and reflects our lack of knowledge of how the system will perform – a lack of knowledge that results from an imperfect knowledge of the system boundary/initial conditions, as well as an inadequate understanding of the various phenomena (Section IV) that can lead to system failure (Apostolakis, 1990). Recall that in Section III it was claimed that the performance of a passive system is highly sensitive to its boundary conditions. A corollary to this claim is that any uncertainty in an analyst's knowledge of the boundary conditions of the system will magnify the uncertainty in the system performance. In fact, it is not only uncertainties in boundary conditions, but also uncertainties in various other system parameters, such as thermal conductivities and pressure form loss coefficients, that complicate our ability of accurately modeling system behavior. As a result, epistemic uncertainties often pose the greatest challenge to reliability assessment.

As we have seen, reliability assessment is really a problem of uncertainty quantification, and as such, it is constructive to identify all the potentially important sources of uncertainty. D'Auria (2004) provides an extensive list of such uncertainties that arise in modeling thermalhydraulic phenomena. The majority of these uncertainties may be classified as model uncertainty. As the name suggests, model uncertainty results from a lack of fidelity between a real system and the necessarily simplified model used to describe the system. However, model uncertainty can be further subdivided into two other categories: representational uncertainty, and solution uncertainty. The former refers to the uncertainty introduced when attempting to represent the physics of a real system with an idealized collection of partial differential equations and other mathematical relations. In the process, various simplifying assumptions are often made; for instance, fluids are often approximated as a continuum to simplify the mathematics. In addition, many complex phenomena are not easily modeled based on first principles; in these cases, constitutive relations based on experimentation are often used. Examples include

interfacial momentum transfer in two phase flow, wall friction, and heat transfer correlations. This introduces further uncertainty due to experimental measurement error and the need to fit complex data structures with simplified continuous mathematical relations. Furthermore, these correlations are often assumed to apply outside of their range of validity or in geometries different from those for which they were derived (D'Auria, 2004).

Solution uncertainty represents the errors introduced when actually solving the representative mathematical model. In almost all cases of interest, these equations must be solved numerically. Hence, the continuous representation is reduced to a discrete representation, resulting in a loss of accuracy. Various numerical errors result as the computational methods employed to solve the discrete equations are limited by machine accuracy. Moreover, solution algorithms generally require averaging of fluid properties over nodes; as a result, improper nodalization can introduce substantial errors. In addition, the governing equations may be further simplified to reduce the complexity of the numerical algorithm and/or to reduce computation speed. D'Auria (2004) points out that many codes are not capable of satisfying the 2^{nd} law of thermodynamics. In addition, codes such as RELAP5 treat all flow as if in a cylindrical pipe. The correlations mentioned above are often only implemented in codes in an approximate form, and interpolation is often employed when these correlations exhibit discontinuities – such is the case when computing heat transfer coefficients in the transition flow regime. Finally, the individuals who developed the codes are only human and subject to error. These examples comprise only a subset of the possible sources of model uncertainty.

The solution of a system of differential equation requires not only a statement of the equations to be solved (the model), but also a statement of the initial conditions and boundary conditions (the inputs). Hence, another class of uncertainty exists that is important for reliability assessment of passive systems, known as input uncertainty. In many cases, the conditions of the plant at the instant a passive system is called into operation are not precisely known. Thus, the initial conditions, such as primary system pressure or heat sink temperature, are subject to a great deal of variability; this variability may be of either aleatory or epistemic nature, or both. In addition, the boundary conditions will also be subject to uncertainty, as will be the case in a LOCA condition when the break size is not precisely known, or when considering condensation when the presence of non-condensable gases is unknown.

The final class of uncertainty to be considered is statistical uncertainty. Statistical uncertainty arises any time inferences are made on a population based on information acquired from a finite sample. In the present case, the population refers to the spectrum of all possible system conditions that result when accounting for each of the aforementioned uncertainties. Statistical uncertainty results because only a finite number of model simulations (samples) can reasonably be performed, and its magnitude will vary inversely with this number. As a result, statistical uncertainty is reducible, and is rightfully classified as an epistemic uncertainty.

VI. Existing Methodologies and Tools for the Reliability Assessment of Passive Systems

To summarize the previous sections, the overall objective of reliability assessment is to quantify the probability of functional failure of passive systems resulting from both the failure of passive components, such as pipes and check valves, and the occurrence of various performance-impairing phenomena. In addition, it is imperative to quantify each of the aforementioned epistemic uncertainties in an attempt to assess their effect on our estimation of the system failure probability. It should be mentioned that the end goal of a reliability assessment requires to incorporation of the passive system reliability into the overall plant PRA. To this end, a variety of approaches have been proposed, both domestically and abroad, the most promising of which are discussed below.

VI.1 Fault Tree Approach to System Reliability

An early approach proposed by Burgazzi (2002) involves the construction of fault trees to assess the failure probability of passive systems. This approach considers first the reliability of a passive system to be the product of both the reliability of system components and the reliability of the passive function. Hence, two branches will extend from the top failure event in a fault tree, connected by an "OR" gate. Each branch corresponds to either component failure or functional failure, as illustrated in Fig. 1 (Burgazzi, 2002). At this point, a traditional fault tree evaluation is performed to determine the failure logic for system components. The assessment of functional failure is performed in a similar manner by relating the failure of the system to a series of degraded states in which the system can exist; an example of a degraded state would be a high concentration of non-condensable gases. Finally, the probability that these degraded states will

be realized is expressed in terms of the failure probability of various components, such as non-condensable vent valves, that are designed to prevent these conditions. Alternatively, the probability of realizing a degraded state can be expressed in terms of a basic occurrence, such as

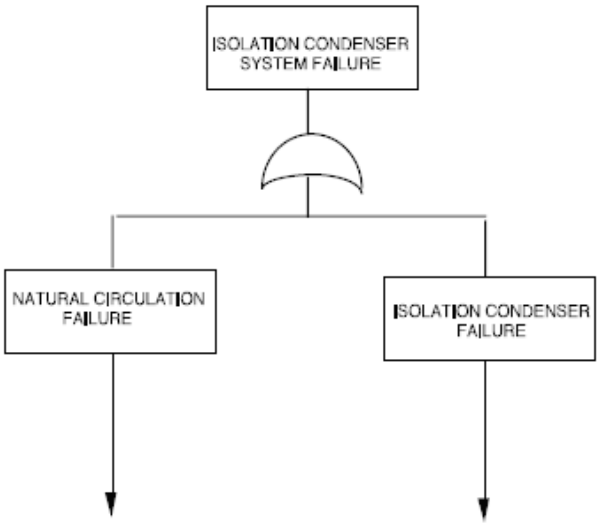

Fig. 1. Example top-level fault tree for passive IC system (Burgazzi, 2002)

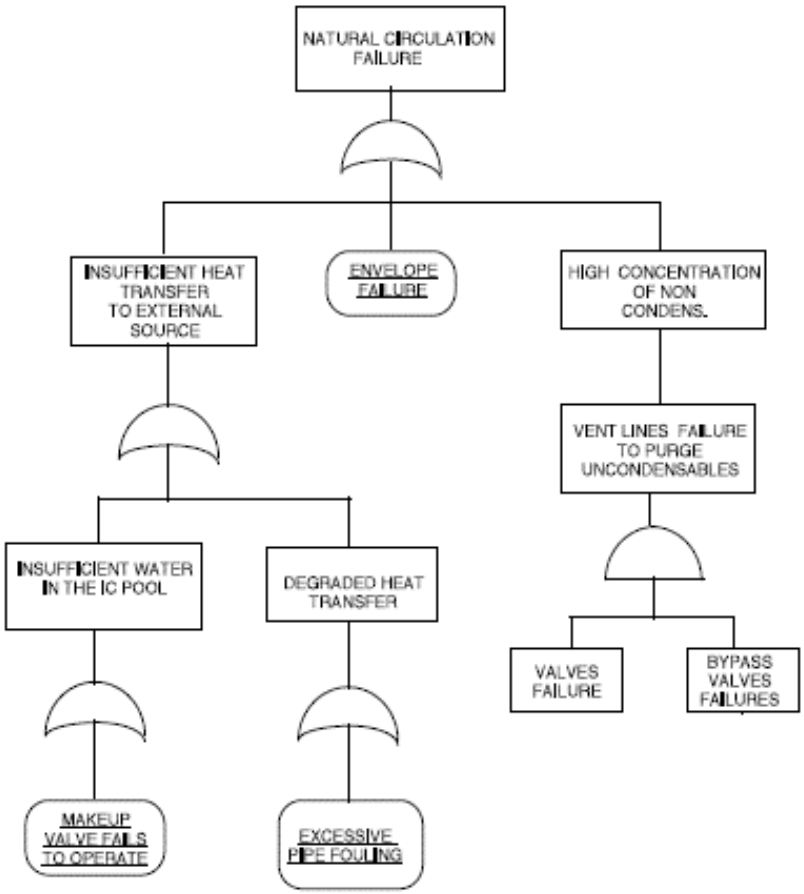

Fig. 2. Fault tree for natural circulation functional failure in IC system (Burgazzi, 2002)

excessive pipe fouling. Figure 2 illustrates the breakdown of natural circulation failure in such a fault tree representation (Burgazzi, 2002).

The primary advantage of this approach to passive system reliability is that it allows ease of implementation of the passive system failure probability into the overall plant PRA. This is because the system failure is expressed in terms of a fault tree, essentially making the system indistinguishable from other active systems in the PRA. However, a variety of limitations exist regarding this approach. To the author's credit, it is admitted that this approach "represents a simplification of the matter whose treatment should encompass a wider research ranging from both the thermal-hydraulic and probabilistic analysis" (Burgazzi, 2002). This approach is only meant to illustrate, at a high level, a possible approach to implementing the reliability of passive systems with other active systems. That being said, one of the main limitations of the approach

concerns the definition of many of the basic fault events, such as excessive pipe fouling. Specifically, the term “excessive” is not well defined, and its exact definition will likely have a large impact on the system failure probability. Furthermore, due to the complexity of passive thermalhydraulic phenomena and the synergism that exists between the various phenomena, it is foreseeable that the appropriate definition for “excessive” will depend upon other conditions in the system. To be more precise, suppose that there exists a specific amount of pipe fouling that is sufficient to fail the system when all other components in the system are in their nominal operating conditions (i.e., not failed). Then, according to the fault tree in Fig. 2, the probability of degraded heat transfer would be simply the probability of achieving that amount of pipe fouling. On the other hand, suppose that the non-condensable vent valves suffer partial failure, resulting in a condition of “low” concentration of non-condensable gases in the system, as compared to the “high” concentration that is necessary to fail the system on its own. In this case, the condensation behavior of the system will be somewhat degraded and a lower degree of pipe fouling (compared to above) may be sufficient to fail the system. Thus, the synergism between different phenomena in the natural circulation system may introduce complex dependencies in the fault tree that cannot be easily accounted for.

An additional limitation of this approach concerns the ability to identify the failure modes of the passive system, including the relevant thermalhydraulic phenomena and the component failures that lead to their occurrence. In later papers, Burgazzi (2004, 2006) describes two qualitative hazard identification tools, Failure Modes and Effects Analysis (FMEA) and Hazard and Operability (HAZOP), that may be capable of assisting analysts in identifying these failure modes. These tools are discussed in the following.

VI.2 FMEA and HAZOP

FMEA is a component level approach, wherein each component in the passive system is identified; in addition, a “virtual” component may be introduced to represent the passive function, such as natural circulation. Following the identification of all system components, the failure modes of each component are identified, followed by a consideration of failure causes. The next steps include the identification of possible preventative and mitigative measures to be taken and the identification of the failure consequences on the system. FMEA is highly qualitative, requiring input from various experts to identify the failure causes of the system

components and their consequences. As such, its usefulness in reliability analysis is limited. The main utility in utilizing an approach such as FMEA is to provide a framework to structure the experts' thought processes and to focus their attention toward basic system processes and dependencies in the hopes of identifying hard-to-spot failures.

An alternative approach proposed by Burgazzi (2004) is the HAZOP methodology. HAZOP is a parameter-based approach, focusing attention on fundamental system parameters (i.e. temperature, pressure, flow rate, etc.) and their effects on system performance. This method requires the identification of all relevant system parameters. Subsequently, a collection of guide words (such as more of, less of, none, etc.) are applied to each parameter. The objective is to force the analyst to consider various "what if" scenarios to illicit valuable information concerning system failure modes. Again, this method is qualitative and is only as valuable as the experts using it. Additionally, the identification of all of the relevant parameters is often a challenging task. Zio et al. (2003) have proposed to use the Analytic Hierarchy Process (AHP) as a tool for parameter identification and ranking based on experts' opinions regarding parameter importance. The AHP is discussed in greater detail in the subsequent section.

VI.3 The Analytic Hierarchy Process for Parameter Identification and Ranking

The Analytic Hierarchy Process was first proposed by Saaty (1980) as a priority ranking tool to be used when making complex decisions. Since its inception, the AHP has enjoyed great success and has recently been recognized by Zio et al. (2003) for its potential applications to reliability assessment of passive systems. The AHP provides a systematic method for decomposing a complex system into a collection of thermal-hydraulic phenomena and the basic parameters that affect those phenomena. In addition, the AHP can be used to qualitatively rank parameters based on expert judgments regarding the influence of these parameters on system performance. The method works by first identifying a top goal, which is generally defined as the high-level objective of the passive system; for instance, the top goal might be to remove decay heat from the core, with a lower-level system objective being to prevent the cladding or fuel from overheating. Next, the components of the system are identified; within each component, various thermalhydraulic phenomena are expected to occur, and these are identified next. Subsequently, each of the identified phenomena is expressed in terms of general parameters, such as heat transfer coefficients and pressure drops. An illustration of such a hierarchy is

provided in Fig. 3 for the example of an isolation condenser taken from Zio et al. (2003). The final steps involve continued decomposition of the general parameters into increasing basic parameters. The bottom of the hierarchy should consist of the most basic system parameters, such as geometries, material properties, or state variables such as temperature and pressure.

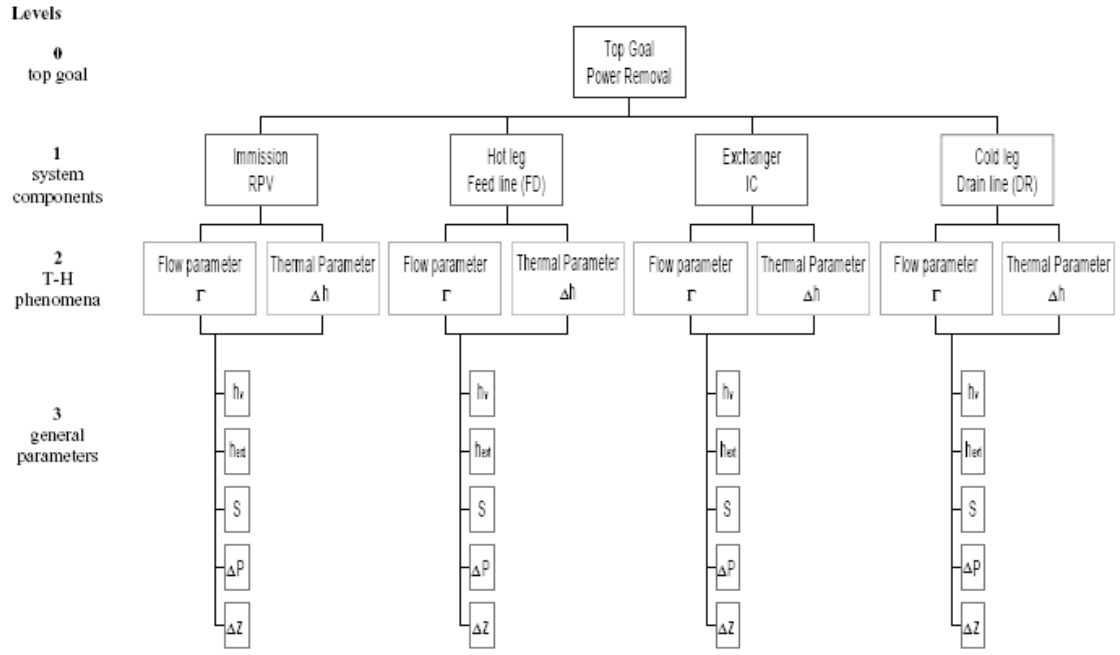

Fig. 3. Example of parameter decomposition via AHP (Zio et al., 2003)

It was stated previously that the AHP can be used to rank parameters based on their expected influence on system performance (the top goal). This is accomplished by assembling a panel of experts and having each perform pairwise comparisons of different parameters. At each level in the hierarchy, the parameters are comparatively ranked on a scale from 1 to 9 based on their effect on the next highest level. The results are arranged in a matrix, and the principal eigenvector of that matrix provides the appropriate ranking. More details are provided by Zio et al. (2003). As an example application of the AHP, Zio et al. (2003) considered an isolation condenser system, the partial hierarchy for which is illustrated in Fig. 3. The authors identified 32 basic parameters that were expected to influence the system performance. In addition, the parameters were ranked based on judgments from five different experts. The eleven most important parameters were identified and compared to the eleven most important parameters

identified through a quantitative sensitivity analysis using standardized regression coefficients. The results show good agreement regarding the parameters that were identified to be important; however, the actual rank of the parameters between the studies differed (Zio et al., 2003). This indicates that the AHP may be useful for screening the most important parameters provided that a large enough subset of the original parameters remains after the screening process. What is meant by 'large enough' is another issue altogether, but from the results in this example, large enough seems to be on the order of 10 parameters.

VI.4 APSRA Methodology

Nayak et al. (2007, 2008) have proposed an alternative methodology for reliability assessment of passive systems, which they have named Assessment of Passive System ReliAbility (APSRA). Figure 4, taken from these references, illustrates the major steps of the APSRA methodology. The first four steps can be considered the preprocessing phase. In this phase, the problem is defined (Step I) and all parameters that affect the system are identified (Step II). Step III includes identifying the failure criteria; that is, identifying what the mission of the system is, and what constitutes failure of that mission. In addition, identification of operational characteristics entails using simplified codes to approximate the behavior of the system to get a feel for what parameters will have the greatest effect on the system performance; this is essentially a sort of sensitivity study using approximate models. Based on the results from this sensitivity study, the key parameters that have the largest impact on system performance are identified in Step V. These parameters will be the subject of further consideration in the remaining analysis, and those parameters that do not greatly affect the system are neglected. Strictly speaking, the preprocessing phase should also include a step for model development. The APSRA methodology calls for the development of two different models; the first is a simplified model discussed previously, and the second is a best-estimate model, using a code such as RELAP5, which will be used in the subsequent steps.

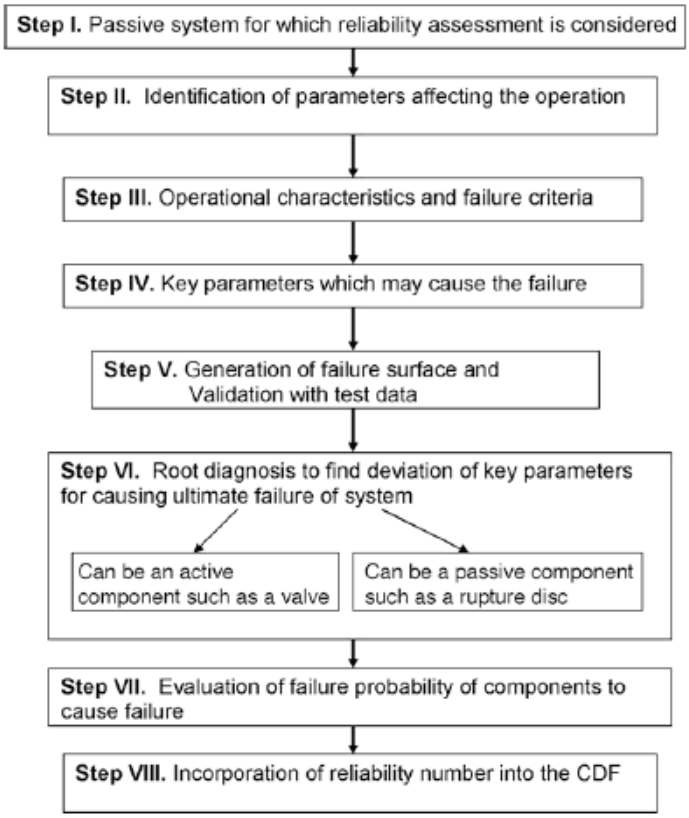

Fig. 4 The APSRA Methodology (Nayak et al., 2008)

After identifying the key parameters and developing the best-estimate system model, Step VI requires the generation of a failure surface, i.e., a surface in the parameter space of the model that marks the boundary between successful and failed system operation. The failure surface is generated by performing a series of simulations with the best-estimate model using a variety of possible parameter values. The authors indicate that the outcomes of these trials are noted (success or failure), and the failure surface is generated accordingly; however, the details of this process have yet to be presented in the literature. Once the failure surface has been generated, it is subject to an extensive experimental validation procedure to quantify the uncertainties in the ability of the best-estimate model to predict success and failure. This validation process is performed on-site at various experimental facilities located at the Bhaba Atomic Research Centre (Nayak et al., 2007, 2008). This step is performed due to the recognition that a great deal of model uncertainty exists when attempting to simulate complex thermal hydraulic phenomena, as discussed in Section V; in particular, the authors note the difficulties in modeling low-flow natural circulation, flow instabilities, CHF during flow oscillations, condensation in the presence

on non-condensable gases, and thermal stratification (Nayak et al., 2008). Most of these phenomena have been described in detail in Section IV. The concern with modeling low-flow natural circulation is due to the difficulty, or even the impossibility, of modeling multi-dimensional flow that may not be fully developed with commonly used systems codes such as RELAP5 (Nayak et al., 2008).

Once the failure surface has been generated, and the uncertainties quantified, a process termed root diagnosis is performed to identify the components whose failures will result in unfavorable parameter deviations, thus failing the system. This is yet another area where the authors fail to provide a great deal of detail, and it is unclear how the authors propose to identify these components. A similar concern was expressed in the discussion regarding the fault tree methodology proposed by Burgazzi. In fact, at this point in the APSRA methodology, the two approaches are very similar; a fault tree for the passive system is created considering the failures of active and passive components, and this fault tree is used to compute the failure probability of system.

The authors have applied the APSRA methodology to assess the failure probability of the Main Heat Transport (MHT) natural circulation system in the Advanced Heavy Water Reactor (AHWR). As a two-phase natural circulation system, the authors have placed considerable emphasis on the occurrence of flow oscillations that can challenge the system performance. The authors claim to have successfully generated a failure surface for the MHT system; however, at the time of publication, no validation experiments had been performed (Nayak et al., 2008). Moreover, the authors' considerable ambiguity in their discussion of failure surface generation and root diagnosis make it difficult to critically evaluate this work. These two tasks are suspected to introduce complications to the analysis and limit its utility, from a practical perspective; yet, without a detailed discussion describing these processes, it is impossible to draw any conclusions. Furthermore, the failure surface that is generated is plant specific, and the uncertainty quantification results from one plant will not be easily adaptable to other plants and systems. As a result, the explicit reliance upon experimentation to quantify the uncertainties in the failure surface may limit the applicability of this approach for plants in which not experimental facilities are available: for instance, new plants that only exist in the early design phase.

VI.5 The RMPS Methodology

In 1999, The Italian National Agency for New Technologies, Energy, and the Environment (ENEA), in collaboration with the University of Pisa and the Polytechnic of Milano, began the development of a new methodology for reliability assessment called REPAS (Reliability Evaluation of PAssive Systems) (EPRI 2007, Jafari et al. 2003, Ricotti et al. 2002). This work laid the foundation for the development of yet another methodology, RMPS (Reliability Methods for Passive Safety functions), beginning in 2001 (Marquès et al. 2005). The development of RMPS was sponsored by the European Union and was carried out by the French Commissariat à l'Energie Atomique (CEA) in collaboration with various European research centers and universities. Figure 5 illustrates the flow diagram for the RMPS methodology (Marquès et al., 2005). Although the diagram appears complicated, the methodology can be described by three phases: a preprocessing and model development phase, a simulation and propagation phase, and an analysis/post-processing phase. Each of these steps is described in the following.

The preprocessing phase of the RMPS methodology is similar to the first several steps of the APSRA methodology and consists first of identifying the system and its intended mission. The mission of the system should be representable by a measurable quantity that can be used to specify the success/failure criteria of the system; an example could be peak cladding temperature (PCT), with the success criteria being to prevent the PCT from exceeding, say, 1204°C. There may exist multiple success/failure criteria corresponding to different components or failure mechanisms; for instance, one success criterion could be to limit the PCT, whereas another success criterion could require limiting the maximum temperature differential at the core outlet to prevent thermal stresses due to strong temperature gradients. Another important step is to identify all the phenomena that may impair system performance (the failure modes); this process may be assisted by the use of methods such as FMEA or HAZOP, as discussed above. Concurrent to this task should be the development of a best-estimate model to employ for system

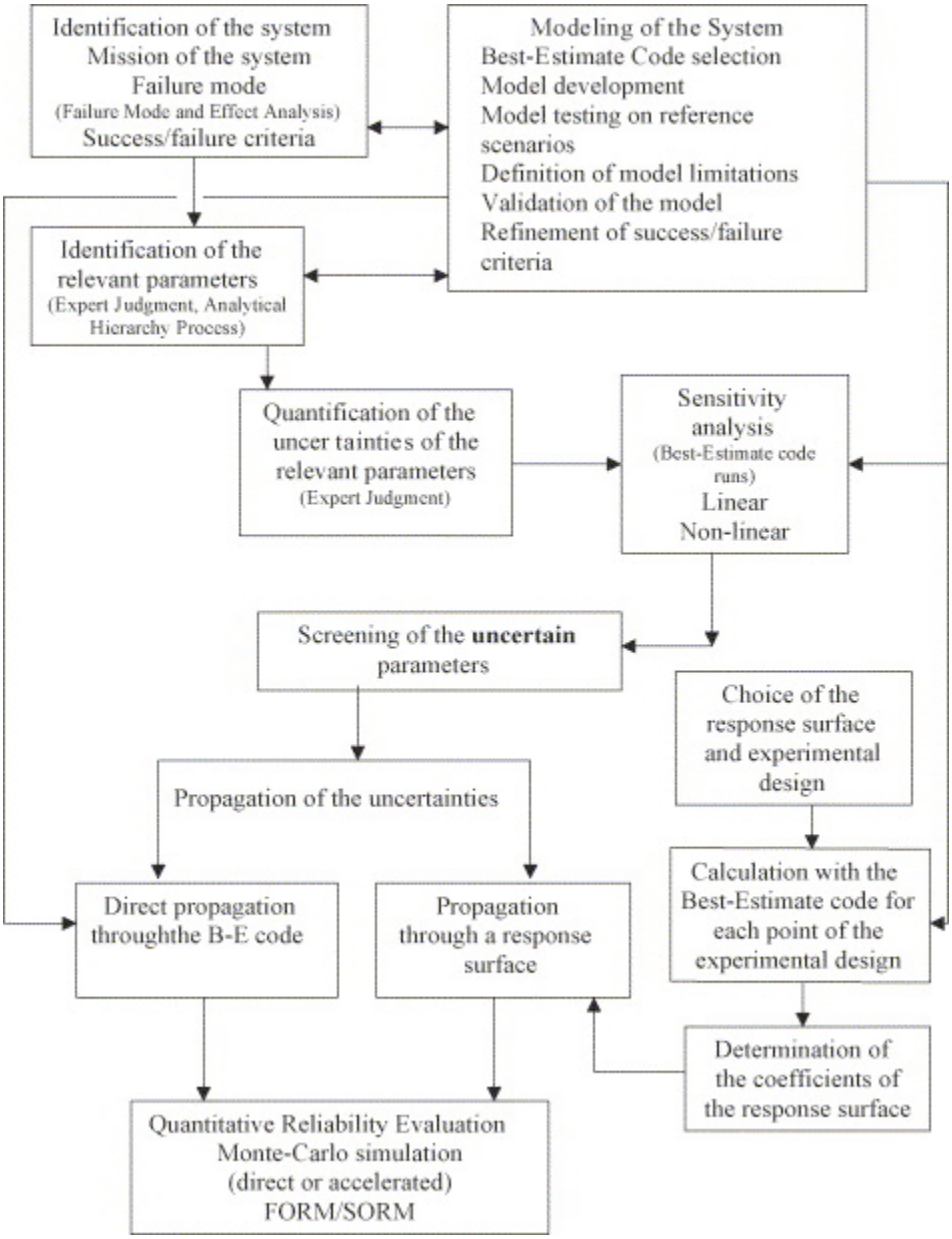

Fig. 5 RMPS methodology flowchart (Marquès et al., 2005)

simulations. If possible, the model should be validated by comparisons with existing experimental data. Additionally, the model may assist in identifying unforeseen failure modes, such as instabilities. The next steps include identifying all the system parameters that are expected to influence the system's performance and screening the most important parameters. The identification and initial screening can be accomplished via the aforementioned AHP, and additional screening of parameters can be accomplished by conducting sensitivity studies using

the best-estimate model to identify the parameters to which the system is most sensitive. Numerous methods of varying complexity (i.e., linear vs. nonlinear) exist for performing these studies (Saltelli et al. 2000, Saltelli et al. 2004).

The next step marks the point where the RMPS methodology differs significantly from the APSRA methodology. The authors of the RMPS methodology have attempted to attribute the uncertainty in passive system performance to the uncertainty in the initial conditions and boundary conditions of the system (Marquès et al. 2005, Marquès et al. 2002). In other words, a considerable amount of uncertainty exists in the exact values of the initial/boundary conditions when the system is called into operation, and this uncertainty is largely responsible for our lack of knowledge of how the system will perform. As a result, these uncertainties in the input parameters need to be quantified in terms of probability density functions. If sufficient data for the parameters are available, these data can be used to generate appropriate density functions using goodness-of-fit tests. However, if available data are insufficient, as is usually the case for applications regarding new or innovative reactor systems, expert judgment will be necessary to select the distributions (Marquès et al., 2005). It is important that any dependencies between different parameters be identified and accounted for, either by correlation matrices or explicit functional relations; this task is very difficult when relying upon expert judgment.

After completing each of the above tasks comes the simulation and propagation phase of the methodology. The goal is to quantitatively assess the impact of uncertainty in the input parameters on the system performance and to compute the failure probability of the system. The authors have identified two approaches for accomplishing this task. The first is regarded as direct-sampling, and the idea is to propagate the uncertainties in the input parameters directly through the code model to obtain the uncertainty in the system performance. This is performed through a number of Monte-Carlo simulations, wherein the input parameter values are randomly selected based on their respective distributions and the code is run for each collection of inputs. The failure probability is then computed by dividing the number of simulations that resulted in failure by the total number of simulations performed. While this is a rather straightforward approach to computing the failure probability, there are a number of drawbacks. First and foremost is that the number of simulations necessary to accurately predict the failure probability is usually quite large; if only a few simulations are performed, the statistical uncertainty will be quite large and the variance in the predicted probability will be high. In addition, failure of the

system is expected to be quite rare, requiring parameters to take on improbable values (the tails of the distributions). As a result, a high number of simulations must be performed to guarantee that the tails of these distributions have been sampled. This is complicated by the fact that the simulations themselves are usually very time-consuming, on the order of several hours (Marquès et al., 2005). Variance reduction techniques, such as stratified sampling and importance sampling, may be able to provide some relief by allowing for more accurate predictions with fewer simulations; however, the benefits of using such techniques are limited and further complicate the analysis.

The second proposed approach is to develop a response surface to approximate the output from the best-estimate model. The response surface is a mathematically simplified model, such as a polynomial surface, that is used to approximate the actual model. To develop the response surface, parameter values are judiciously selected based on experimental design techniques, such as fractional factorial designs or Taguchi orthogonal arrays (Box and Draper 2007, Roy 1990). Simulations are performed for each of the selected collections of parameters, and the results are then fitted with a surface in parameter space, similar to least-squares regression. The assumption, then, is that this fitted surface well-represents the system behavior for all parameter values. The failure probability is then computed by propagating the input uncertainty through the response surface, as opposed to the original best-estimate model. The use of the response surface greatly improves computation speed; hence, many more samples can be drawn than what would have otherwise been feasible due to time-constraints. This allows for a reduction in statistical uncertainty in predicting the failure probability. The drawback is that the response surface is, by definition, a simplification of the original model, and therefore introduces additional epistemic uncertainty. This uncertainty can be estimated based on the fidelity between the original model and the response surface (expressed in terms of the coefficient of determination (Fong et al. 2008). Thus, the assumption that the response surface represents well the system behavior for parameter values can be clarified to mean that all deviations from the response-surface predictions are accounted for by this uncertainty. Unfortunately, this need not be the case, nor is it possible to prove this assumption to be valid.

The final step of the RMPS methodology requires incorporating the computed passive system failure probability into the overall plant PRA. Marquès et al. (2005) propose to accomplish this task by adding an event corresponding to passive system failure to any event tree

for any accident sequence where the system is expected to participate. The authors present an example of using the RMPS methodology to estimate the failure probability for the Residual Passive Heat Removal system on the Primary circuit (RP2) during a Total Loss of Power Supply event. The RP2 system is similar to the PRHR system in the AP1000. The authors identified 24 parameters that were expected to influence system behavior, including the initial level of water in the heat sink pools, the amount of fouling in the heat exchanger tubes, the initial power level, and the instant at which the isolation valves are opened. Additionally, uncertainty in the selected ANS decay heat curve was expected to contribute to the failure probability. Indeed, the authors conclude based on sensitivity studies that the ANS curve uncertainty contributed the most to system failure probability (Marquès et al., 2005). Additional uncertain parameters that were deemed of high importance include the heat sink pool levels and the amount of non-condensable gases present (Marquès et al., 2005). Another partial application of the RMPS methodology was applied by Marquès et al. (2002) to the isolation condenser system. In this example, the system pressure was determined to be the most important parameter, followed by the collapsed water level in the RPV and the heat sink pool level. It should be noted that model uncertainty is not accounted for in the published examples for the RMPS methodology (Marquès et al., 2005).

VI.6 Contributions from MIT

Various studies have been conducted at MIT concerning the reliability of passive safety systems. These studies have been more focused on the passive systems utilized in advanced reactor designs, as opposed to LWRs. Moreover, these studies were aimed primarily at identifying potential design options to improve safety. A series of studies have been published regarding the reliability of a passive decay heat removal (DHR) system in a gas-cooled fast reactor (GFR) (Pagani et al. 2005, Mackay et al. 2007, Fong et al. 2008). In the first of these studies, described by Pagani et al. (2005), a simplified steady-state model was considered. The approach that was adopted for the reliability assessment was very similar to that of the RMPS methodology, with the exception of the treatment of model uncertainty. Pagani et al. (2005) recognized that model uncertainty can be attributed to errors in the correlations used to predict various thermalhydraulic parameters, such as Nusselt numbers and friction factors. Thus, the authors propose to use the adjustment factor approach, which requires introducing a distributed multiplicative (or additive) factor that represents epistemic uncertainty in the model (Pagani et al.

2005, Zio and Apostolakis 1996). For simplicity, the authors assumed that all of the uncertain parameters and adjustment factors were normally distributed, with means and standard deviations based on industry practice and experience or expert judgment (Pagani et al., 2005). Pagani et al. (2005) conclude that a passive system can actually be less reliable than an active system designed to accomplish the same mission. This is because of the high epistemic uncertainty associated with passive system performance that results in a degraded safety margin. Further, the authors conclude that passive systems may benefit more from redundancy than active systems.

Recognizing the modeling limitations of the previous analysis, Mackay et al. (2007) expand the analysis to account for transient effects by modeling the system in RELAP5. Due to the increased computation time necessary to perform transient simulations, the authors opted to use a stratified sampling technique, known as Latin Hypercube Sampling (LHS), to propagate the parameter and model uncertainties (Mackay et al., 2007). This allowed for a reduction in the number of simulations that needed to be performed to more reasonable levels. The analysis revealed that when multiple DHR loops were modeled, the coolant flow was capable of bypassing the core by flowing between multiple cooling loops. In some cases, flow reversal was observed in the core. This was due to the large pressure drop in the core, and the tendency for the flow to choose the path of least resistance. These results provide warning against modeling only a single coolant loop and assuming that the additional loops will perform similarly. In addition, check valve leakage was identified as an important parameter for its effect on DHR performance.

Fong et al. present results from the reliability assessment of two decay heat removal systems working in parallel in the lead-cooled Flexible Conversion Ratio Reactor (FCCR). The two systems analyzed were the Reactor Vessel Auxiliary Cooling System (RVACS) and the Passive Secondary Auxiliary Cooling System (PSACS). The computation time to perform simulations is particularly limiting in this work. Due to the high thermal capacity of the lead coolant, and the consequent slowly evolving system transients, the mission time for these systems was taken to be 72 hours (Fong et al. 2008). As a result, the time to perform each simulation, performed with RELAP5-3D, was on the order of 30 hours. This provided strong motivation to pursue the response surface technique discussed previously. The authors selected 5 parameters for the reliability study, and these parameters were used to construct a quadratic

response surface. Additionally, the authors found that this quadratic response surface was able to provide a good fit to the simulated data. The response surface error was estimated based on the approximately normally distributed residuals, and it was found that the reliability estimate for the system is strongly dependent upon this error.

References

1. Ang, A.H-S., Tang, W.H., *Probability Concepts in Engineering: Emphasis on Applications to Civil and Environmental Engineering*, 2nd Ed., Wiley, 2006.

2. Apostolakis, G.E., "The Concept of Probability in Safety Assessments of Technological Systems," *Science*, Vol. 250, pp. 1359-1364, 1990.

3. Box, G.E.P., Draper, N.R., *Response Surfaces, Mixtures, and Ridge Analyses*, 2nd Ed., Wiley, 2007.

4. Burgazzi, L., "Passive System Reliability Analysis: A Study on the Isolation Condenser," *Nuclear Technology*, Vol. 139, pp. 3-9, 2002.

5. Burgazzi, L., "Reliability Evaluation of Passive Systems Through Functional Reliability Assessment," *Nuclear Technology*, Vol. 144, pp. 145-151, 2003.

6. Burgazzi, L., "Evaluation of Uncertainties Related to Passive Systems Performance," *Nuclear Engineering and Design*, 230, pp. 93-106, 2004.

7. Burgazzi, L., "Failure Mode and Effect Analysis Application for the Safety and Reliability Analysis of a Thermal-Hydraulic Passive System," *Nuclear Technology*, Vol. 156, pp. 150-158, 2006.

8. Burgazzi, L., "Thermal-Hydraulic Passive System Reliability-Based Design Approach," *Reliability Engineering and System Safety*, 92, pp. 1250-1257, 2007.

9. Challberg, R.C., Cheung, Y.K., Khorana, S.S., Upton, H.A., "ESBWR Evolution of Passive Features," Proc. of ICONE 6, May 10-14, 1998.

10. D'Auria, F., "Approach and Methods to Evaluate the Uncertainties in System Thermalhydraulic Calculations," *Mecánica Computacional*, Vol. 23, pp. 1411-1425, 2004.

11. Der Kiureghian, A., "Analysis of Structural Reliability Under Parameter Uncertainties," To be published in *Probabilistic Engineering Mechanics*, Available online March 2008.

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

13. ESBWR Fact Sheet, http://www.ge-energy.com/prod_serv/products/nuclear_energy/en/new_reactors/esbwr.htm, Aug. 17, 2008.

14. Fong, C.J., and Apostolakis, G.E., "The Use of Response Surface Methodology to Perform Uncertainty Analyses on Passive Safety Systems," Proceedings of *PSA '08*,

International Topical Meeting on Probabilistic Safety Assessment, Knoxville, Tennessee, September 7–11, 2008, American Nuclear Society, La Grange Park, Illinois.

15. International Atomic Energy Agency, *Safety Related Terms for Advanced Nuclear Plants*, IAEA-TECDOC-626, Vienna, Austria, 1991.

16. Jafari, J., D'Auria, F., Kazeminejad, H., Davilu, H., "Reliability Evaluation of a Natural Circulation System," *Nuclear Engineering and Design*, 225, pp. 79-104, 2003.

17. Mackay, F.J., Apostolakis, G.E., Hejzlar, P., "Incorporating Reliability Analysis into the Design of Passive Cooling Systems with an Application to a Gas-Cooled Reactor," *Nuclear Engineering and Design*, Vol. 238, Issue 1, pp. 217-228, 2007.

18. Marquès, M., Pignatel, J.F., D'Auria, F., Burgazzi, L., Müller, C., Cojazzi, G., La Lumia, V., "Reliability Methods for Passive Safety Functions," Proc. of ICONE 10, April 14-18, 2002.

19. Marquès, M., Pignatel, J.F., Sagnes, P., D'Auria, F., Burgazzi, L., Müller, C., Bolado-Lavin, R., Kirchsteiger, C., La Lumia, V., Ivanov, I., "Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment," *Nuclear Engineering and Design*, 235, pp. 2612-2631, 2005.

20. Nayak, A.K., Sinha, R.K., "Role of Passive Systems in Advanced Reactors," *Progress in Nuclear Energy*, 49, pp. 486-498, 2007.

21. Nayak, A.K., Gartia, M.R., Antony, A., Vinod, G., Sinha, R.K., "Passive System Reliability Analysis Using the APSRA Methodology," *Nuclear Engineering and Design*, Vol. 238, Issue 6, pp. 1430-1440, 2008.

22. Pagani, L.P., Apostolakis, G.E., Hejzlar, P., "The Impact of Uncertainties on the Performance of Passive Systems," *Nuclear Technology*, Vol. 149, pp. 129-140, 2005.

23. Reyes, J.N., *Natural Circulation in Water Cooled Nuclear Power Plants: Phenomena, Models, and Methodology for Reliability Assessments*, IAEA-TECDOC-1474, Annex 12, Vienna, Austria, 2005.

24. Ricotti, M.E., Bianchi, F., Burgazzi, L., D'Auria, F., Galassi, G., "The REPAS Study: Reliability Evaluation of Passive Safety Systems," Proc. of ICONE 10, April 14-18, 2002.

25. Roy, R.K., *A Primer on the Taguchi Method*, Society of Manufacturing, 1990.

26. Saaty, T.L., *The Analytic Hierarchy Process*, McGraw-Hill, New York, 1980.

27. Saha, D., *Natural Circulation in Water Cooled Nuclear Power Plants: Phenomena, Models, and Methodology for Reliability Assessments*, IAEA-TECDOC-1474, Annex 5, Vienna, Austria, 2005.

28. Saltelli, A., Tarantola, S., Campolongo, F., Ratto, M., *Sensitivity Analysis in Practice: A Guide to Assessing Scientific Models*, Wiley, 2004.

29. Saltelli, A., Chan, K., Scott, E.M., *Sensitivity Analysis*, Wiley, 2000.

30. Shultz, T.L., "Westinghouse AP1000 Advanced Passive Plant," *Nuclear Engineering and Design*, 236, pp. 1547-1557, 2006.

31. Vijayan, P.K., Nayak, A.K., *Natural Circulation in Water Cooled Nuclear Power Plants: Phenomena, Models, and Methodology for Reliability Assessments*, IAEA-TECDOC-1474, Annex 7, Vienna, Austria, 2005.

32. Zio, E., Apostolakis, G.E., "Two Methods for the Structured Assessment of Model Uncertainty by Experts in Performance Assessments of Radioactive Waste Repositories," *Reliability Engineering and System Safety*, 54, pp. 225-241, 1996.

33. Zio, E., Cantarella, A., Cammi, A., "The Analytic Hierarchy Process as a Systematic Approach to the Identification of Important Parameters for the Reliability Assessment of Passive Systems," *Nuclear Engineering and Design*, 226, pp. 311-336, 2003.