

**RISK-INFORMED DESIGN GUIDANCE FOR FUTURE
REACTOR SYSTEMS**

by

MICHAEL J. DELANEY, GEORGE E. APOSTOLAKIS*, AND MICHAEL J.
DRISCOLL

Department of Nuclear Engineering, Room 24-221
Massachusetts Institute of Technology
Cambridge, MA 02139-4307, USA

* Corresponding author. Email address: apostola@mit.edu; Fax: +1-617-258-8863

ABSTRACT

Future reactor designs face an uncertain regulatory environment. It is anticipated that there will be some level of probabilistic insights in the regulations and supporting regulatory documents for Generation-IV nuclear reactors. Central to current regulations are Design Basis Accidents (DBAs) and the General Design Criteria (GDC), which were established before probabilistic risk assessments (PRAs) were developed. These regulations implement a structuralist approach to safety through traditional defense in depth and large safety margins. In a rationalist approach to safety, accident frequencies are quantified and protective measures are introduced to make these frequencies acceptably low. Both approaches have advantages and disadvantages and future reactor design and licensing processes will have to implement a hybrid approach. This paper presents an iterative four-step risk-informed methodology to guide the design of future-reactor systems using a gas-cooled fast reactor emergency core cooling system as an example. This methodology helps designers to analyze alternative designs under potential risk-informed regulations and to anticipate design justifications the regulator may require during the licensing process. The analysis demonstrated the importance of common-cause failures and the need for guidance on how to change the quantitative impact of these potential failures on the frequency of accident sequences as the design changes. Deliberation is an important part of the four-step methodology because it supplements the quantitative results by allowing the inclusion in the design choice of elements such as best design practices and ease of online maintenance, which usually cannot be quantified. The case study showed that, in some instances, the structuralist and the rationalist approaches were inconsistent. In particular, GDC 35 treats the double-ended break of the largest pipe in the reactor coolant system with concurrent loss of offsite power and a single failure in the most critical place as the DBA for the emergency core cooling system. Seventeen out of the forty-five variations that we considered violated this DBA. Using PRA techniques, we found that the mean frequency of this accident was very low, thus indicating that deterministic criteria such as GDC 35 must be reassessed in the light of risk insights.

1. INTRODUCTION

New nuclear reactor concepts face many design and licensing challenges and advanced reactor designs are competing against one another for funding in a technology downselect process. It is implicitly understood in the Generation-IV competition that a preferred advanced reactor design must be easily licensed and competitive in the future market with other energy sources.

The Generation-IV Technology Roadmap (US Department of Energy, 2002) has proposed a number of objectives for future nuclear energy systems that include economic competitiveness, sustainability, safety and reliability, proliferation resistance, and physical protection. These objectives provide a basis to measure the overall worth of an advanced reactor design. Nuclear reactor regulations outline minimum safety-system functional requirements. Safety plays a primary role in reactor design as these requirements must be met for a reactor to be licensed. At this preliminary stage of advanced reactor design, when major safety systems and fundamental aspects of reactor designs are still being formulated, the objective of a low Core Damage Frequency (CDF) dominates all other considerations in the quantitative analysis.

A fundamental challenge when dealing with safety issues is how to handle the relevant uncertainties. Before the advent of Probabilistic Risk Assessment (PRA), these uncertainties were largely unquantified and the design and regulatory philosophy relied on the concept of defense in depth (DID) and large safety margins to ensure that accident frequencies were low. This “structuralist” approach to safety (Sorensen et al, 1999) is embodied in the structure of the regulations. For example, in the United States, Title 10, Part 50 of the Code of Federal Regulations (U.S. Code of Federal Regulations, 2004) establishes the minimum design requirements for water-cooled reactors in Appendix A, “General Design Criteria for Nuclear Power Plants”. The General Design Criteria (GDC) require reactors to be designed with sufficient margin to assure that postulated accident sequences are protected against. The postulated accidents are also known as Design Basis Accidents (DBAs). The unquantified accident frequencies are addressed by protecting against DBAs and by meeting or exceeding the GDC.

An example of a criterion used to identify unacceptable designs under current regulations is the single failure criterion (SFC) established in the GDC. This criterion

states that a single failure of active components, including valves and pumps, should not lead to the failure of a safety system (US Nuclear Regulatory Commission, 2003a; IEEE, 2000). The SFC does not apply to passive components (Holahan, 2003). So, for instance, a single loop “passive” Emergency Core Cooling System (ECCS) that includes one check valve, would violate the single failure criterion. However, it is possible to apply for an exemption to have the check valve deemed passive.

PRA, which quantifies accident frequencies, has matured sufficiently since its introduction in 1975 so that the US Nuclear Regulatory Commission (USNRC) has started to use it in regulatory decision-making (US Nuclear Regulatory Commission, 1998a). These decisions are *risk-informed* rather than *risk-based*. This means that risk information is one input to an integrated decision-making process that also utilizes traditional requirements and safety philosophies, i.e., structuralist DID requirements. The quantification of uncertainties has led to the emergence of the “rationalist” model of DID, which asserts that DID is “the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression” (Sorensen et al, 1999). Of course, one can argue that the intent of the structuralist DID provisions is to compensate for uncertainty also. As Sorensen et al, (1999) state: “What distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits.”

Applications of the rationalist approach have shown that some current regulatory requirements that are based on the structuralist approach do not contribute much to safety and, therefore, constitute unnecessary regulatory burden. One of the objectives of risk-informing the regulations is, in fact, the removal of such burden while maintaining acceptable safety levels as measured by the CDF and Large Early Release Frequency (LERF).

We note that neither the structuralist nor the rationalist approach to safety by itself can guarantee low CDF and LERF. For example, the first major reactor PRA (US Nuclear Regulatory Commission, 1975) identified an accident sequence (interfacing systems loss of coolant accident) that had been missed by the structuralist approach. The

PRA limitations are also well known (Apostolakis, 2004). Incompleteness of the analysis (deterministic and probabilistic) is always a concern.

The USNRC is exploring the use of risk information in the licensing of future reactors (US Nuclear Regulatory Commission, 2003b). The USNRC utilizes three concepts to create a framework for risk-informed regulations: a hierarchical framework structure with the goal of protecting the public health and safety, a balanced regulatory approach that maintains the philosophy of (structuralist) defense-in-depth, and quantitative guidelines based on safety goals to define how safe is safe enough for advanced nuclear power plants. Deterministic screening criteria such as the single failure criterion of GDC 17, 21, 24, 34, 35, 38, 41, and 44 may be replaced under risk-informed regulations (Sorensen, 2002). Also, DBAs that are shown to contribute little to a plant's total core damage frequency are candidates for replacement with a reliability goal in risk-informed regulations.

Under current regulations, proposed advanced reactor design options that do not meet the GDC or defend against DBAs would be screened out from further consideration unless the designer applied for an exemption. An example of a USNRC staff assessment of an advanced reactor applicant's licensing approach and application for exemptions based upon current regulations can be found in (US Nuclear Regulatory Commission, 2002).

Several issues stem from utilizing the current GDC and DBAs for advanced reactors. Because of the unquantified safety implications of the GDC and DBAs, the designer is forced to determine which regulations impose undue regulatory burden and for which exemptions to apply, thus starting the time-consuming review process. This state of affairs may discourage the development of innovative designs. In addition, the SFC does not account for common-cause failures. Clearly, the intent of the GDC is to reduce the frequency of accidents. Utilizing the SFC may overlook an important failure mode. In a risk-informed environment, replacing GDC 35 and the SFC with a reliability goal may lead to simpler, more complete, transparent, and defensible regulations. This would greatly reduce the need for exemptions.

The risk guidelines proposed by the USNRC for light water reactor regulations are illustrated in Table 1 (US Nuclear Regulatory Commission, 2000). As can be seen,

the structure of these guidelines is consistent with the defense-in-depth approach towards accident prevention and mitigation. Future reactors are expected to meet, and preferably improve upon, these guidelines. Individual sequences cannot contribute more than 10% to the total CDF. Further, initiators are broken down into three categories: anticipated initiators, infrequent initiators, and rare initiators. Their frequencies and corresponding Conditional Core Damage Probabilities (CCDPs) are also shown in Table 1.

APPROXIMATE LOCATION OF TABLE 1

The focus of this paper is the design of an ECCS following potential regulatory requirements for future reactors. Regulations for specific Generation-IV reactors are still being formulated. Therefore, there is not yet any specific regulatory guidance for future reactors. However, based upon discussions at a USNRC public meeting on advanced reactor licensing (US Nuclear Regulatory Commission, 2003b), it seems likely that advanced reactor regulations will be risk-informed. Therefore, regulations for Generation-IV reactors will be based upon both recent USNRC work on risk-informing current regulations and on the deterministic current regulations where applicable.

The research presented in this paper implements the “bare-bones” design and licensing approach outlined in (Apostolakis et al., 2001). A key point of this approach is the negotiation between the designer and regulator to establish acceptable quantitative goals for safety functions and systems. The pre-negotiation phase is explored here. This stage involves a future reactor designer postulating what the regulator might require for the reactor to be licensed based upon current regulations and risk-informed activities. This stage is also when the designer can look critically at possible regulations and suggest changes.

An iterative four-step design guidance methodology adapted from (Apostolakis et al., 2004) is presented as a means to guide designers towards better plant designs. This methodology is described in depth in the methodology section. A case study is presented to demonstrate the usefulness of the iterative four-step methodology in identifying pertinent licensing issues. The case study involves the ECCS[†] for the MIT design of a Gas-Cooled Fast Reactor (GFR). The concept of iterative bare-bones design guidance is

[†] We note that we do not distinguish between ECCS and the Safe Shutdown System (SCS) or the Emergency Cooling System (ECS).

applied to the case study. A bare-bones ECCS design is defined as the minimum combination of structures, systems, and components (SSCs) necessary for the system function to be accomplished. From the bare-bones design, components are added, modified or substituted for based on designer insights, and the ECCS configuration is modified based upon PRA insights and probabilistic and deterministic screening criteria. The decision as to which design is desirable is not based on the analytical results alone. It is supplemented by a deliberation that addresses other issues, such as stakeholder concerns, best design practices, and ease of online maintenance. In all, nine ECCS designs are taken through the iterative four-step methodology starting from a bare-bones ECCS design.

Mizuno et al. (2005) utilize iterative design guidance to improve the CDF for the International Reactor Innovative and Secure (IRIS) similar to the present ECCS case study. However, their case study differs from ours in several ways. Most apparent, the ECCS case study addresses one safety system while the IRIS design guidance addresses the entire reactor design. Also, the case study begins from a bare-bones ECCS design while the IRIS guidance begins from a design that was fully developed using traditional engineering and design methods. Finally, unlike Mizuno et al., we investigate regulatory issues for each design of the iterative design guidance.

2. METHODOLOGY

The designer decision-making methodology for selecting plant design options under risk-informed regulations is illustrated in Figure 1. This methodology was adapted from Apostolakis et al. (2004). The adaptation incorporates the bare-bones plant design methodology in Apostolakis et al. (2001) so as to allow the advanced reactor designer to analyze a design based upon likely regulations. The use of this methodology also provides a probabilistic analysis that can be used as justification for changes to deterministic requirements for future reactors. The case study presented in this paper will examine ECCS designs. The goal of the methodology is to help decision makers choose better future reactor design options.

APPROXIMATE LOCATION OF FIGURE 1

Step 1 is to formulate an initial design. The plant designers typically accomplish this using engineering judgment and intuition. For the case study, the GFR designers formulated a bare-bones ECCS design.

Step 2 is to analyze designs quantitatively. PRA is used as the design analysis tool in the iterative design guidance methodology. The PRA (General Atomics Technologies, 1986; US Nuclear Regulatory Commission, 1990) is a primary decision support tool due to its ability to integrate all of the elements of system performance and to represent the uncertainties in the results and its transparency for the safety regulators. Any considerations beyond those captured in the PRA of the ECCS and supporting systems were considered during the deliberation.

Step 3 is to screen out unacceptable designs through deterministic and probabilistic criteria. For nuclear power plants, the major sources for screening unacceptable designs are regulations and supporting regulatory documents. Designs that do not pass the screening criteria are deemed unacceptable. Under current regulations, proposed advanced reactor designs that do not meet the GDC would be screened out from further consideration unless the designer applied for an exemption.

The probabilistic screening in Step 3 utilizes the PRA performed in Step 2. Any option whose risk exceeds the risk guidelines of the risk-informed regulations will be deemed unacceptable. These plant design options can either be removed from further consideration or modified in an attempt to meet the reliability guidelines of the regulations. Only the surrogate risk guideline of core damage frequency will be used in the case study. It is currently impossible to calculate the CCFP, as the containment has yet to be designed for the GFR of the case study.

In the fourth and final step, the decision makers deliberate upon the designs as ranked via PRA. The deliberation is necessary because the PRA might not capture everything that the decision makers deem important and may not be comprehensive. In the event that either the decision makers are not thoroughly satisfied with any of the designs or the analysis suggested possible improvements to the designs, the methodology can be iterated until the decision makers are satisfied.

3. CASE STUDY

The case study involves the design of a Generation-IV Gas-Cooled Fast Reactor (GFR) currently under development at MIT. The GFR design analyzed here uses CO₂ at 20 MPa as the primary coolant. Both direct and indirect cycle versions of the main-mode cooling/power-conversion system are being developed, so a bare-bones ECCS design suitable to either is analyzed and modified iteratively using the four-step methodology.

3.1. Step 1: Formulation of the Emergency Core Cooling System

Design

Step 1 of the four-step methodology is to formulate the initial design, which was produced by the GFR design team, a group of engineers with expertise in such fields as reactor physics and thermal-hydraulics. This design was given to the GFR PRA group to analyze. The application of the four-step methodology led to additional designs. In all, nine designs were considered in the case study. Eight designs were proposed in addition to the initial, bare-bones, design. This was in an effort to meet deterministic and probabilistic screening criteria and to gain insights to be used in the deliberation.

Figure 2 is a schematic for the bare-bones emergency core cooling system design. The ECCS is intended to prevent a Loss of Coolant Accident (LOCA) initiating event from leading to core damage. The most likely method of losing the reactor coolant (CO₂) would be a pipe break in the main-mode cooling. In the MIT GFR, the reactor coolant's pressure is approximately 20 MPa during normal operation. A pipe break in the main cooling system would allow the coolant to escape through the main cooling loop pipe. This would cause the reactor to depressurize and the main cooling system would fail. At this point, the emergency core cooling system would be required to operate to prevent core damage.

APPROXIMATE LOCATION OF FIGURE 2

Core cooling in the initial ECCS design is accomplished by the blower (labeled B) moving the primary coolant (CO₂) through the core (point 1 to point 2), past a check valve that prevents backflow during non-emergency operation (point 2 to point 3), and then through the Heatric Heat Exchanger (Heatric, 2004) (point 3 to point 1). Heat is

transferred from the primary CO₂ to a secondary water loop in the Heatric heat exchanger. The secondary water is circulated to the water-boiler heat exchanger (labeled WBHX) through double-containment piping by a motor-driven pump. Heat is then transferred from the secondary loop to another water loop, which boils to form steam that deposits its energy to the ultimate heat sink.

Other than a physical failure of any of the components described so far, critical concerns for the design are supplying AC power to the blower and DC power to the instrumentation and control systems. The bare-bones ECCS design provides only offsite power to the blower, and a single DC battery powers instrumentation and control systems.

3.2. Step 2: Analysis of ECCS Designs

Providing a very reliable means of cooling the core in the event of a LOCA is a critical concern of the GFR design team. PRA is used in Step 2 as the design analysis tool to quantify the contribution to conditional core damage probability that each ECCS design will make given a LOCA.

Figure 3 illustrates the event tree used in the PRA of the ECCS designs. We show the event tree that was used for the evaluation of all the designs, rather than showing a series of trees appropriate to each design. Thus, as indicated in the figure, “secondary onsite AC power” did not appear in the event tree that was used in the first six designs. Similarly, “onsite Diesels” were not part of the bare-bones design. As can be seen from the event tree, failures of ECCS components are not the only consideration in the analysis. In the event of a LOCA, the Reactor Shutdown System (RSS) – the system that trips the reactor - is required to function. As is the convention, “up” in the event tree indicates system success while “down” illustrates system failure. It was conservatively assumed for the case study that the failure of the reactor to trip led directly to core damage. Sequence 11 in Figure 3 illustrates the failure of the RSS leading directly to core damage. Since the RSS has not yet been designed, the failure probability of the reactor shutdown system was estimated based upon system failure probabilities in (General Atomics Technologies, 1986) and (De Laquil, 1976).

Moving from left to right along the event tree, the supply of offsite power to the ECCS is considered next. Assuming the reactor successfully trips, power is required to spin the blower. The probability of the loss of offsite power was taken from (US Nuclear Regulatory Commission, 2001). If offsite power is unavailable, power could still be supplied to the electric motor by onsite diesel generators. In the initial design, the failure probabilities of onsite Diesels and of secondary onsite AC power are set equal to unity.

Assuming that either onsite or offsite power is available, the availability of onsite DC power for instrumentation and control must next be considered in the analysis. It was assumed for the case study that loss of DC power resulted in the unavailability of the ECCS since the system could not be controlled or monitored. Finally, assuming that DC power is available in conjunction with onsite or offsite power, the emergency core cooling system itself is considered in the analysis. As the ECCS is the only safety system in place to prevent core damage in the event of a LOCA, the failure of the ECCS leads directly to core damage.

APPROXIMATE LOCATION OF FIGURE 3

The probabilistic analyses were carried out using the SAPHIRE computer code (INEL, 2004). Common-cause failures were addressed for similar, redundant components via the Beta-factor model using PWR values from (Marshall and Rasmuson, 1995). If values were not available for a component, a generic value of $\beta = 0.05$ with an error factor of 3 was used. Due to the current status of the GFR design, design details are sparse and therefore generic failure data were utilized. Uncertainty analysis was carried out using the Monte Carlo method with a sample size of 10,000.

Failure data used in the ECCS case study were gathered from multiple sources (Westinghouse, 2003; Ingersoll, 2004; Bush, 1978; Broadhurst and Scarborough; 1980; Eide, 2003). Gas-reactor data were difficult to obtain, as the current U.S. commercial reactor fleet is comprised entirely of light-water reactors. It is recognized that the LWR component failure data are not optimal; however, ECCS components have not been designed in detail so generic LWR failure data were viewed as an acceptable approximation for the early-on design guidance of the ECCS.

The LOCA and ECCS-loop LOCA frequencies were taken from the AP-1000 PRA (Westinghouse, 2003). The frequencies of small, medium, and large LOCAs were

5×10^{-4} , 4×10^{-5} , 5×10^{-6} per reactor year, respectively. Because of the gas coolant, the frequencies of large-, medium-, and small-pipe break LOCAs were summed leading to the use of 5.45×10^{-4} per reactor year as the LOCA frequency for the analysis of ECCS designs. The frequency of a small LOCA (5×10^{-4} per reactor year) was used for the ECCS-loop LOCA because it was the most likely LOCA. It is recognized that the AP-1000 pipe failure data may not be the optimal data to use for a gas-cooled reactor. However, pipe failure data for the AP-1000 reflect the state-of-the-art in pipe materials and manufacturing. Also, the MIT GFR is at such an early stage of design that the use of generic failure data is warranted until more details about the plant are developed.

3.3. Step 3: Screening Criteria for the ECCS

Step 3 is to screen out unacceptable plant design options through deterministic and probabilistic criteria. The deterministic screening criteria used in the case study were GDC 35 and the ECCS DBA of the Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (SRP) (US Nuclear Regulatory Commission, 1981) of current LWR regulations. The CDF surrogate risk guidelines, outlined in the methodology section, will be used as the probabilistic screening criteria.

Abundant emergency core cooling, provided by the ECCS, is required by GDC 35 to be available in the event of a single failure of an ECCS component and either the loss of onsite or offsite power. According to the SRP, an ECCS must be designed to withstand the following postulated LOCA: a double-ended break of the largest reactor coolant line, the concurrent loss of offsite power, and a single failure of an active ECCS component in the worst possible place.

Regarding probabilistic screening criteria, a LOCA frequency of 5.45×10^{-4} per reactor year and ECCS-loop LOCA frequency of 5.00×10^{-4} per reactor year fall under the “Infrequent Initiator” (initiator frequency per reactor year is less than 10^{-2} and greater than 10^{-5}) category of the surrogate risk guidelines (Table 1). A conditional core damage probability of $\leq 10^{-2}$ is required for infrequent initiators. Therefore, the conditional probability that the ECCS fails to provide adequate core cooling, leading to core damage, must be less than 10^{-2} given a LOCA. Another screening criterion resulting from the surrogate risk guidelines is that no individual sequence should contribute more than 10% of the total CDF. A baseline CDF of 10^{-4} per reactor year (the largest acceptable CDF

under the surrogate risk guidelines) implies that an individual sequence contribution to CDF can be no more than 10^{-5} per reactor year. In the case of the GFR LOCA accident sequence, this criterion is automatically met, if the CCDP guideline is met. This is because a LOCA frequency of 5.45×10^{-4} per reactor year and the maximum allowed CCDP of 10^{-2} lead to a CDF of 5.45×10^{-6} per reactor year. It is also possible for a LOCA to occur due to reactor vessel rupture. This accident sequence was not considered because its probability of occurrence is considered low enough to be classified as a “rare initiator,” and because a PCIV is virtually immune from this type of failure.

A final probabilistic screening criterion resultant from the surrogate risk guidelines is the Conditional Early Containment Failure Probability (Table 1). Since this probability was impossible to calculate at this stage of the MIT GFR design, the sole probabilistic screening criterion used in our case study was therefore the maximum allowed CCDP of 10^{-2} .

4. RESULTS AND DELIBERATION

Designs were screened under the deterministic and probabilistic screening criteria in Step 3. The ECCS and supporting systems were configured initially with no onsite diesel generators and only one (100% capable) onsite DC battery. The results of the comparison of the designs versus the deterministic screening criteria are listed in Table 2. The results of the comparison of the designs versus the probabilistic screening criterion are listed in Table 3.

APPROXIMATE LOCATION OF TABLE 2

APPROXIMATE LOCATION OF TABLE 3

As can be seen in Table 2, the initial design (Design 1) does not meet the deterministic screening criterion of GDC 35 for any number of redundant ECCS loops. The initial design violates GDC 35 by both not providing an onsite AC power supply and by a single failure of the one DC battery leading directly to failure of the safety system. As shown in Table 3, design 1 does not meet the CCDP probabilistic screening criterion either for any loop configuration, as all numbers of ECCS loops result in a CCDP larger than 10^{-2} . As per the iterative four-step design guidance methodology illustrated in Figure 1, the initial design 1 was modified.

Designs were iteratively modified based upon either screening criteria or PRA insights gained during the analysis of a design. For instance, designs 1-3 did not meet deterministic screening criteria and hence were modified. It should be noted that designs 2 and 3 did meet the probabilistic screening criteria. This suggests that the deterministic screening criteria taken from current regulations may be overly conservative as compared to the probabilistic screening criteria. This may provide a basis for an application for exemption from the deterministic regulation. However, one can not draw definitive conclusions regarding deterministic screening criteria, such as the requirement for onsite AC power or the single failure criterion, from one accident sequence because these criteria may affect other accident sequences and safety systems. Therefore, disagreement on the acceptability of design options based upon deterministic and probabilistic screening criteria in this case study does not necessarily have any regulatory implications.

PRA insights from the analysis in Step 2 were the other basis for modifying an ECCS design. The far right column in Table 3 lists PRA insights for each design. These insights were used to either change the configuration of the design (Designs 5 and 6), add a secondary onsite power source (designs 7 and 8), or to add a nitrogen accumulator system (design 9).

The description of the bare-bones ECCS design (design 1, Figure 2) in Section 3.1 is sufficient to describe designs 1-6. This is because designs 2-6 are simply adding redundancy to the initial design.

Designs 7 and 8 – the secondary onsite pneumatically powered turbine design and the secondary onsite fossil-fired microturbine design – each added a secondary onsite AC power source to power the electric motor. The secondary onsite turbine design (design 7) is illustrated in Figure 4. If offsite power and the on-site emergency diesels are unavailable, the electric motor can be powered by an onsite turbine in design 7. In the event of a loss of both offsite power and the onsite emergency diesels, the valve labeled VE opens. Nitrogen then flows from the accumulator to the turbine (labeled T) outside of the Prestressed Cast Iron Vessel (PCIV). The nitrogen spins the turbine, which in turn spins the electric generator (labeled G). The generator then powers the electric motor (labeled EM), which spins the blower. It should be noted that similar to the onsite emergency diesel generators, the number of secondary onsite turbine loops could be

independent of the number of ECCS loops. A 100 m³ accumulator tank at 10 MPa would provide approximately one day of emergency power per loop.

APPROXIMATE LOCATION OF FIGURE 4

Figure 5 illustrates the secondary onsite microturbine design (design 8). Design 8 provides secondary power to the blower in manner similar to design 7. In the event of a station blackout the electric switch labeled SE opens. Natural gas constantly flows from an offsite natural gas connection to the microturbine. The accumulator tank is provided in case of the loss of offsite natural gas. A 100 m³ accumulator tank at 10 MPa would provide approximately ten days of emergency power per loop. The microturbine is powered and spun via natural gas combustion, which in turn spins the electric generator. The generator then powers the electric motor, which then spins the blower. Again, it should be noted that the number of secondary onsite turbine loops could be independent of the number of ECCS loops.

APPROXIMATE LOCATION OF FIGURE 5

Design 9 is illustrated in Figure 6. In this design, nitrogen accumulators provide a passive means of spinning the blower in the event of a LOCA. For the nitrogen accumulator design, power can be supplied to the blower by three diverse sources. If either offsite power or onsite emergency diesel power is available, the blower is spun by an electric motor (labeled EM). If neither of these power sources is available, the third possibility for moving coolant past the core involves the N₂ accumulator (labeled A). When primary pressure is lost due to a LOCA, the valve labeled VP opens. In the event of a station blackout the valve labeled VE opens. Nitrogen then flows from the accumulator to the turbine (labeled T). The nitrogen spins the turbine, which in turn spins the blower (labeled B). A 100 m³ accumulator tank at 10 MPa would provide approximately one day of emergency power per loop. Unlike the secondary onsite turbine and microturbine design options, the nitrogen accumulator system is part of an ECCS loop.

APPROXIMATE LOCATION OF FIGURE 6

Unfortunately, in addition to providing a passive means of performing emergency core cooling, the nitrogen accumulator design adds another path for the coolant to escape the reactor vessel. Piping is required to connect the nitrogen accumulators, which are

located outside of the reactor vessel to each ECCS loop inside the reactor vessel. A break in this piping would lead to a LOCA. For the ECCS loop LOCA, the loop in which the LOCA occurred would be unable to perform its function of cooling the core. It is likely that double containment piping would be employed – a common practice in the chemical industry.

Table 4 gives the components used for each ECCS design. If a component was added independently of the ECCS loops, its configuration is listed in parentheses. This table can be used as an easy reference to quickly determine what ECCS components and which configuration correlates to which design number.

APPROXIMATE LOCATION OF TABLE 4

The event tree illustrated in Figure 3 was used for ECCS designs 1-8. In designs 1-6, failure of offsite and emergency diesel AC power results in an ECCS that cannot function. This leads to core damage. ECCS designs 7 and 8 provide a secondary means of onsite AC power.

The nitrogen accumulator ECCS design (Design 9) event tree is illustrated in Figure 7. Unlike the secondary onsite turbine and microturbine design options, the nitrogen accumulator system is part of an ECCS loop. This is reflected in the nitrogen accumulator ECCS design event tree illustrated in Figure 7. In addition, because the nitrogen accumulator system is passive, onsite DC power for instrumentation and control is not required for system success.

APPROXIMATE LOCATION OF FIGURE 7

The nitrogen accumulator design adds another path for the coolant to escape the reactor vessel. Since piping is required to connect the nitrogen accumulators, which are designed to be outside of the reactor vessel, to each ECCS loop inside the reactor vessel, a break in this piping would lead to a LOCA. For an ECCS-loop LOCA, the loop in which the LOCA occurred would be unable to perform its function of cooling the core. The event tree for an ECCS-loop LOCA is the same as for a LOCA illustrated in Figure 7, however only the ECCS loops where the LOCA did not occur remain available to cool the core.

Table 5 lists the mean core damage frequencies for designs considered during the four-step methodology and the percentage change in the mean CDF as compared to the

initial bare-bones design. The CDFs listed are for the 3x100% ECCS configuration. It should be noted that, for all designs except for design 9 (the nitrogen accumulators design addition), the 2x100%, 3x50%, and 4x50% ECCS loop configurations resulted in almost identical CDFs – primarily due to the way that common-cause failures were accounted for. Decision-makers should be aware of this when deliberating upon ECCS designs in Step 4 of the design guidance methodology.

APPROXIMATE LOCATION OF TABLE 5

In the fourth and final step of the design guidance methodology, the decision makers deliberate[‡] upon the designs. Other considerations in addition to the CDF of ECCS designs are reflected upon during the deliberation. Since a Generation-IV reactor was analyzed, the work presented in the Generation-IV Roadmap (US Department of Energy, 2002) by the Nuclear Energy Research Advisory Committee (NERAC) was looked at as a reference for objectives to be considered when designing an advanced nuclear reactor. NERAC has presented four “Goal Areas.” These are sustainability, economics, safety and reliability, and proliferation resistance and physical protection.

As can be seen from Table 3, for designs 1-8, there is an insignificant improvement in CCDP when adding redundant ECCS loops beyond 2x100% capability. This is due to the use of the Beta factor to model common-cause failures. For example, a 2-component parallel system (2x100% capable) requires failure of both components for the system to fail. Under the Beta factor model (using $\beta=0.05$), identical components can either fail randomly or all components can fail due to a common cause. Using a component failure probability for the two components, A and B, of $u=1x10^{-3}$, the probability of failure of the 2x100% capable system due to random causes is:

$$P_{2x100\%random} = P(A) * P(B) = u^2 = 1x10^{-6}$$

The Common-Cause Failure (CCF) probability of the 2x100% capable system is:

$$P_{2x100\%CCF} = \beta * u = 5x10^{-5}$$

The total 2x100% capable system failure probability is:

$$P_{2x100\%fail} = P_{random} + P_{CCF} = 5.1x10^{-5}$$

[‡] Deliberation is an important part of a risk-informed decision-making process. It has been proposed by the National Research Council (1994) for choosing technologies in the case of environmental cleanup and is part of the “integrated decision-making process” of the USNRC (1998a).

Adding an identical redundant component, C, to bring the system capability to 3x100% does little to change the total failure probability in the Beta factor model. The total failure probability of the 3x100% capable system is:

$$P_{3x100\%fail} = P_{random} + P_{CCF} = P(A) * P(B) * P(C) + P_{CCF} = u^3 + \beta * u = 1x10^{-9} + 5x10^{-5} \cong 5x10^{-5}$$

It can be seen that adding identical, redundant components beyond 2x100% does little to decrease the system failure probability when using the beta factor common cause failure model. Other models exist that do not describe CCF probabilities as pessimistically as the beta-factor model, such as the Multiple Greek Letter model and Alpha factor model (Marshall and Rasmuson, 1995). These refined models, however, would not produce a significant difference between the CCDPs corresponding to the 2x100% and 3x100% capable ECCS loops.

In the CCF literature that we reviewed (Rasmuson et al., 1998; Marshall et al., 1998; US Nuclear Regulatory Commission, 1989; Fleming and Mosleh, 1995; Idaho National Engineering and Environmental Laboratory, 1997) and communications we had with CCF experts (Fleming, 2004; Mosleh, 2004), no quantitative guidance was found as to how to change the values of the beta factor when the design changes. However, there is some guidance on methods to qualitatively reduce CCFs during the design stage. Reduction of CCFs is therefore left to Step 4, the deliberation phase of the design guidance methodology. Coupling factors can be used to qualitatively reduce CCFs during design. A coupling factor is a characteristic of a group of components that identifies them as susceptible to the same cause of failure. Coupling factors identified in Rasmuson et al. (1998) were hardware (48.3%), maintenance (26.1%), operations (14.1%), and environment (11.5%). Qualitative CCF insights can be deduced from the coupling factors. For example, while the mean CCDP of design 8 was nearly identical for the 2x100% capable and 3x50% capable ECCS loops (Table 3), it is noted that the coupling factor “environment” would be reduced for the 3x50% capable ECCS loops. Since, ~99% of the CCDP for design 8 was due to CCFs of ECCS or onsite DC components, the 3x50% capable configuration’s reduction of the environmental coupling factor reduces the CCF rate which in turn would reduce the CCDP. Therefore, the

3x50% ECCS configuration may be more desirable than the 2x100% ECCS configuration for design 8.

Online maintenance was also considered during the deliberation. Although it is possible that a 1x100% capable configuration may be allowed under a probabilistic screening criterion, no maintenance on the loop could take place while the reactor was online. The safety function of a 1x100% capable ECCS configuration could not be accomplished when the loop was down for testing or maintenance.

In this case study, the GFR decision makers are still deliberating on the results of the ECCS design guidance analysis. In particular, the use of microturbine power packages is of interest because of their purported high reliability and the potential to run continuously thereby providing assurance of readiness and elimination of the failure to start sequence. The use of fuel cells is under consideration also. Microturbines are also a focus of further deliberation because similar components have not been previously used, although the Oskarshamm BWRs and the ABWR supplement their diesel generators with conventional gas turbines. In the event that the decision makers decide they are not thoroughly satisfied with any of the ECCS designs or if they see possible improvements of the ECCS design based upon the formal analysis, the design guidance methodology can be iterated until the decision makers are satisfied.

5. CONCLUSIONS

Great care is necessary when modifying a design based upon insights discovered during the four-step methodology because adding components or changing the configuration of components can change the PRA model significantly. It was originally assumed that adding components to a bare-bones design would simply translate to adding the component into the PRA model. However, as in the case when modeling design 9 (the nitrogen accumulator addition), new accident sequences can be introduced with the addition of new components.

Many cases were found during the iterative four-step design guidance in which ECCS-loop configurations were acceptable according to a probabilistic screening criterion, but unacceptable under deterministic screening criteria. The frequencies of both the LOCA and the ECCS-loop LOCA initiating events fell in the infrequent initiator

range (10^{-2} per reactor year \leq Initiator Frequency $\leq 10^{-5}$ per reactor year). According to the USNRC proposed surrogate risk guidelines, a mean conditional core damage probability of less than or equal to 10^{-2} is required for such initiators. We note that this comparison includes the contribution of common-cause failures, which are not included in GDC 35. In all, seventeen of the forty-five designs analyzed in the case study passed the surrogate risk guidelines, but did not meet the deterministic criteria. Risk-informing the GDC would help ease undue regulatory burden and lead to more economical designs. This could occur while maintaining reliability and without compromising plant safety. Replacing the single failure criterion with a reliability goal within a regulatory structure, as described above, could lead to simpler, more complete, transparent, and defensible regulations for future reactors. A review of other GDC that are candidates for becoming risk-informed is given in Sorensen (2002).

Other considerations beyond those encompassed in the PRA and in the formal analysis need to be taken into account during the deliberation. The impact of a design on the fundamental objectives of sustainability, economics, reliability, proliferation resistance, and physical protection should be considered during the deliberation. Also, matters such as the possibility of online maintenance in addition to the contribution to the CDF of a design need to be addressed during Step 4. Qualitative methods for reducing the CDF due to common-cause failures also are considered. No quantitative methods for modeling reductions in CCF have been proposed, therefore, considerations of CCF rates between designs and the impact of steps taken to reduce CCFs are considered qualitatively during the deliberation. Finally, deliberation is also the step in which best-design practices would be considered even though the PRA results themselves might be insensitive to such practices. It is the deliberation step that makes the process risk-informed and prevents it from being risk-based. It is at this step that the designers and the regulators must consider the limitations of both the structuralist approach to safety (how much defense in depth is enough?) and the rationalist approach (what if we are wrong in our assumptions and analyses?).

The iterative design guidance methodology led to a reduction in the CDF contribution due to a LOCA of over two orders of magnitude from the baseline ECCS design to Design 8 (from 1.21×10^{-5} to 7.58×10^{-8} per reactor year for the 3x100% loop

configuration, Table 5). Of the designs analyzed, the design that presently appears best in terms of core damage frequency is Design 8 at 3x100% (the secondary onsite AC power microturbine design) with a CDF contribution due to a LOCA of 7.58×10^{-8} per reactor year and the elimination of the failure-to-start failure mode for an onsite AC power supply. Many directions for future work are available to improve the design guidance of the ECCS and to guide the design of other GFR systems. For instance, the collection of failure data appropriate for gas reactors would lead to less uncertainty in the results of the design guidance. Also, more information concerning the reliability of microturbines needs to be gathered. Microturbines are a new technology that has never been used in a nuclear power plant emergency power supply system. As such, they would be thoroughly scrutinized during the licensing process. Therefore, a concerted effort would have to be made during the design process to obtain accurate reliability and safety pertinent information regarding microturbines.

It is possible that the best ECCS design may not lead to the best GFR design when other accident sequences are considered. ECCS components can be used as part of other safety systems when faced with initiators other than LOCAs, for example events during depressurized refueling. Other accident sequences, resulting from initiating events such as the loss of offsite power or an inadvertent control rod withdrawal, need to be analyzed as the design of the GFR is further developed to ensure a safe and balanced nuclear reactor.

ACKNOWLEDGMENTS

We thank Pavel Hejzlar of MIT for useful discussions on the GFR design. We also thank Gary Holahan and Prasad Kadambi of the USNRC, John Lehner of Brookhaven National Laboratory, Karl Fleming of Technology Insights, Inc., Ali Mosleh of the University of Maryland, and Curtis Smith of Idaho National Engineering and Environmental Laboratory for providing useful information. This work was supported by the US Nuclear Regulatory Commission under a cooperative agreement with the MIT Department of Nuclear Engineering and by the US Department of Energy (DOE) under a Nuclear Energy Research Initiative. The views presented here are those of the authors and do not necessarily represent the views of the USNRC or the USDOE.

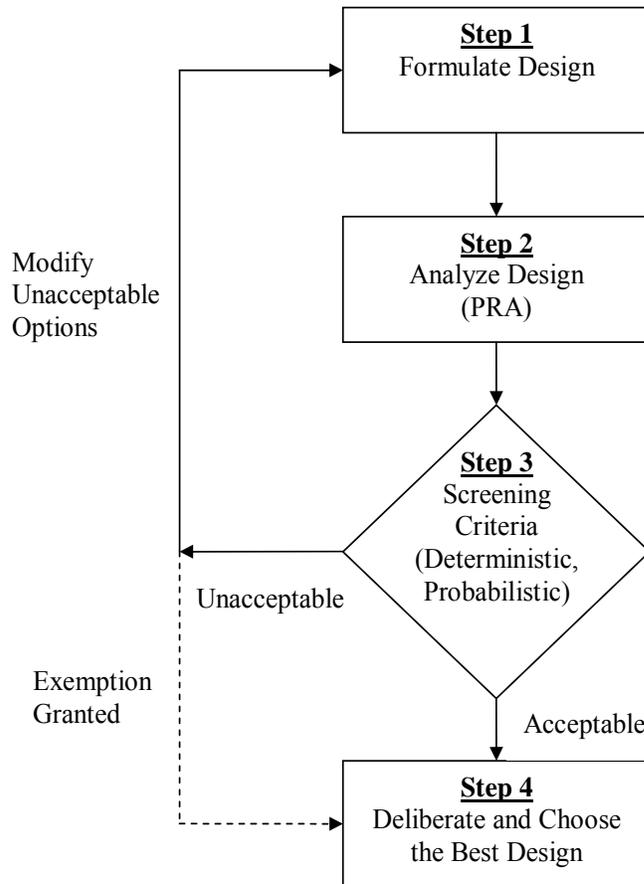


Figure 1. Iterative Design Guidance Methodology

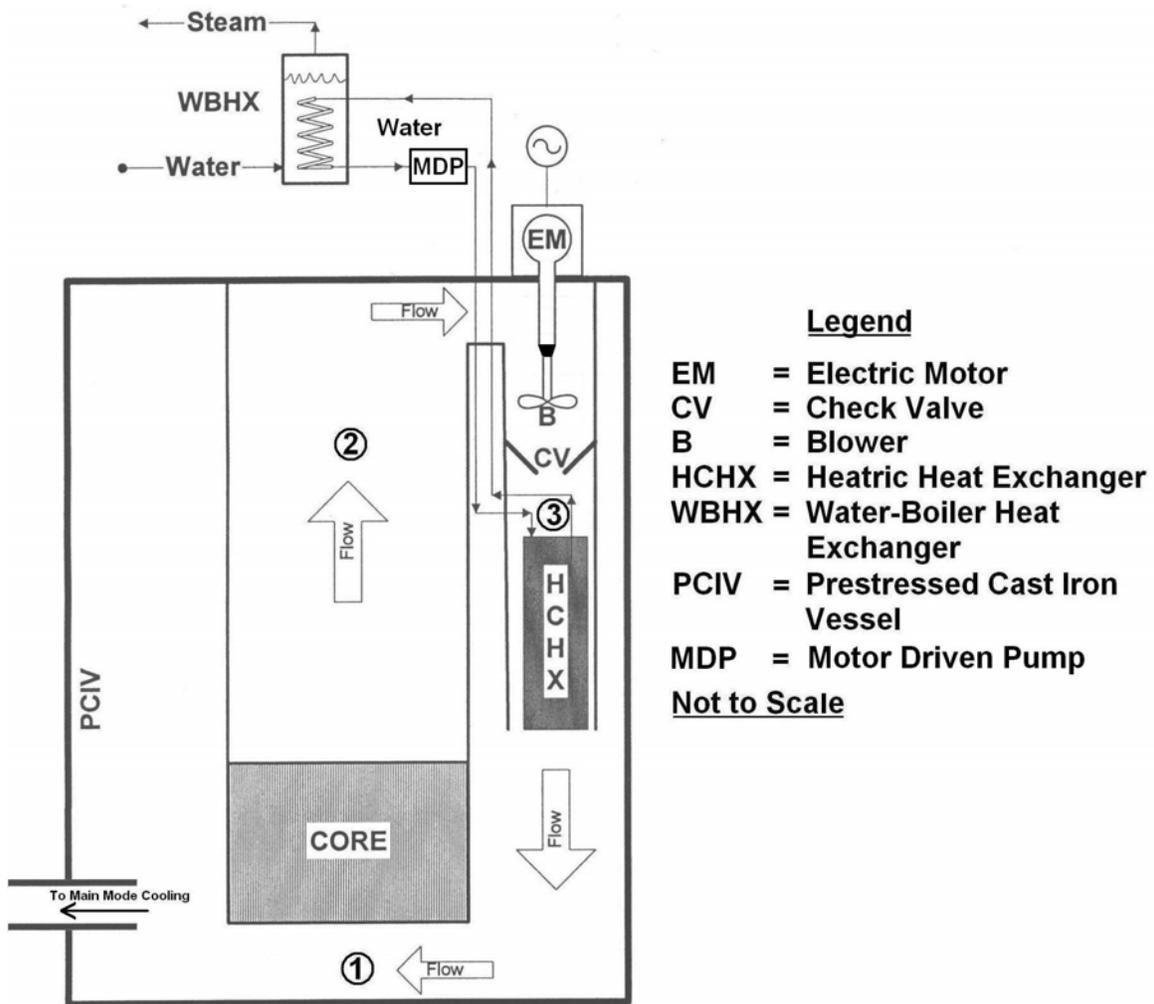
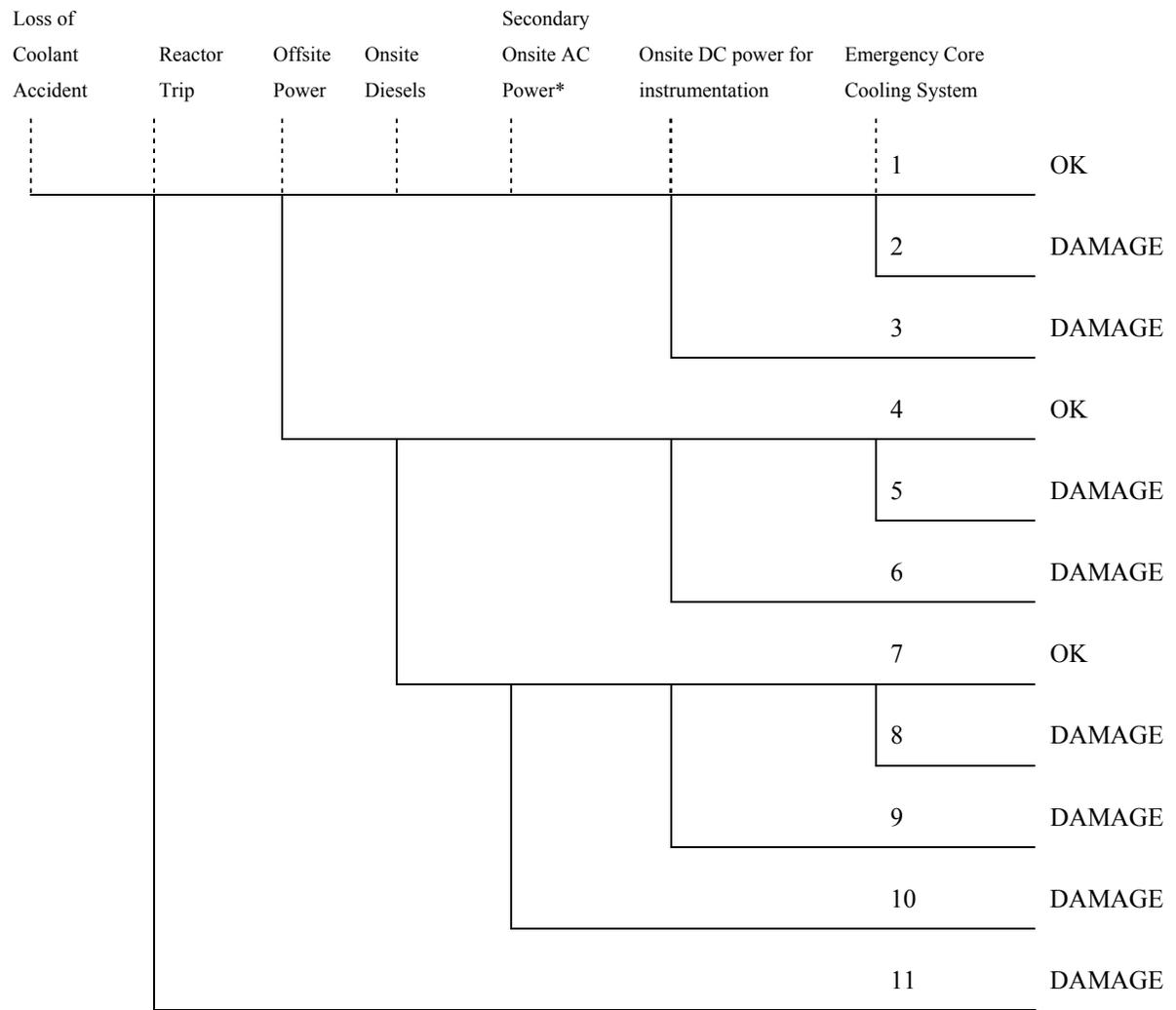


Figure 2. ECCS Designs 1-6



*Secondary onsite power not available for Designs 1-6

Figure 3. ECCS Event Tree (Designs 1-8)

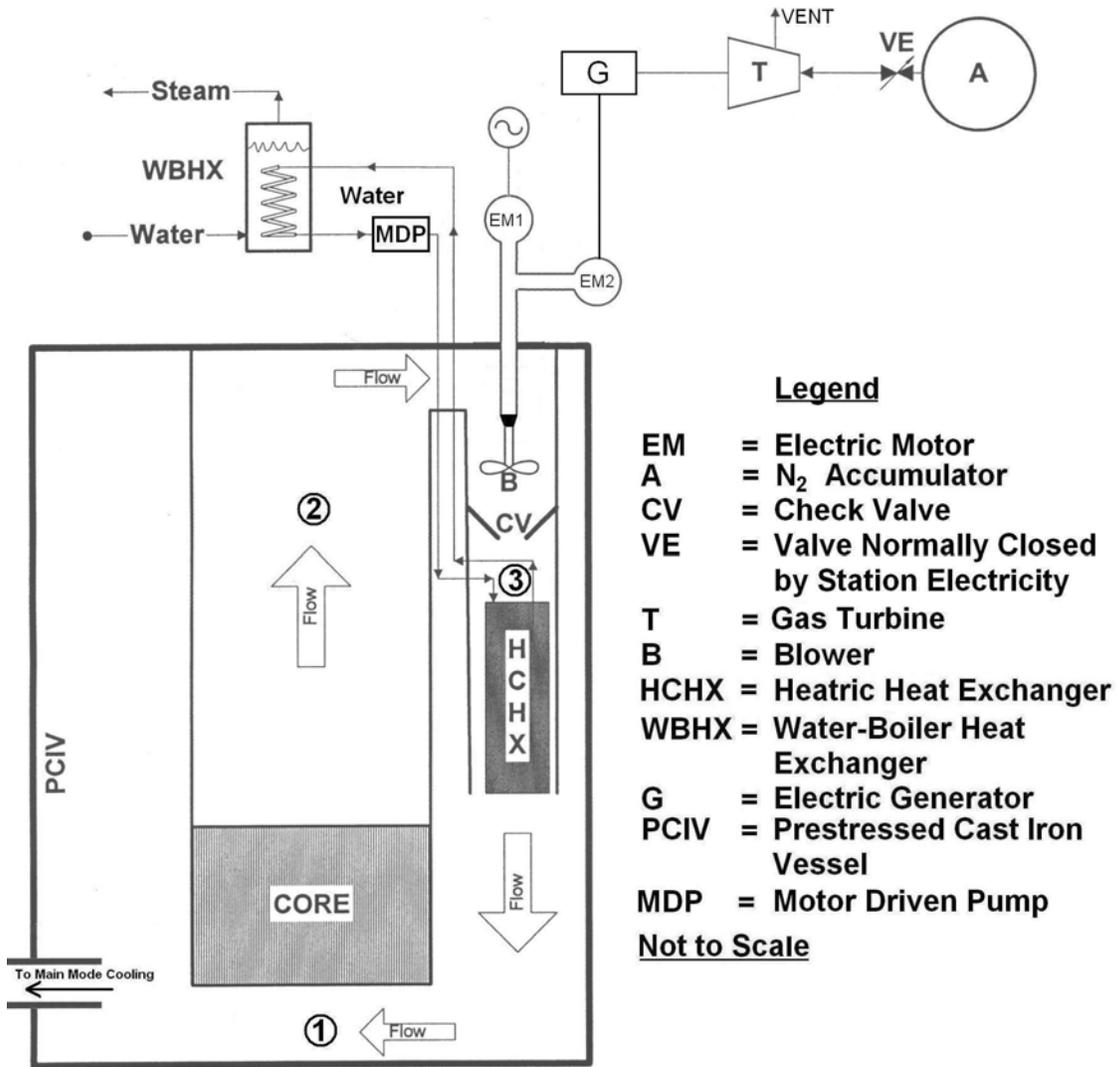


Figure 4. Secondary Onsite AC Power Design: Turbine (Design 7)

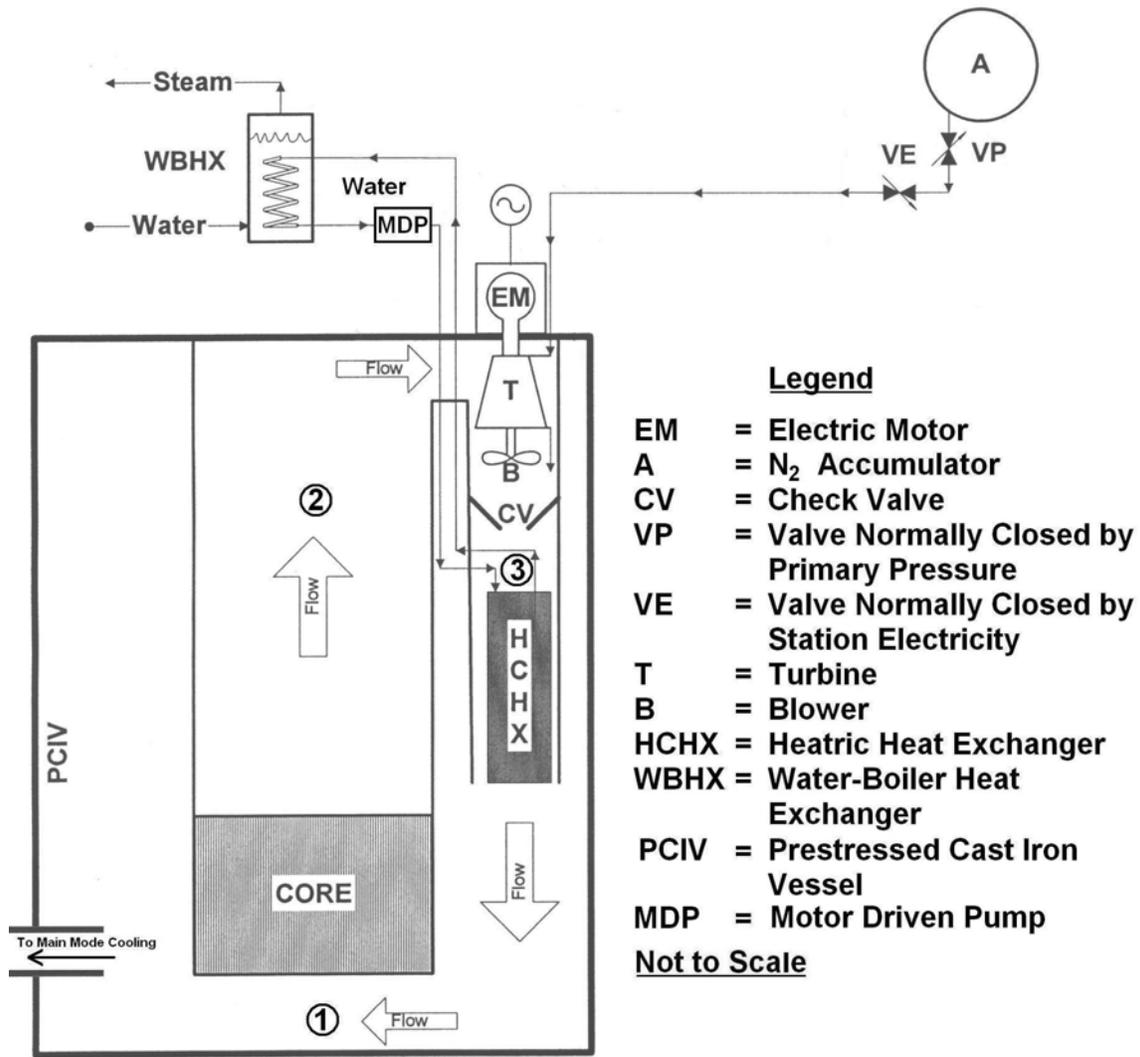
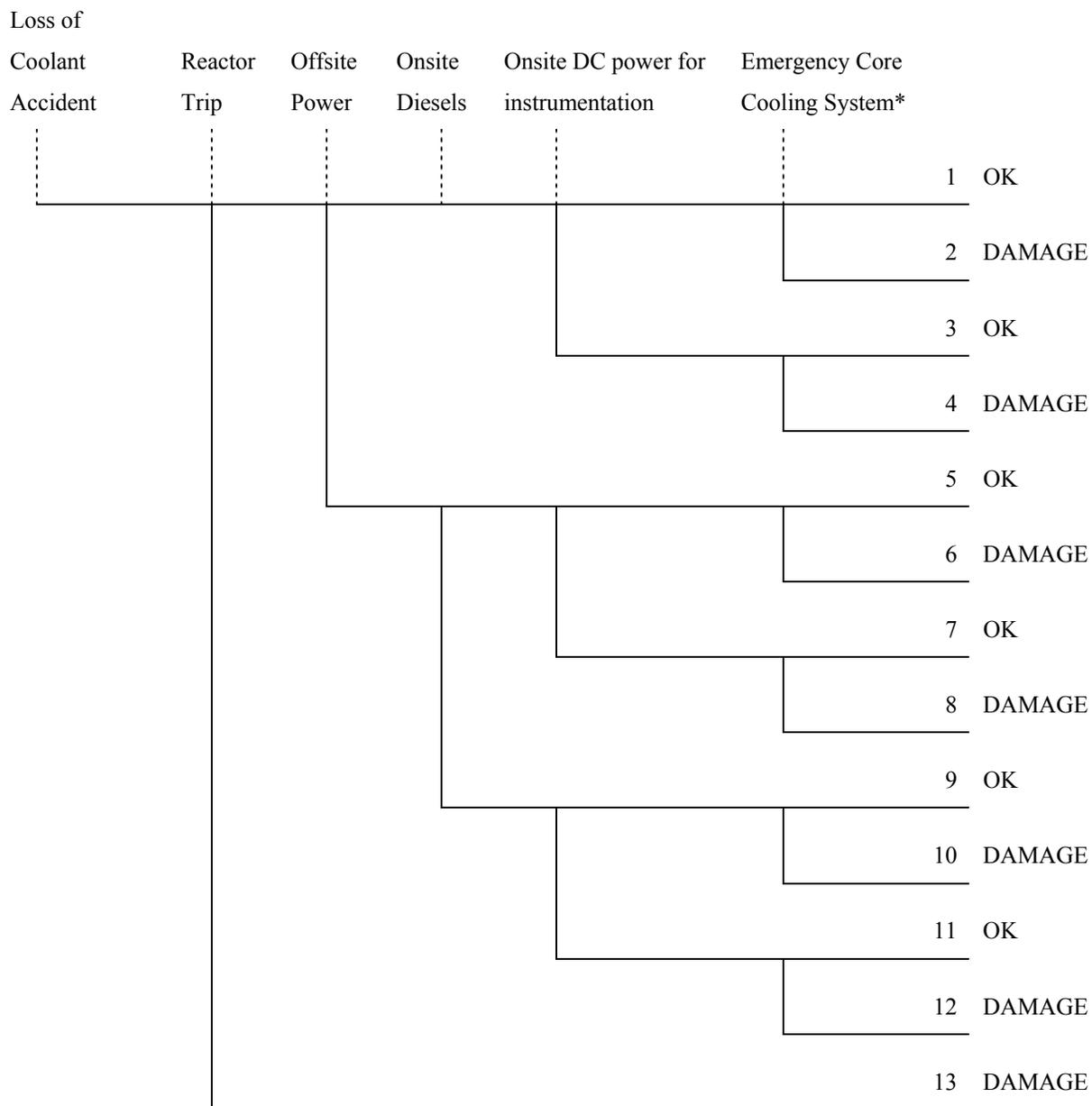


Figure 6. ECCS Design: Nitrogen Accumulator



*Remaining loops for ECCS Loop LOCA

Figure 7. Nitrogen Accumulator ECCS Design Event Tree (Design 9)

Table 1. Surrogate Risk Guidelines (US Nuclear Regulatory Commission, 2000)

	Prevent		Mitigate
	Plant Core Damage Frequency $\leq 10^{-4}/\text{year}$		Conditional Probability of Early Containment Failure $\leq 10^{-1}$
	Initiator Frequency	Conditional Core Damage Probability	Conditional Early Containment Failure Probability
Anticipated Initiators	$\leq 1/\text{year}$	$\leq 10^{-4}$	$\leq 10^{-1}$
Infrequent Initiators	$\leq 10^{-2}/\text{year}$	$\leq 10^{-2}$	$\leq 10^{-1}$
Rare Initiators	$\leq 10^{-5}/\text{year}$	≤ 1	≤ 1

Table 2. Screening based on deterministic criteria.

Design Number	Configuration	Number of ECCS Loops					Comments
		1x100%*	2x100%	3x50%	3x100%	4x50%	
		Meet Deterministic Screening Criteria?					
1	No Diesels, 1x100% DC Battery	No	No	No	No	No	Violates SFC, no onsite AC power,
2	1x100% Diesel, 1x100% DC Battery	No	No	No	No	No	Violates SFC
3	1x100% Diesel, 2x100% DC Battery	No	No	No	No	No	Violates SFC + Loss of Offsite Power
4	2x100% Diesel, 2x100% Battery	No	Yes	Yes	Yes	Yes	1x100% violates SFC
5	2x100% Diesel, 2x100% Battery, 2x100% Transmission	No	Yes	Yes	Yes	Yes	1x100% violates SFC
6	3x100% Diesel, 2x100% Battery, 2x100% Transmission	No	Yes	Yes	Yes	Yes	1x100% violates SFC
7	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Turbine	No	Yes	Yes	Yes	Yes	1x100% violates SFC
8	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Microturbine	No	Yes	Yes	Yes	Yes	1x100% violates SFC
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission, Nitrogen Accumulator	No	No	No	Yes	Yes	1x100%, 2x100%, 3x50% violate SFC

*Violates single failure criterion of GDC 35

Table 3. Screening based on probabilistic criteria.

Conditional Core Damage Probability given LOCA*							
Design Number	Configuration	Number of ECCS Loops					PRA Insights (3x100% ECCS Loops)
		1x100%**	2x100%	3x50%	3x100%	4x50%	
Mean CCDP							
1	No Diesels, 1x100% DC Battery	No (2.51E-2)	No (2.20E-2)	No (2.20E-2)	No (2.20E-2)	No (2.20E-2)	<ul style="list-style-type: none"> • LOOP accounts for ~99% of risk
2	1x100% Diesel, 1x100% DC Battery	Yes (5.71E-3)	Yes (2.32E-3)	Yes (2.36E-3)	Yes (2.31E-3)	Yes (2.31E-3)	<ul style="list-style-type: none"> • Failure of diesel is largest contributor to risk (50.3%)
3	1x100% Diesel, 2x100% DC Battery	Yes (4.86E-3)	Yes (1.68E-3)	Yes (1.72E-3)	Yes (1.67E-3)	Yes (1.67E-3)	<ul style="list-style-type: none"> • 1 Diesel account for 86.6% of risk
4	2x100% Diesel, 2x100% Battery	Yes (3.82E-3)	Yes (5.97E-4)	Yes (6.29E-4)	Yes (5.81E-4)	Yes (5.81E-4)	<ul style="list-style-type: none"> • LOOP + CCF of diesels accounts for 14.5% of risk • LOOP + random failure of diesels accounts for 27.1% of risk • 1 DC Transmission loop accounts for 25.1% of risk
5	2x100% Diesel, 2x100% Battery, 2x100% Transmission	Yes (3.75E-3)	Yes (4.69E-4)	Yes (5.02E-4)	Yes (4.52E-4)	Yes (4.52E-4)	<ul style="list-style-type: none"> • LOOP + CCF of diesels accounts for 18.5% of risk • LOOP + random failure of diesels accounts for 35.5% of risk
6	3x100% Diesel, 2x100% Battery, 2x100% Transmission	Yes (3.59E-3)	Yes (5.18E-4)	Yes (5.34E-4)	Yes (2.96E-4)	Yes (2.96E-4)	<ul style="list-style-type: none"> • LOOP + CCF of diesels accounts for 2.84% of risk • LOOP + random failure of diesels accounts for 1.8% of risk
7	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Turbine	Yes (3.40E-3)	Yes (1.61E-4)	Yes (1.97E-4)	Yes (1.43E-4)	Yes (1.43E-4)	<ul style="list-style-type: none"> • ~99% of risk due to CCF of ECCS or DC components
8	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Microturbine	Yes (3.42E-3)	Yes (1.55E-4)	Yes (1.88E-4)	Yes (1.38E-4)	Yes (1.38E-4)	<ul style="list-style-type: none"> • ~99% of risk due to CCF of ECCS or DC components
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission, Nitrogen Accumulator	Yes (2.16E-4)	Yes (1.15E-4)	Yes (1.66E-4)	Yes (1.03E-4)	Yes (1.03E-4)	<ul style="list-style-type: none"> • ~99% of risk due to CCF of ECCS components
Conditional Core Damage Probability given ECCS Loop LOCA***							
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission, Nitrogen Accumulator	No (1.00E+0)	Yes (4.70E-3)	Yes (7.48E-3)	Yes (1.49E-4)	Yes (1.49E-4)	<ul style="list-style-type: none"> • ~86.6% of risk due to CCF of ECCS components • 12.1% of risk due to random failure of ECCS components

*LOCA Frequency = 5.45E-04

**Violates single failure criterion of GDC 35

***ECCS Loop LOCA Frequency = 5.00E-04

Table 4: List of components and configuration for ECCS designs

Design Number	ECCS List of Components
1 (Bare-bones design)	Blower, electric motor, check valve, Heatric heat exchanger, motor driven pump, water-boiler heat exchanger
	Added Components, as compared to bare-bones design (configuration, if different than number of ECCS loops)
1	None
2	Diesel (1x100%), DC Battery (1x100%)
3	Diesel (1x100%), DC Battery (2x100%)
4	Diesel (2x100%), DC Battery (2x100%)
5	Diesel (2x100%), DC Battery (2x100%), DC Transmission (2x100%)
6	Diesel (3x100%), DC Battery (2x100%), DC Transmission (2x100%)
7	Diesel (3x100%), DC Battery (2x100%), DC Transmission (2x100%), Turbine (1x100%), Accumulator (1x100%), Electric Valve (1x100%), Generator (1x100%), Secondary Electric Motor
8	Diesel (3x100%), DC Battery (2x100%), DC Transmission (2x100%), Microturbine (1x100%), Natural Gas Accumulator (1x100%), Electric Switch (1x100%), Generator (1x100%), Offsite Natural Gas Connection (1x100%), Secondary Electric Motor
9	Diesel (3x100%), DC Battery (2x100%), DC Transmission (2x100%), Nitrogen Accumulator, Electric Valve, Pressure Valve, Turbine

Table 5. Results of the Iterative PRA ECCS Design Guidance

Design Number	Configuration	3x100% ECCS loops Mean CDF	CDF reduction factor over initial bare-bones design
1	No Diesels, 1x100% DC Battery	1.21×10^{-5}	1.00
2	1x100% Diesel, 1x100% DC Battery	1.29×10^{-6}	9.4
3	1x100% Diesel, 2x100% DC Battery	8.59×10^{-7}	14.1
4	2x100% Diesel, 2x100% Battery	3.11×10^{-7}	39.0
5	2x100% Diesel, 2x100% Battery, 2x100% Transmission	2.47×10^{-7}	49.0
6	3x100% Diesel, 2x100% Battery, 2x100% Transmission	1.64×10^{-7}	73.8
7	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Turbine	7.96×10^{-8}	152.0
8	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Microturbine	7.58×10^{-8}	159.6
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission, Nitrogen Accumulator	1.35×10^{-7}	89.6

List of Figures

Figure 1. Iterative Design Guidance Methodology

Figure 2. ECCS Designs 1-6

Figure 3. ECCS Event Tree (Designs 1-8)

Figure 4. Secondary Onsite AC Power Design: Turbine (Design 7)

Figure 5. Secondary Onsite AC Power Design: Microturbine (Design 8)

Figure 6. ECCS Design: Nitrogen Accumulator

Figure 7. Nitrogen Accumulator ECCS Design Event Tree (Design 9)

List of Tables

Table 1. Surrogate Risk Guidelines (USRNC, 2000)

Table 2. Screening based on deterministic criteria

Table 3. Screening based on probabilistic criteria

Table 4: List of components and configuration for ECCS designs

Table 5. Results of the Iterative PRA ECCS Design Guidance

Nomenclature

10CFR50	Code of Federal Regulations, Title 10, Part 50
ABWR	Advanced Boiling Water Reactor
BWR	Boiling Water Reactor
CCDP	Conditional Core Damage Probability
CCF	Common-Cause Failure
CDF	Core Damage Frequency
CECFP	Conditional Early Containment Failure Probability
DBA	Design Basis Accident
ECCS	Emergency Core Cooling System
ECS	Emergency Cooling System
GDC	General Design Criteria
GFR	Gas-Cooled Fast Reactor
IRIS	International Reactor Innovative and Secure
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LWR	Light Water Reactor
NERAC	Nuclear Energy Research Advisory Committee
PCIV	Prestressed Cast Iron Vessel
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
RSS	Reactor Shutdown System
SCS	Shutdown Cooling System
SFC	Single Failure Criterion
SRP	Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants
SSC	Systems, Structures, and Components
USDOE	United States Department of Energy
USNRC	United States Nuclear Regulatory Commission

REFERENCES

- Apostolakis, G.E., 2004. How Useful is Quantitative Risk Assessment? *Risk Analysis*, 24, 515-520.
- Apostolakis, G.E., Koser, J.P. and Sato, G., 2004. Decision Analysis and its Application to the Frequency of Containment Integrated Leakage Rate Tests. *Nuclear Technology*, 146, 181-198.
- Apostolakis, G.E., Golay, M.W., Camp, A.L., Durán, A.L., Finnicum, D.J. and Ritterbusch, S.E., 2001. *A New Risk-Informed Design and Regulatory Process*. Proceedings of the Advisory Committee on Reactor Safeguards Workshop on Future Reactors, June 4-5, 2001, Report NUREG/CP-0175, pp. 237-248, US Nuclear Regulatory Commission, Washington, DC.
- Broadhurst, R.H., Scarborough, J.C., 1980. Assessment of Gas Turbine Failure Modes from Historical Steam Turbine Experience, *American Nuclear Society Transactions*, 35, 391-393.
- Bush, S.H., 1978. A Reassessment of Turbine Generator Failure Probability, *Nuclear Safety*, 19, 681-698.
- De Laquil, P., 1976. *An Accident Probability Analysis and Design Evaluation of the Gas-Cooled Fast Breeder Reactor Demonstration Plant*, Cambridge, Massachusetts, Massachusetts Institute of Technology, Ph.D. Thesis.
- Eide, S.A., 2003. Historical Perspective on Failure Rates for U.S. Commercial Reactor Components, *Reliability Engineering and System Safety*, 80, 123-132.
- Fleming, K.N., 2004. Technology Insights, Inc. Personal Communication.

Fleming, K.N., and Mosleh, A., 1995. *Classification and Analysis of Reactor Operating Experience Involving Dependent Events*, Report EPRI NP-3967, Electric Power Research Institute, Palo Alto, California.

General Atomics Technologies, 1986. *Probabilistic Risk Assessment of the Modular HTGR Plant*, Report HTGR-86-011, San Diego, CA.

Heatric World-Wide, 2004. Available at: <http://www.heatric.com>.

Holahan, G., 2003. U.S. Nuclear Regulatory Commission, Personal Communication.

Idaho National Engineering and Environmental Laboratory, 2004. SAPHIRE, Available at: <http://saphire.inel.gov>.

Idaho Engineering and Environmental Laboratory, 1997. *Common Cause Failure Database and Analysis System*, Report INEEL/EXT-97/00696, Idaho Falls, ID.

IEEE, 2000 *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generation Station Safety Systems*, New York, NY.

Ingersoll Rand Energy Systems, 2004. Manufacturer Data, Available: <http://www.irpowerworks.com>.

Marshall, F.M., and Rasmuson, D.M., 1995. *Common-Cause Failure Data Collection and Analysis System Volume 6 - Common-Cause Failure Parameter Estimations*, Idaho National Engineering Laboratory, Report INEL-94/0064, Idaho Falls, ID.

Marshall, F.M., Rasmuson, D.M., and Mosleh, A., 1998. Common Cause Failure Susceptibilities at Nuclear Power Plants, *Probabilistic Safety Assessment and Management 4 (PSAM 4) Proceedings*, Mosleh, A and Bari, R.A. eds., Volume 1, Springer-Verlag, New York, NY.

Mizuno, Y., Ninokata, H., and Finnicum, D.J., 2005. Risk-informed design of IRIS using a level-1 probabilistic risk assessment from its conceptual design phase, *Reliability Engineering and System Safety*, 87, 201-209.

Mosleh, A., 2004. Department of Materials and Nuclear Engineering, University of Maryland. Personal Communication.

National Research Council, 1994. *Building Consensus through Risk Assessment and Management of the Department of Energy's Environmental Remediation Program*, National Academy Press, Washington, DC.

Rasmuson, D.M., Mosleh, A. and Marshall, F.M., 1998. Some General Insights from the USNRC's Common Cause Failure Database, *Probabilistic Safety Assessment and Management 4 (PSAM 4) Proceedings*, Mosleh, A and Bari, R.A. eds., Volume 1, Springer-Verlag, New York, NY.

Sorensen, J.N., 2002. *Some Observations on Risk-Informing Appendices A & B to 10 CFR Part 50*, Report prepared for the Advisory Committee on Reactor Safeguards, NUREG-1755, U.S. Nuclear Regulatory Commission, Washington, DC.

Sorensen, J.N., Apostolakis, G. E., Kress, T.S., and Powers, D.A., 1999. "On the Role of Defense in Depth in Risk-Informed Regulation," *Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment*, pp. 408-413, Washington, DC, August 22 - 26, American Nuclear Society, La Grange Park, Illinois.

U.S. Code of Federal Regulations, 2004. Title 10, Part 50, Appendix A. *General Design Criteria for Nuclear Power Plants*, US Government Printing Office, Washington, DC.

U.S. Department of Energy, 2002. *A Technology Roadmap for Generation IV Nuclear Energy Systems*, Washington, DC.

U.S. Nuclear Regulatory Commission, 2003a. *Application of the Single-Failure Criterion to Safety Systems*, Regulatory Guide 1.53, Washington, DC.

U.S. Nuclear Regulatory Commission, 2003b. Framework for a Risk-Informed Regulatory Structure for Advanced Reactors, Public Meeting, Rockville, MD, November 19.

U.S. Nuclear Regulatory Commission, 2002. *NRC Staff's Preliminary Findings Regarding Exelon Generation's (Exelon's) Proposed Licensing Approach for the Pebble Bed Modular Reactor (PBMR)*, Adams Accession No. ML020860097, Washington, DC.

U.S. Nuclear Regulatory Commission, 2001. *Feasibility Study of a Risk-Informed Alternative to 10CFR50.46, Appendix K and GDC 35*, SECY-01-0133, Washington, DC.

U.S. Nuclear Regulatory Commission, 2000. *Framework for Risk-Informing the Technical Requirements of 10CFR50*, SECY-00-0198, Washington, DC.

U.S. Nuclear Regulatory Commission, 1998a. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis*, Regulatory Guide 1.174, Washington, DC. Available at www.nrc.gov.

U.S. Nuclear Regulatory Commission, 1998b. *Options for Risk-Informing Revisions to 10 CFR Part 50 – Domestic Licensing and Utilization Facilities*, SECY-98-0300, Washington, DC.

U.S. Nuclear Regulatory Commission, 1990. *Severe Accident Risks: An Assessment For Five U.S. Nuclear Power Plants*, Report NUREG-1150, Washington, DC.

U.S. Nuclear Regulatory Commission, 1989. *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, Report NUREG/CR-4780, Washington, DC.

U.S. Nuclear Regulatory Commission, 1981. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, NUREG-0800, Rev. 2, Washington, DC.

U.S. Nuclear Regulatory Commission, 1975. *Reactor Safety Study: An Assessment of Accident Risks In U.S. Commercial Nuclear Power Plants*, WASH-1400 (NUREG-75/014), Washington, DC.

Westinghouse Electric Company, 2003. *AP-1000 Probabilistic Risk Assessment*, Revision 1, Pittsburgh, PA.