INL/EXT-13-30019

Light Water Reactor Sustainability Program

Technical Basis Guide Describing How to Perform Safety Margin Configuration Risk Management

James Knudsen
Curtis Smith

August 2013

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

Idaho National Laboratory

INL/EXT-13-30019

Light Water Reactor Sustainability Program

Technical Basis Guide Describing How to Perform Safety Margin Configuration Risk Management

James Knudsen
Curtis Smith

August 2013

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov/lwrs

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

SUMMARY

The INL has carried out a demonstration of the RISMC approach for the purpose of configuration risk management. We have shown how improved accuracy and realism can be achieved by simulating changes in risk – as a function of different configurations – in order to determine safety margins as the plant is modified. We described the various technical issues that play a role in these configuration-based calculations with the intent that future applications can take advantage of the analysis benefits while avoiding some of the technical pitfalls that are found for these types of calculations. Specific recommendations have been provided on a variety of topics aimed at improving the safety margin analysis and strengthening the technical basis behind the analysis process.

CONTENTS

FIGURES

TABLES

ACRONYMS

ATR	Advanced Test Reactor
CDF	core damage frequency
CRM	Configuration Risk Management
DOE	Department of Energy
FDF	fuel damage frequency
HEP	human error probability
HRA	human reliability analysis
INL	Idaho National Laboratory
LERF	large early release fraction
LWR	light water reactor
NRC	Nuclear Regulatory Commission
PI	performance indicator
PRA	probabilistic risk assessment
PSF	performance shaping factors
R&D	research and development
RISMC	Risk Informed Safety Margin Characterization
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SDP	Significance Determination Process
SSC	system, structure, and component
T-H	thermal-hydraulics

Technical Basis Guide Describing How to Perform Safety Margin Configuration Risk Management

1. BACKGROUND

Configuration risk management is an important process that evaluates testing and maintenance activities that are proposed while the reactor is at full power. Performing these activities while at full power provide many benefits to the plant owner/operators, improving both economics and safety. Configuration risk management helps identify if these activities should be allowed while at power based on their risk impact. The proposed configuration is evaluated and if the increase in the risk metric of choice does not exceed a predefined safety threshold then the planned activities can proceed. Different plant configurations, depending upon safety system and duration, can have different impacts on risk.

Configuration risk management is also used to evaluate degraded conditions that have occurred at plants. This evaluation is based on the plant configuration during the degraded condition to assess what the increase in risk was observed. Given this information, management changes can be implemented to decrease the future likelihood of being in these degraded conditions.

In general, configuration risk management can be defined as consisting of three parts:

- **Configuration**: Assess the plant configuration accounting for the status of plant components.
- **Risk**: Quantify a risk metric (e.g., core damage frequency, core damage probability) for the assessed plant configuration which typically includes comparison against nominal plant configuration.
- **Management**: Take measures to avoid risk-significant configurations, acquire better understanding of the risk level of a particular plant configuration, and/or limit the duration and frequency of such configurations that cannot be avoided.

In this report, we describe the technical basis behind how to use the Risk Informed Safety Margin Characterization (RISMC) process for configuration risk management activities. To help demonstrate technical issues and solutions, we use both the Advanced Test Reactor (ATR) and other models as example calculations. The following sections provide background information about different potential applications of risk management in the Significance Determination Process (SDP), using risk monitors to calculate the risk, and lastly how the a variety of probabilistic models (e.g., operator actions, common cause failures) can impact the final result.

1.1 Significance Determination Process (SDP)

The SDP was developed by the Nuclear Regulatory Commission (NRC) based on Commission paper SECY-00-007A as a tool to evaluate inspection findings related to reactor safety. This method was

designed to assign a probabilistic risk characterization to public health and safety. SDP uses risk insights when determining the significance of the inspection finding. SDP was developed to be consistent with thresholds used for risk-informed plant Performance Indicators (PIs). Therefore, both inspection findings and PIs can be used as inputs into the plant performance part of the Reactor Oversight Process. From the initial SDP tool of just reactor safety, other SDP tools were developed to characterize the safety significance of issues related with emergency preparedness, occupational and public radiation safety, physical protection, fire protection, shutdown operations, containment integrity, operation requalification, and steam generator tube rupture. Depending upon the information available, these SDP tools evaluate the finding using either quantitative risk evaluation methods or risk-informed through expert judgment.

The SDP tool of interest in this report is to evaluate at-power reactor safety to determine the significance of the inspection finding. Note though that the methods and technical solutions described will also be applicable to other modes of plant operation such as during low-power modes. Within the full-power SDP approach, the traditional process uses a worksheet defined in Appendix A of Inspection Manual Chapter (IMC) 0609. (NRC Inspection Manual, 2011) The worksheet is designed to screen the inspection findings as Green or greater than Green. If the worksheet cannot screen the inspection finding (i.e., Green), then a detailed analysis is required. This detailed analysis will use a probabilistic risk assessment model developed for the plant to determine the significance of the finding. Colors are then assigned to the assessment of the inspection finding.

The quantitative and qualitative definitions of the SDP colors (IMC 0609, Section 4) are:

a. **Red** (high safety or security significance) is quantitatively greater than 10^{-4} Δ core damage frequency (CDF) or 10^{-5} Δ large early release frequency (LERF). Qualitatively, a Red significance indicates a decline in licensee performance that is associated with an unacceptable loss of safety margin. Sufficient safety margin still exists to prevent undue risk to public health and safety.

b. **Yellow** (substantial safety or security significance) is quantitatively greater than 10^{-5} and less than or equal to 10^{-4} ΔCDF or greater than 10^{-6} and less than or equal to 10^{-5} ΔLERF. Qualitatively, a Yellow significance indicates a decline in licensee performance that is still acceptable with cornerstone objectives met, but with significant reduction in safety margin.

c. **White** (low to moderate safety or security significance) is quantitatively greater than 10^{-6} and less than or equal to 10^{-5} ΔCDF or greater than 10^{-7} and less than or equal to 10^{-6} ΔLERF. Qualitatively, a White significance indicates an acceptable level of performance by the licensee, but outside the nominal risk range. Cornerstone objectives are met with minimal reduction in safety margin.

d. **Green** (very low safety or security significance) is quantitatively less than or equal to 10^{-6} ΔCDF or 10^{-7} ΔLERF. Qualitatively, a Green significance indicates that licensee performance is acceptable and cornerstone objectives are fully met with nominal risk and deviation.

The ΔCDF is the metric that is calculated using a risk-informed process. ΔCDF is the increase in annualized CDF risk due to identified deficiencies compared to the nominal annualized CDF based on nominal routine plant operations. The ΔCDF calculation starts with determining the conditional core damage frequency, which is then multiplied by the duration to obtain the conditional core damage

probability. The conditional part is due to the deficiency observed and calculated using the PRA model to determine the probability that the condition came to a core damage state. The second part is the nominal CDF multiplied by the duration of the deficiency to obtain the core damage probability. The nominal CDF includes the risk contribution from component failures that are expected. The core damage probability is subtracted from the *conditional* core damage probability and then annualized by dividing by 1 yr. By annualizing the deficiency, the inspection finding is comparable with the PIs and can be used in the NRC Action Matrix.

In this report, we extend this general idea of using risk models to calculate a configuration specific safety margin and risk metrics (core and/or fuel damage frequency) using the simulation-based approach as described in the RISMC methodology developed as part of the Light Water Reactor (LWR) Sustainability Program. (Smith, Rabiti, & Martineau, 2012)

1.2 Configuration Risk Monitor

Risk monitors are software tools used by nuclear power plant staff to schedule maintenance activities. The risk monitor will query the plant's PRA and analyze the proposed configuration(s). The result from this calculation determines the risk significance of the configuration and whether or not the scheduled activity should be performed or modified. Risk monitors are used to set up work activities weeks in advance to help work schedulers and plant personnel be prepared on the status of the plant and what components/systems are available.

Risk monitors can be used to assess risk both quantitative using the full PRA including external conditions and qualitatively using defense in depth. The quantitative assessment calculates the change in core damage frequency based on the selected components being removed for testing or maintenance activities. This change in core damage frequency can now be compared to a chart that can be used to determine if the proposed work should proceed. The same process can be evaluated qualitatively by accounting for defense in depth. The following color charts can be used in risk informed process to determine if work should proceed. Table 1-1 provides information and example thresholds that can be used for a qualitative or quantitative evaluation. The thresholds can be adjusted depending upon the plant specific requirements.

A risk monitor has been developed at the Idaho National Laboratory (INL) using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) program for the Advanced Test Reactor (ATR). (Idaho National Laboratory, 2011) This risk monitor uses some of the SAPHIRE interfaces and its internal solving logic but has its own input and output display. Specific to the ATR probabilistic risk assessment (PRA), the risk monitor has been developed in order to monitor change in risk for two safety metrics: core damage frequency (CDF) and fuel damage frequency (FDF).

The ATR risk monitor is designed to continuously monitor in near-real-time the plant CDF or FDF so operations staff can make risk informed decisions regarding important equipment needing immediate repair. The risk monitor also is used in preplanning activities. These activities are based on required maintenance activities or scheduled testing and maintenance activities. The risk monitor provides insights on how risk significant these activities are and if such configurations should be entered into and if they are how long should the configuration be required.

Table 1-1. Color chart used in qualitative/quantitative assessment of plant configuration.

Color	Equipment Availability	CDF Thresholds	Consideration
GREEN	≥ N + 2	< 5E-5/yr	– Preserve operable equipment to the extent possible – Manage special issues that can impact defense in depth – Normal work controls
YELLOW	N + 1	5E-5/yr to 5E-4/yr	– Should be avoided if possible, but not considered potentially risk significant – Prior authorization obtained from Work Controls Manager and Operations Manager – Correct the cause based on the time in configuration and resources available – Assess return to service of selected equipment – Protect risk significant equipment – Return to "GREEN" should be priority
ORANGE	N	5E-4/yr to 1E-3/yr	– Requires senior management review and approval – Minimize exposure using return to service priorities – Develop and implement contingency actions – Protect risk significant equipment
RED	< N	> 1E-3/yr	– Never plan to enter
Note: N = minimum equipment required for each safety function or plant transient			

The ATR risk monitor provides the facility work planners with risk profiles detailing the proposed work. Figure 1-1 shows a generic output from the ATR risk monitor.

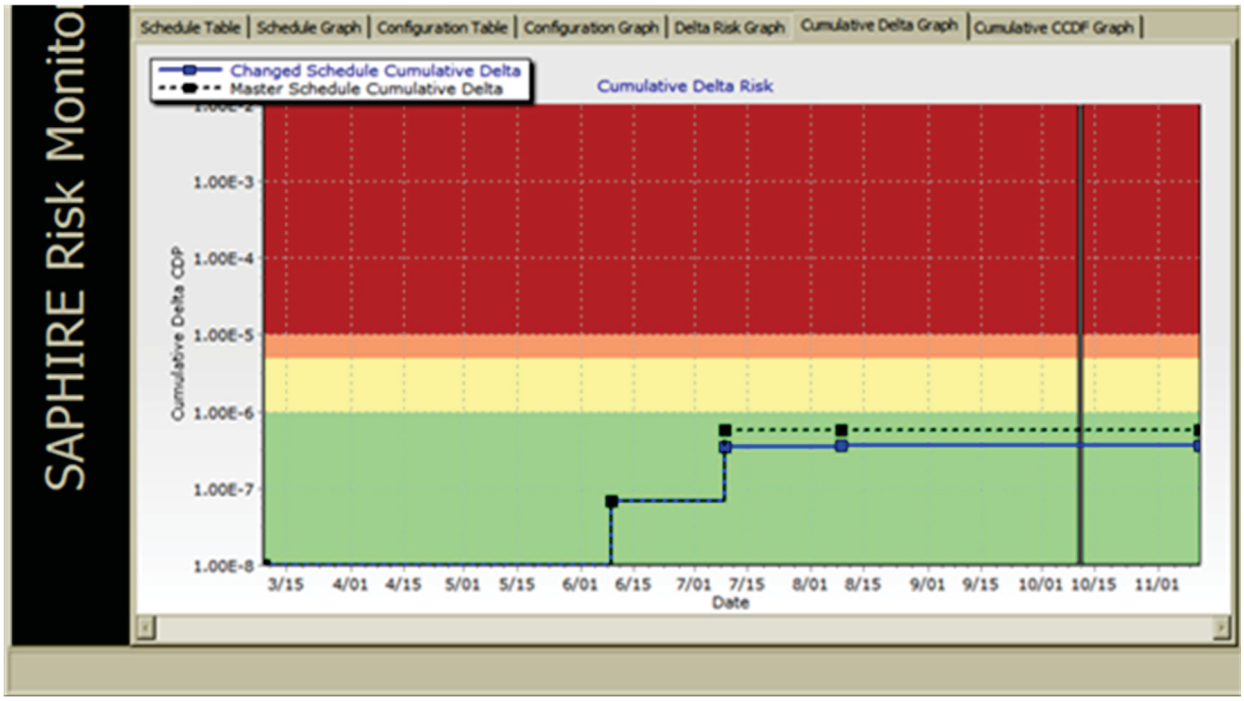

Figure 1-1. ATR risk monitor output plot.

1.3 Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H)

Human operations over time have been shown to have impacts on accidents at many industries. (Rasmussen, Nixon, & Warner, 1990) Because of the impacts of human operations to accidents, they are modeled in PRAs as part of the system. These interactions are identified as the human-machine interface. The process of analyzing these impacts on industry accidents has led to an evolving field on human reliability analysis (HRA). Standardized plant analysis risk human reliability analysis (SPAR-H) is one method that has been used to perform HRA. SPAR-H was developed as a simple method to help in accounting for human errors when: (a) performing safety studies such as PRA; (b) helping to risk-inform the inspection process; (c) reviewing special issues; and (d) helping to risk-inform regulation. (Gertman, Blackman, Marble, Byers, & Smith, 2005)

SPAR-H is a worksheet process that identifies the human error probability (HEP) dependent on the operator response being an action or diagnosis type. An operator action can be identified as starting a pump or other activities performed when following plant procedures. A diagnosis action can be identified as reliance on knowledge and expertise to understand existing conditions and prioritize plan of actions based on information available. The SPAR-H worksheet also takes into account performance shaping factors (PSFs). PSFs are designed to influence the HEP based on information available to respond to

existing conditions and other factors. The factors that are used to shape the HEP are: 1) available time; 2) stress and stressors; 3) experience and training; 4) complexity; 5) ergonomics (including human-machine interface); 6) procedures; 7) fitness for duty; and 8) work processes. These PSFs can positively or negatively influence the HEP.

Figure 1-2 shows how the PSFs are utilized to influence the HEP. This method is used in the ATR PRA on calculating the different operator action HEPs. This method is also used when assessing the different potential configurations of the ATR systems. These adjustments are all part of using a risk-informed approach to safety.

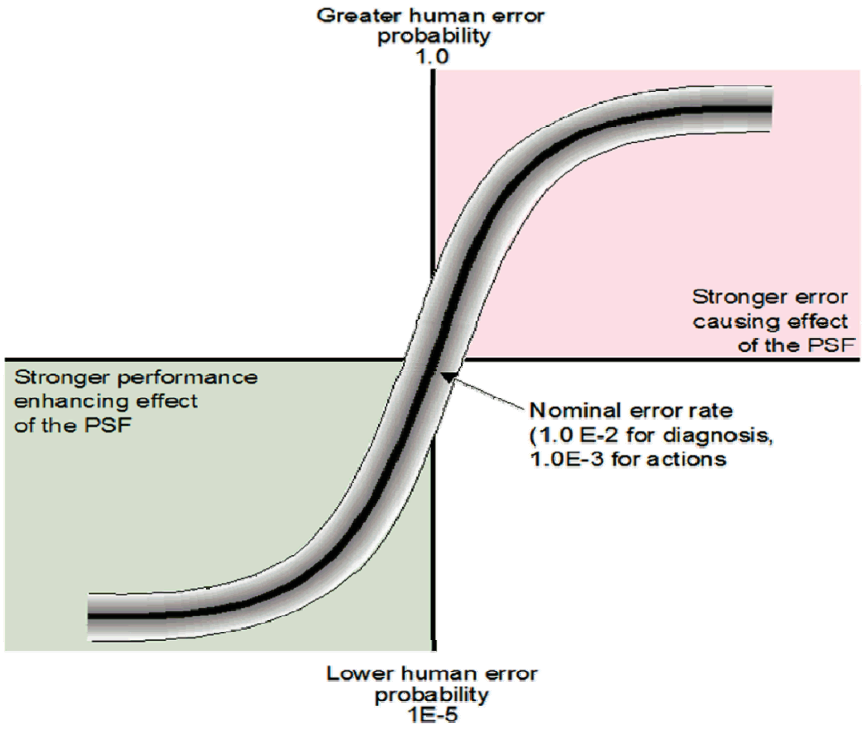

Figure 1-2. Mean HEP as a function of the influence of performance shaping factors.

One use of models such as SPAR-H is to integrate the operator model directly into the RISMC simulation framework in order to produce HEPs that change as the nature of the accident scenario changes. For example, during a simulation run, the time available to carry out an activity (one of the PSFs in SPAR-H) will change which implies a change in the HEP. This information can be used as part of the simulation to provide enhanced realism in the configuration risk management.

1.4 Background on the Advanced Test Reactor (ATR)

Constructed in 1967, the ATR is a pressurized water test reactor that operates at low pressure and low temperature. It is located at the Reactor Technology Complex on the INL site, about 40 miles from Idaho Falls, Idaho. The reactor is pressurized and is cooled with water. The reactor core includes a beryllium reflector (the reflector helps concentrate neutrons in the reactor core, where they are needed for fuels and materials testing). The reactor vessel is a 12-foot diameter cylinder, 36-feet high, and is made of stainless steel. The reactor core is 4 feet in diameter and height and includes 40 fuel elements capable of producing a maximum power of 250 MW. The reactor inlet temperature is 125°F, and the outlet temperature is 160ºF. The reactor pressure is 390 pounds per square inch. (Idaho National Laboratory)

The ATR core is designed to be flexible for research purposes. The reactor can be brought online and powered down several times a year (resulting in several cycles per year) in order to change experiments or perform maintenance. The reactor is also powered down automatically in the event of abnormal experimental conditions or power failure. The internal components of the reactor core are replaced as necessary every 7–10 years to prevent radiation fatigue. Experiments are changed on average every seven weeks, and the reactor is in nominal operation (110 MW) approximately 75% of the year.

An example of the reactor core, vessel, experimental piping, and control systems is shown in Figure 1-3. A line diagram (also known as a piping-and-instrumentation diagram) is shown in Figure 1-4 and represents typical components found in experimental flow loops.

The ATR has a detailed PRA. As part of the development of the ATR PRA, select thermal-hydraulic (T-H) calculations were performed with the RELAP5 (RELAP5 Code Development Team, 2012) series of systems analysis tools. However, like most other PRAs, the coverage of risk scenarios by T-H calculations is very minimal. Nonetheless, for some of those scenarios that are modeled by RELAP5, the plant T-H characteristics have been validated by operational data. In addition to the RELAP5 T-H input deck, the ATR has an updated PRA using current practice static fault tree and event tree models. The PRA software tool used to both edit and solve the probabilistic model is the INL-developed SAPHIRE software. (Idaho National Laboratory, 2011)

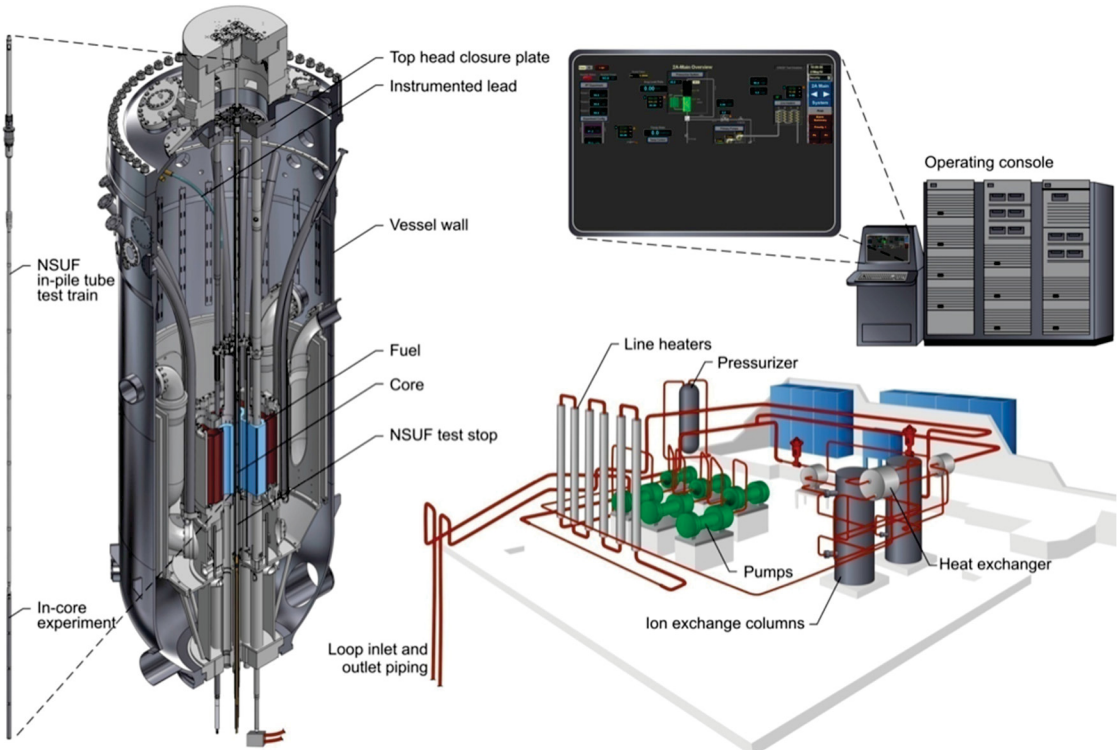

Figure 1-3. ATR experiment loop schematic representation.

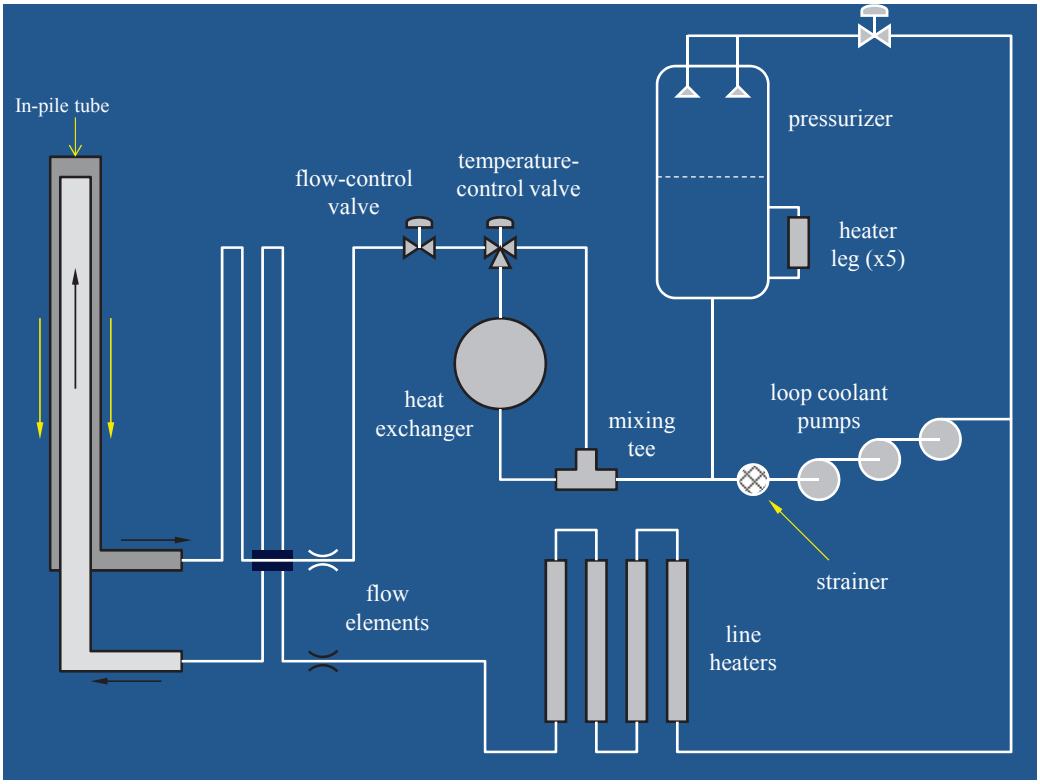

Figure 1-4. Component line diagram for an ATR experiment loop.

2. CONFIGURATION RISK MANAGEMENT TECHNIQUE

The RISMC method for determining safety margin and risk metric (CDF and/or FDF) will be used when applying the configuration risk management process to the ATR plant. The RISMC method will be able to calculate the safety margin based on the proposed configuration (i.e., the component being removed for testing or maintenance activities). The different configurations will have varying degrees of risk on the plant. By evaluating this increase in risk, the remaining safety margin is determined.

The RISMC method calculates a safety margin based on the concept of probabilistic margin, which is defined by the probability of the load exceeding the capacity. An example of this would be a pump failing to perform its required function due to overheating. A pump is designed to operate within temperature constraints and outside those constraints, the likelihood of pump failure increases. The pump's operating temperature is a distribution f(**C**) and its loading condition (room temperature) is a second distribution f(**L**). The probabilistic margin would then be represented by Pr[f(**L**) > f(**C**)].

The result for simulating both the load and capacity and then comparing them as shown in the expression above provides the probabilistic safety margin. The probabilistic safety margin is a numerical value quantified that key safety metrics will be exceeded under specified accident sequences. Figure 2-1 shows a simplistic example of how this process works.

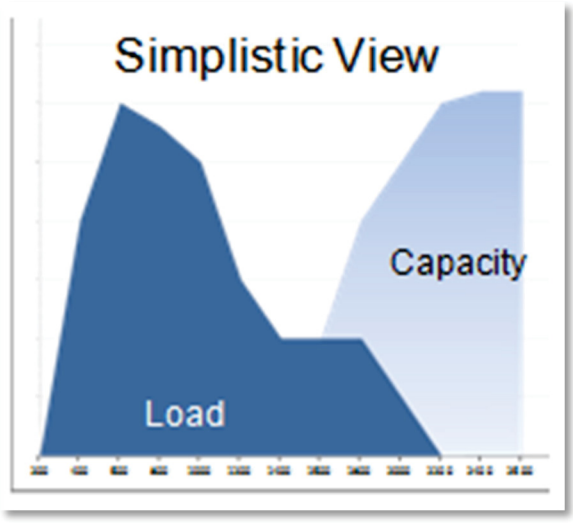

Figure 2-1. Simplistic view of the probabilistic safety margin.

To illustrate the RSMIC process, an example configuration will be evaluated. The example will evaluate a configuration to obtain the safety margin (risk) based on a component being unavailable for a duration of time.

2.1 Safety Margin Case Study Process

The safety margin for different plant specific configurations will be discussed and evaluated. The evaluation process will use the specific steps identified in the RISMC process, which includes a methodology for carrying out simulation-based studies of safety margin. (Smith, Rabiti, & Martineau, 2012) Figure 2-2 provides an overview of each of the RISMC process steps.

The RISMC process steps are listed below with a figure depicting the process.

1. Characterize the issue to be resolved and the safety figures of merit to be analyzed in a way that explicitly scopes the modeling and analysis to be performed.

2. Describe the decision-maker and analyst's state-of-knowledge (uncertainty) of the key variables and models relevant to the issue. For example, if long-term operation is a facet of the analysis, then potential aging mechanisms that may degrade components should be included in the quantification.

3. Determine issue-specific, risk-based scenarios and accident timelines.

4. Represent plant operation probabilistically using the scenarios identified in Step 3. For example, plant operational rules (e.g., operator procedures, technical specifications, maintenance schedules) are used to provide realism for scenario generation. Because numerous scenarios will be generated, the plant and operator behavior cannot be manually created like in current risk assessment using event- and fault-trees. In addition to the *expected* operator behavior (plant procedures), the probabilistic plant representation will account for the possibility of failures.

5. Represent plant physics mechanistically. The plant systems-level code is used to develop distributions for the key plant process variables (i.e., loads) and the capacity to withstand those loads for the scenarios identified in Step 4. Because there is a coupling between Steps 4 and 5, they each can impact the other. For example, a calculated high loading (from pressure, temperature, or radiation) in an SSC may disable a component, thereby impacting an accident scenario.

6. Construct and quantify probabilistic load and capacity distributions relating to the figures of merit analyzed to determine the probabilistic safety margin.

7. Determine how to manage uncharacterized risk. Because there is no way to guarantee that all scenarios, hazards, failures, or physics are addressed, the decision maker should be aware of limitations in the analysis and adhere to protocols of "good engineering practices" to augment analysis.

8. Identify and characterize the factors and controls that determine safety margin in order to propose Margin Management Strategies. Determine whether additional work to reduce uncertainty would be worthwhile or if additional (or relaxed) safety control is justified.

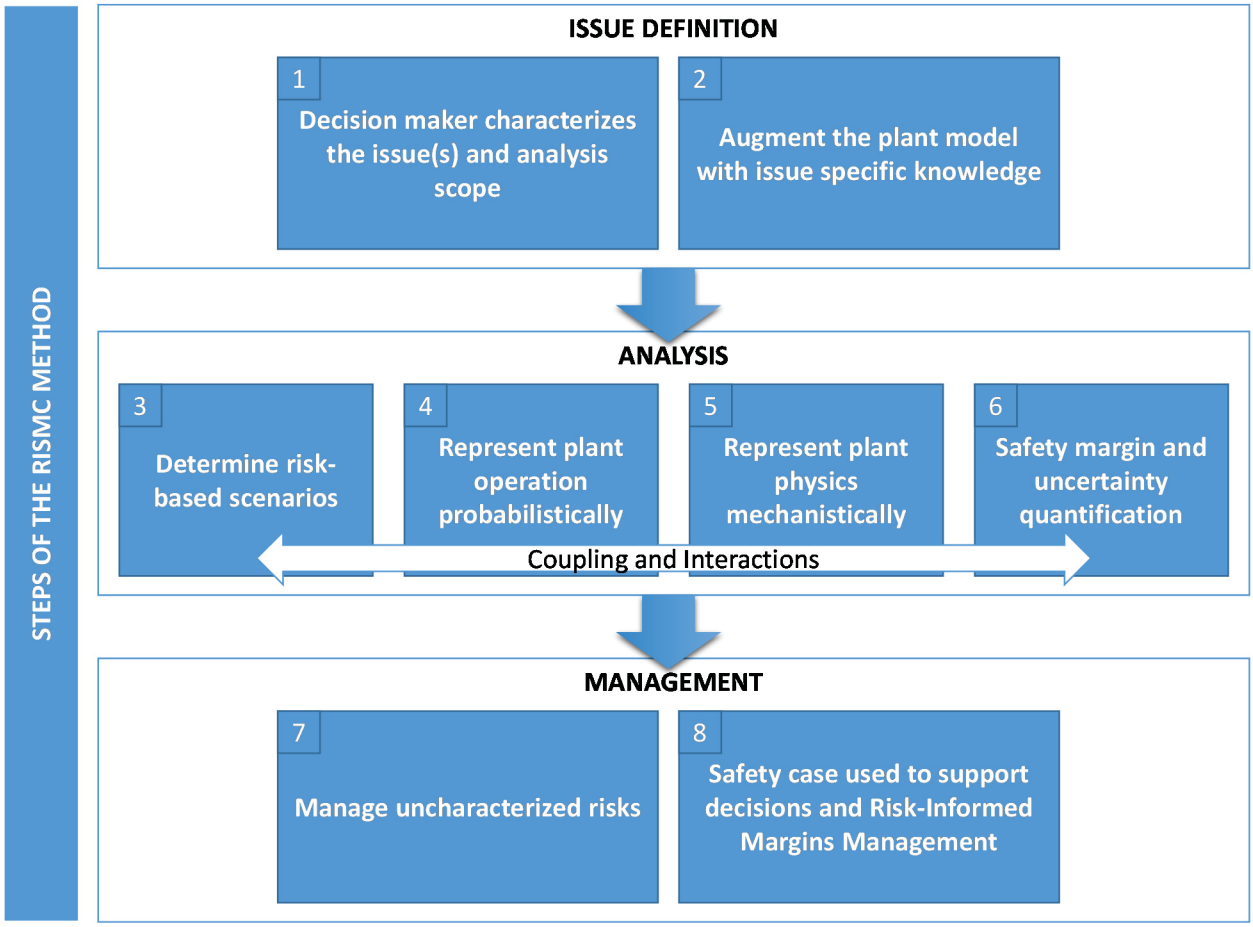

Figure 2-2. Depiction of the high-level steps required in the RISMC method.

The RISMC process will be demonstrated to evaluate the plant configuration (i.e., component(s) unavailable due to maintenance activities or in a degraded condition) to obtain the safety margin and risk metric. The result from this evaluation will be compared to a baseline result. The reason for this comparison is the plant under normal operation will have a safety margin built in and under certain conditions this safety margin may be reduced. The result of the RISMC process will show a safety margin calculation given the current configuration that can be compared to a pre-determined safety margin and then a delta change in risk. Using both of these metrics, minimum remaining safety margin and delta change in risk, will be used for plant personnel to make decisions on allowing the activities to proceed.

2.1.1 Application of RISMC Simulation Process

The RISMC simulation process will be used to perform the configuration risk management evaluations. The RISMC simulation process ties both the physical parameters of the plant and the component reliability (failure of components/systems) together. For the configuration risk management part, the component reliabilities will take into account those that are removed from service for maintenance or testing activities or in degraded conditions. The simulation is performed on the

configuration of the plant and the duration of the configuration. Configuration risk management can be a forward looking evaluation and also a retrospective evaluation, i.e., SDP. The configuration of planned maintenance activities will only be entered if there is sufficient safety margin – otherwise the configuration will be adjusted.

Configuration risk management assesses the different configurations that the plant could be in when components are removed for maintenance activities or degraded condition. These configurations can take the form of a component being unavailable to perform its required function due to being unavailable for maintenance or testing as long as it is within technical specifications and the duration is no longer than the required limiting conditions of operation. This configuration places the mitigating system in a degraded condition if an initiating event were to occur. These types of configurations need to be evaluated in to understand amount of safety margin remaining.

The process steps to perform configuration evaluations are provided below.

1) The plant is operating at a steady state condition prior to the simulation. The first part is to simulate the PRA based on different initiating events. Each initiating event is simulated due to its impact on the reactor plant. Given an initiating event occurs, perform T-H calculations on the reactor plant applicable to the evolving scenario. Plant status from the T-H calculations provides feedback to the mitigating systems in order to determine success criteria.

2) The plant physics (pressure, temperature, and flow rate) are used to determine the success criteria for the mitigating systems. The PRA and system-specific information will provide the system alignment and failure rates/probabilities for the components. Based on the plant physics and the component failure rates, the simulation process determines if the mitigating system was able to meet the plant requirement to place it into a safe and stable condition or a stable condition until it transitions to the next required mitigating system.

3) If the mitigating system fails to perform its required function, T-H calculations are performed to determine the plant status based on this condition and timing into the initiating event. If the plant reaches an unsafe condition (e.g., elevated core temperatures), the simulation stops (unless the accident progression is to also be modeled) and this scenario is a failed state. If the plant does not reach a degraded state, then the next mitigating system is simulated. This next mitigating system provides the required defense in depth.

4) If the mitigating system met the plant requirements to place it in a safe condition, the simulation process ends and this scenario is a success state. If however, another mitigating system is required for the plant to be placed in a safe and stable condition, the simulation continues onto the next mitigating system.

5) The simulation continues until the plant T-H calculations and the mitigating systems place the plant into a success state or a failure state.

6) The mitigating systems will be simulated based on the potential configurations. For example, if one train of a two train system will be out for maintenance or degraded condition, then the simulated mitigating system will account from this condition. The simulation will also account for the duration the configuration.

A simple example of the simulation process discussed above is shown in Figure 2-3. The figure displays each of the steps required to perform the simulation process. The system response (degraded) box is where the RISMC simulation process changes to account for the different potential configurations. For this simple case of a loss of normal feedwater initiating event, the mitigating system is in a degraded condition based on one of the three trains is unavailable. The remaining trains are simulated to determine if they operate in order to meet the plant requirements to place it in a stable condition. The stable condition is denoted by the upper box given successful operation of one of the two pumps. However, if the remaining trains fail to start or run (each will have different effects on the plant physics) the T-H calculations are performed to determine if a degraded plant state has occurred. If this degraded state did occur, a safety margin is calculated and this ends the simulation. The process starts back over until a sufficient number of simulations have been performed.

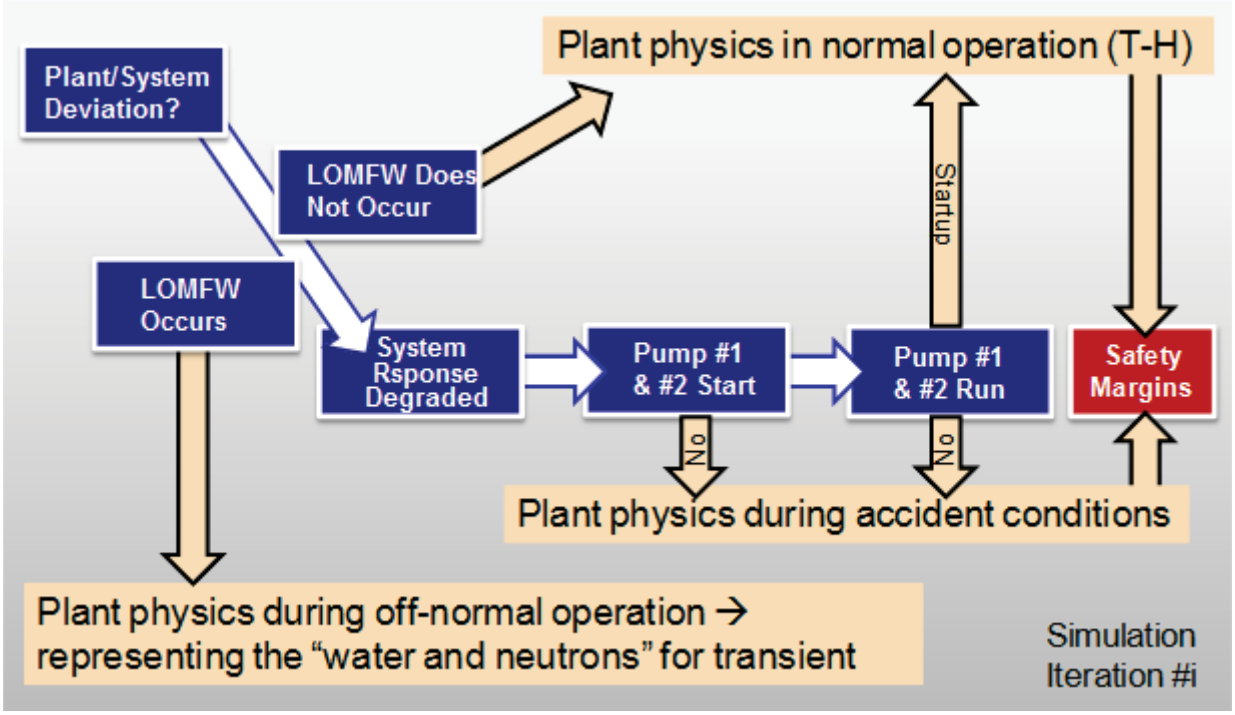

Figure 2-3. Simple example of applying the RISMC process steps.

2.1.2 Simulation process versus traditional PRA application to evaluation potential configuration risk

Configuration risk management has been traditionally evaluated using the traditional PRA approach instead of the RISMC simulation process discussed above. The traditional PRA utilizes fault tree/event tree logic to develop sequences that are assumed to lead to core damage or safe and stable conditions. The traditional PRA traces time out to 24 hours (another possibly questionable assumption, recall that the Fukushima Units 2 and 3 did not see core damage until 24 hours after the initiating event, which is assumed to be "ok" in traditional PRA models) and assumes if the mitigating system operates for this duration then system success is achieved. The traditional PRA also assumes a decay heat level at the start of the event, which is time equal to zero. Usually no consideration is taken into account for the

change in decay heat level given the equipment operated for some time after the event but failed prior to the assumed 24 hours. (Note: this failure mode has been receiving attention in trying to account for the duration of success prior to the time the component failed, something simulation methods can handle directly.) The failure of equipment during operation has impacts in different areas of the PRA; timing to core damage, additional time to recover from event, battery depletion time, etc. This timing issue can have significant impacts on the overall result.

Recommendation #1

When using the RISMC simulation-based approach, the analysis "mission time" should be based upon plant physics (such as peak clad temperatures) rather than a predetermined time window as is currently used in traditional PRA.

For the simple example that will be discussed below, the traditional PRA structure that would be developed is shown in Figure 2-4. The simple PRA structure uses an event tree to define the scenarios (sequence) that lead to core damage or safe and stable condition. The fault tree also shown in Figure 2-4 provides the logic structure of a two train system required to provide decay heat removal capability given the initiating event were to occur. The one sequence is solved to obtain all of the potential cut sets. Note that we use this traditional approach simply to contrast with the improved methods available as part of the RISMC framework.

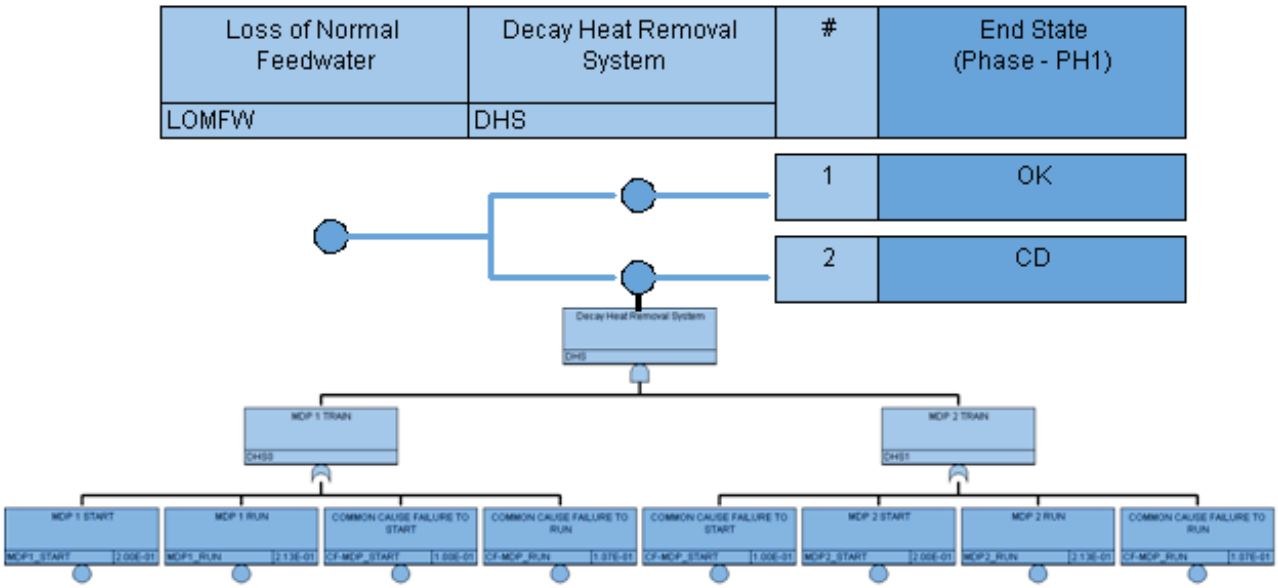

Figure 2-4. Simple example of traditional PRA event tree/fault tree.

The results from solving the logic model are listed in Table 2-1. There are a total of six different combinations that lead to core damage.

Table 2-1. Loss of normal feedwater example event tree results.

Cut Set #	**Individual Cut Set**	**Basic Event Description**
1	LOMFW CF-MDP_RUN	Loss of Normal Feedwater (initiating event) COMMON CAUSE FAILURE TO RUN
2	LOMFW CF-MDP_START	Loss of Normal Feedwater (initiating event) COMMON CAUSE FAILURE TO START
3	LOMFW MDP1_RUN MDP2_RUN	Loss of Normal Feedwater (initiating event) MDP 1 RUN MDP 2 RUN
4	LOMFW MDP1_RUN MDP2_START	Loss of Normal Feedwater (initiating event) MDP 1 RUN MDP 2 START
5	LOMFW MDP1_START MDP2_RUN	Loss of Normal Feedwater (initiating event) MDP 1 START MDP 2 RUN
6	LOMFW MDP1_START MDP2_START	Loss of Normal Feedwater (initiating event) MDP 1 START MDP 2 START

2.1.3 Example of simulating probabilistic operations

Using the same example as in the previous section, the simulation process can be viewed as a "Swiss cheese model" where each of the inputs is simulated until they occur. Failure of the simulation occurs when all of the negative inputs line up as illustrated in Figure 2-5. The initiating event is simulated until it occurs as shown by the red arrow and yellow arrow. Given the occurrence of the initiating event, the mitigating systems are then simulated to see if system failure has occurred. If the mitigating system is successful, no core damage occurs as depicted by the yellow arrow. If the mitigating systems fail and they all fail in a single path as depicted by the red arrow, this leads to the condition being analyzed, in this case core damage. The simple simulation example below will illustrate this process.

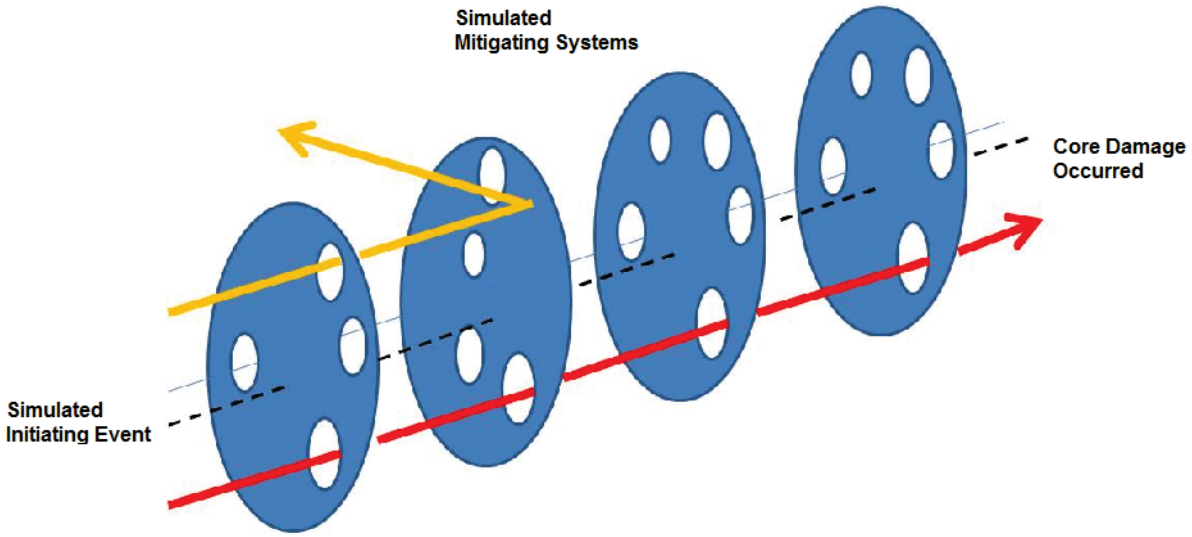

Figure 2-5. Swiss Cheese Model to illustrate the simulation process. (Reason, 1990)

2.1.3.1 Calculating the Nominal Case

An example configuration risk management will be evaluated using the RISMC method. (Refer to Appendix A for a more detailed explanation of the discrete event simulation process that this simple example utilizes.) The example will look at the perturbation of the operating reactor due to a loss of normal feedwater, which will cause the standby feedwater system to start and provide decay heat removal. For this example, the data used for the sampling part will be higher than what the expected probabilities will be for these components. This example will first perform the sampling based on nominal alignment, i.e., two pumps in the system and a success criterion of one-of-two pump trains. Then, to illustrate the configuration risk management part, one pump train will be removed due to a degraded condition. For this example, the probabilistic models for the plant events are:

- Loss of normal feedwater – LOMFW ~ Poisson(λ=0.1/yr)
- Failure of a MDP to start – MDP_START ~ Binomial(p=0.2/demand)
- Failure of a MDP to run – MDP_RUN ~ Poisson(λ=0.01/hr)
- Beta factor for both pumps to start or run = 0.5

where the "~" means "defined as the probabilistic distribution."

A simulation analysis was created and ran N number of iterations. The first check was to see if the initiating event occurred within the mission of the next year. The results of this simulation are shown in Figure 2-6, where an iteration represents a single year of plant operation. Based on this simulation process, whenever the duration was less than one year, it was assumed that the initiating event (LOMFW) occurred. From the figure, there were a total of 9 initiating events over 100 hundred iterations (years), which is on average of what we would expect.

For this example, 91 iterations (years) out of the 100 iterations (years), no initiating event occurred and the other 9 iterations (years) a loss of normal feedwater initiating event occurred. However, just because the initiating event happened does not mean that core damage has occurred at the plant. The next process is to account for the standby mitigating equipment.

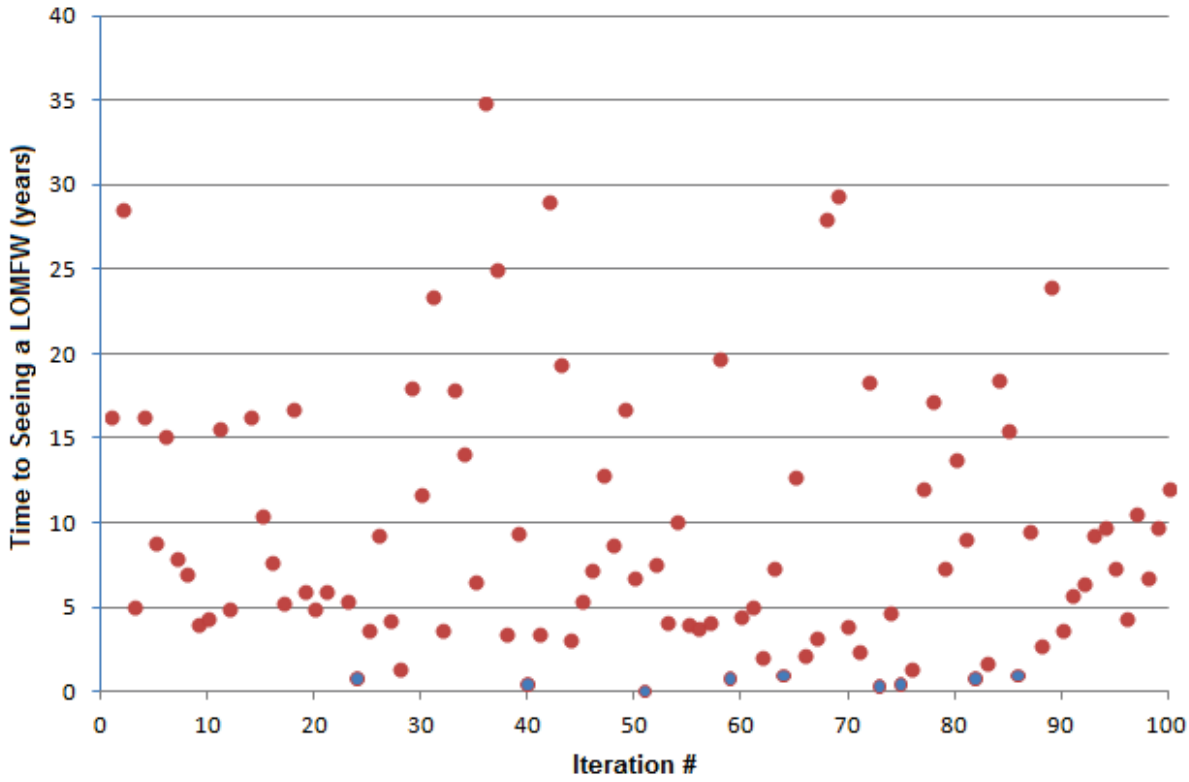

Figure 2-6. Simulation results of LOMFW initiating event occurrence.

The simulation now checks to see if the standby decay heat removal system failed to respond given an initiating event. Every time there is an initiating event, the system is required to start and provide cooling. To perform this check, the probability of a motor-driven pump failing to start is checked to see if it is less than the failure probability of 0.2. If this is the case, then it is assumed that the pump is failed. Based on the nine initiating event occurrences, three times the first pump failed to start. Since this is a two train system now the process must check to see if the second pump failed to start. For this simple case, the second pump can fail either dependently or independently. To account for the dependence (i.e., common cause failure), the beta probability (conditional probability that if one pump has failed the probability of the other pump failing is not independent) is checked to see if the probability is less than

the sampled value. If this is the case, then the second pump is assumed to have failed to start which is system failure. If the sampled probability is larger than the beta probability, then the independent fails to start probability of the second pump is checked. Based on this multi-step process, Figure 2-7 shows that there were two system failures once due to common cause and once due to both independent failures.

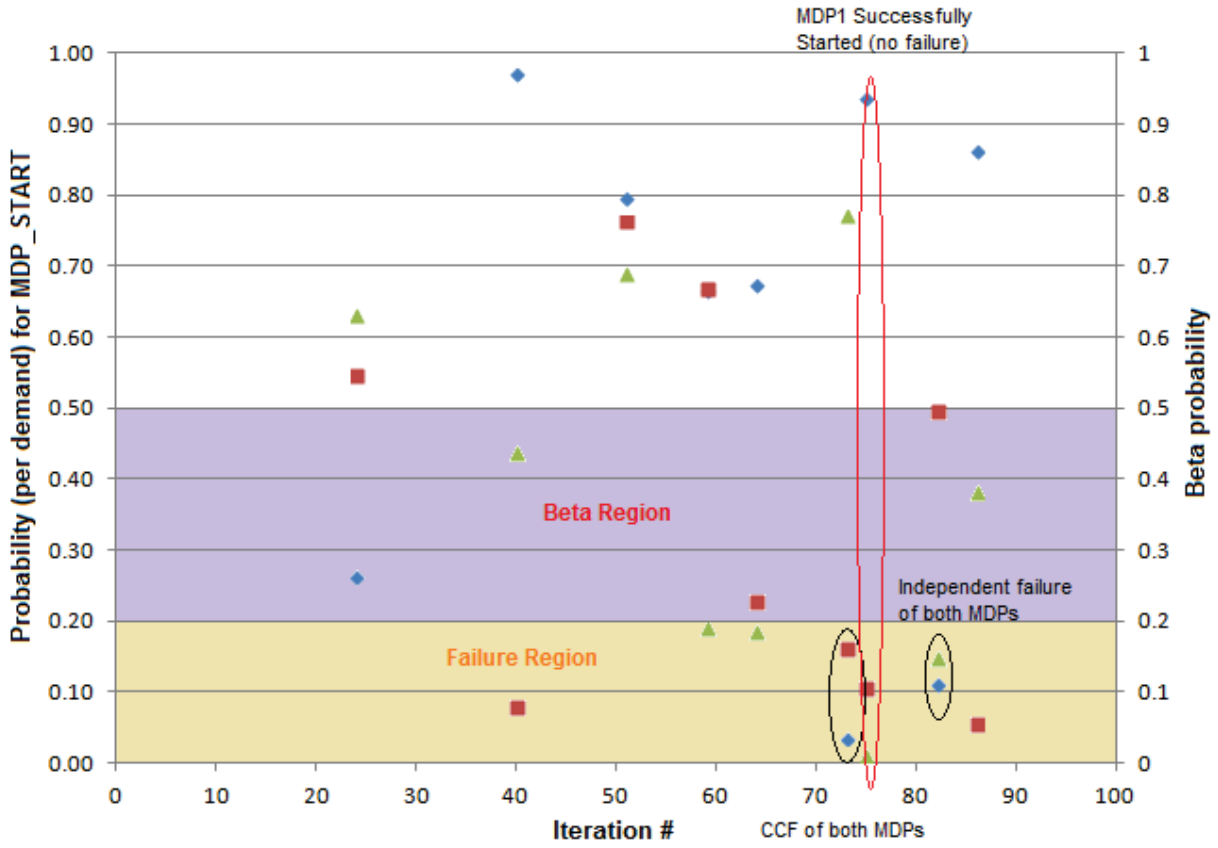

Figure 2-7. Simulation results of mitigating system failing to start.

The last part of the example is to consider when the MDP(s) have started and question did they operate for the full mission time. This mission time can be adjusted based on the reactor physics that will be evaluated and tied to the probability simulation. However, for this simple example it will be assumed if the pump operated for 24 hours the system is successful. The determination of system success or failure is the same as what was done from the failing to start. An operating duration was calculated randomly and then checked against the 24 hour duration. If the calculated time was greater than 24 hours, the system successfully performed its intended function. Figure 2-8 shows that the system failed to provide cooling flow longer than 24 hours twice. Both of these system failures are due to common cause failure. This was determined by checking if the first pump failed to operate for the full 24 hours and if it did not, then a random probability was checked against the beta probability. Again, it was assumed that if a single pump failed, the probability of the second one failing is its conditional probability (beta) versus independent failure. There were no system failures due to both pumps failing to operate for 24 hours.

The results of this nominal simulation will be discussed along with the simulation process for conditional case in the next section.

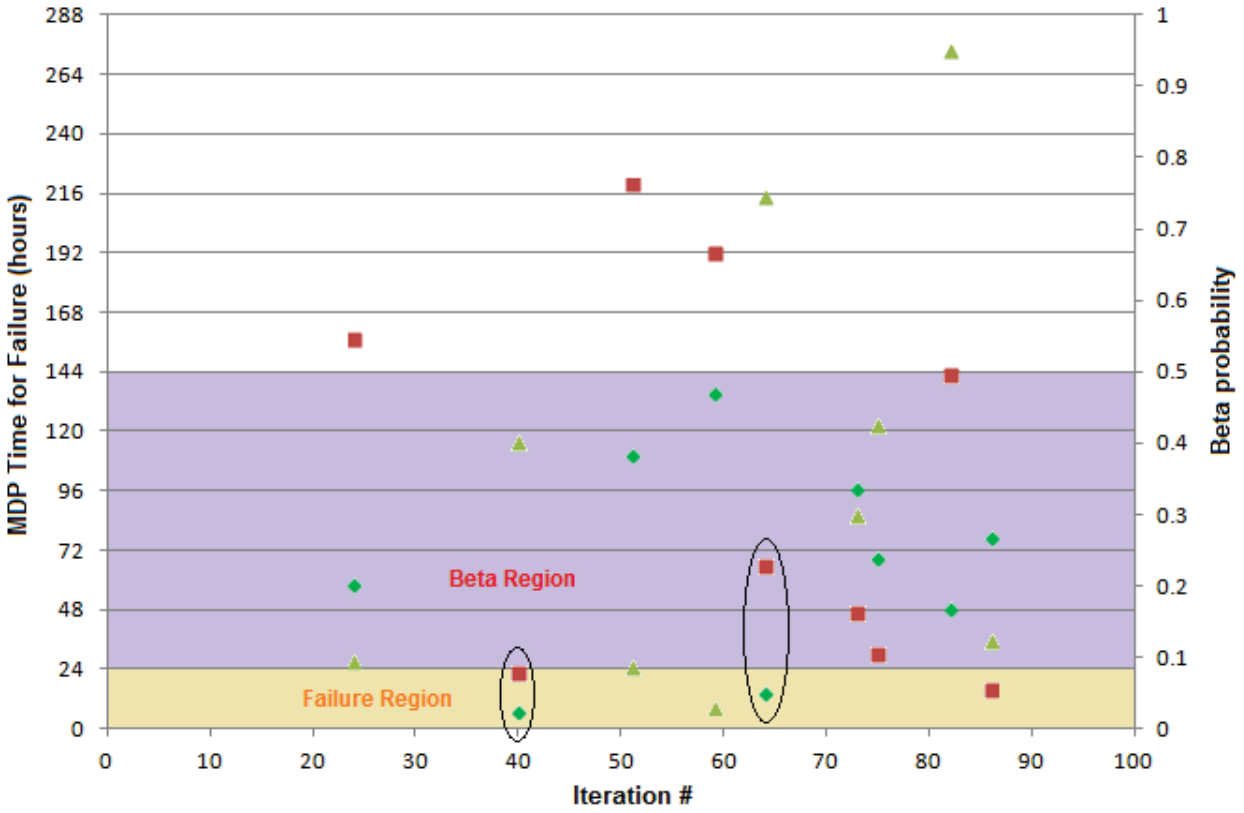

Figure 2-8. Simulation results of mitigating system failing to operate for 24 hours.

2.1.3.2 Calculating the Conditional Case

The example simulation process discussed above was used to obtain the baseline result. However, this same process needs to be used in order to determine the overall change to plant safety margin given one of the pump trains is unavailable. The same example will be used to illustrate that process. Once the simulation is finished (Step 4 of the RISMC method), the next process is to execute Step 5 of the RISMC method which is how to incorporate the plant physics calculations into the process. The incorporation of Step 5 of the RISMC method will be discussed below.

The simple simulation, Step 4 of the RISMC method, is performed based on Steps 1 - 3 of the RISMC method. Steps 1 - 3 are to characterize the analysis and set up the scenarios. For this case one of the pump trains will be unavailable to perform its intended function for some duration.

The simulation first identified the potential of having an initiating event occurring within a year of operation. Figure 2-9 lists the number of initiating events that occurred over 100 iterations. There were a total of 11 initiating events that occurred.

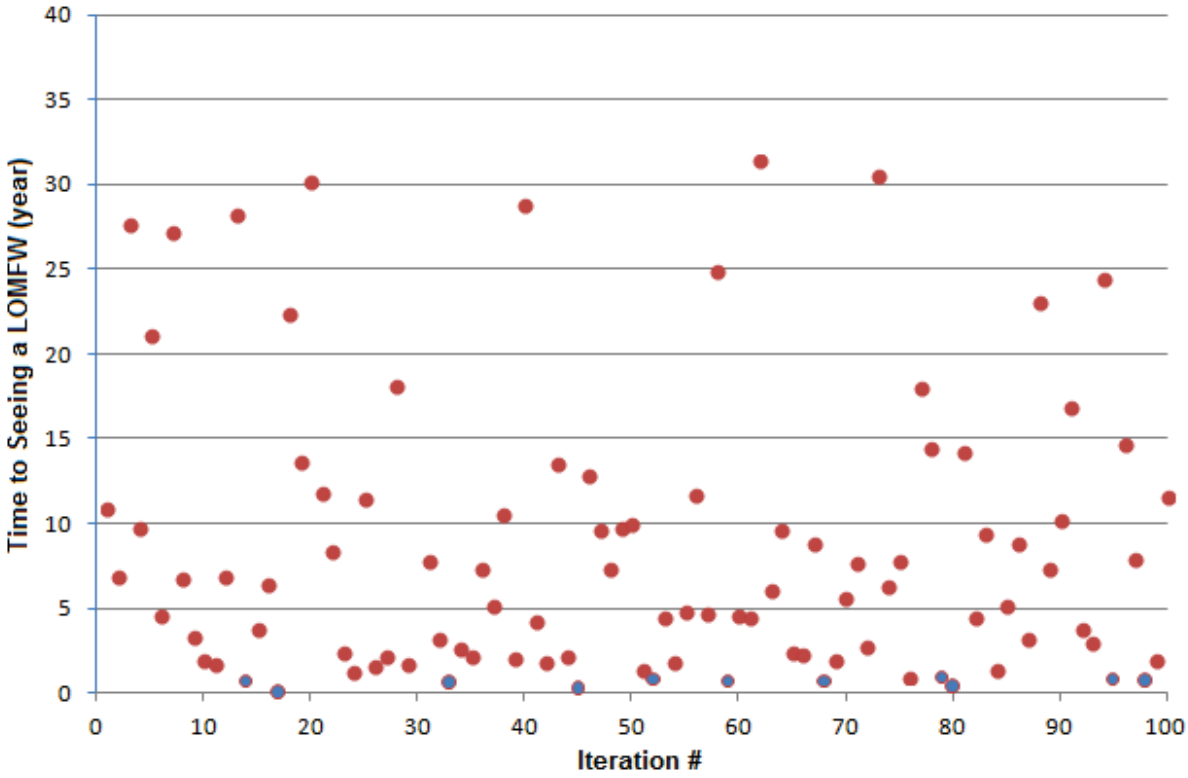

Figure 2-9. Simulation results of LOMFW initiating event occurrence.

The next part looked at the failure of the standby decay heat removal system. Every time there is an initiating event, the system is required to start and provide cooling. To perform this check, the probability of a motor-driven pump failing to start is checked to see if it is less than the failure probability of 0.2. If this is the case, then it is assumed that the pump is failed. Based on the ten initiating event occurrences, three times the first pump failed to start. Since this is a two train system now the process must check to see if the second pump is unavailable. For this simple case, the second pump is assumed to be unavailable 75 percent of the time over a 1 year period (note that "real" components are not typically unavailable this long in actual practice, this assumption is just for illustrative purposes). If the sampled probability is less than 0.75, it is assumed the second pump is unavailable and the system is failed. Based on this multi-step process, Figure 2-10 shows three times the system failed to perform its required function.

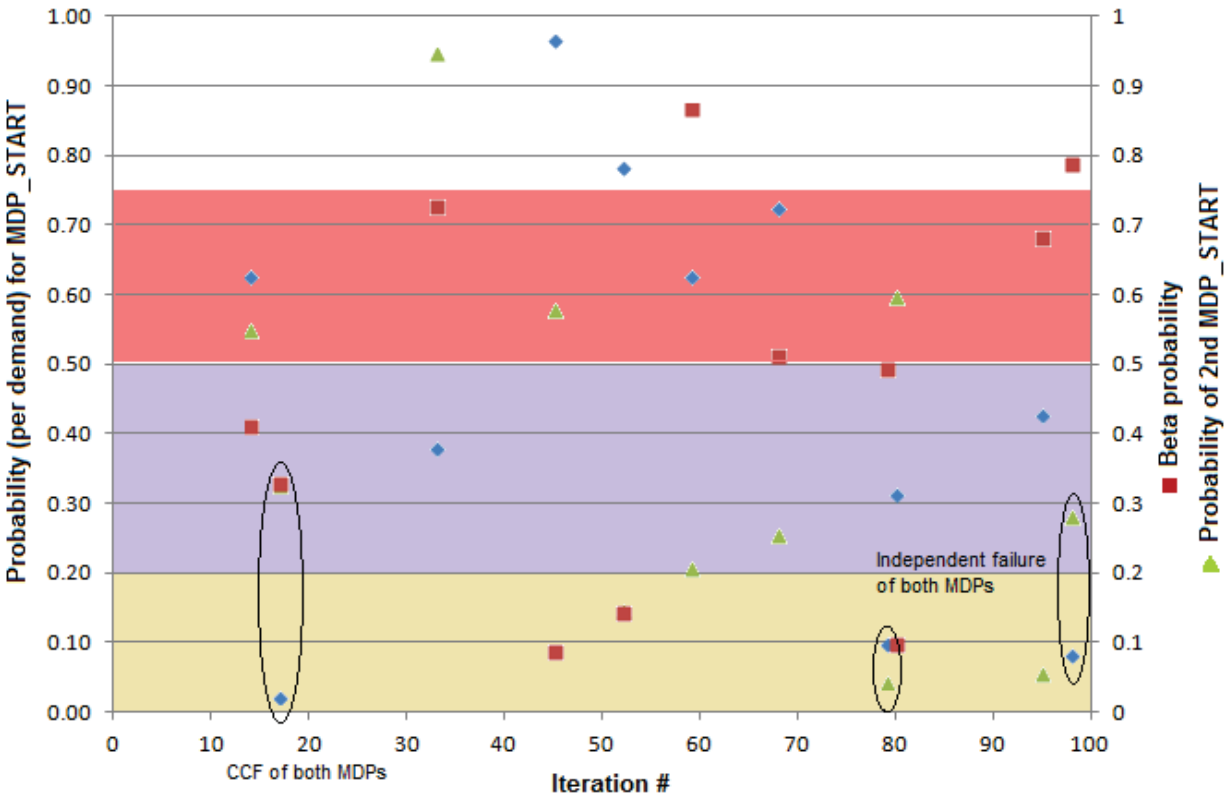

Figure 2-10. Simulation results of mitigating system failing to start.

The next part is to look at the decay heat removal system failing to operate for the mission time required. This simulation process is the same as that discussed above. There was only one time out of the eleven initiating events that the system failed to operate for the full 24 hours. Figure 2-11 shows the operating times for both pumps given the system successfully started.

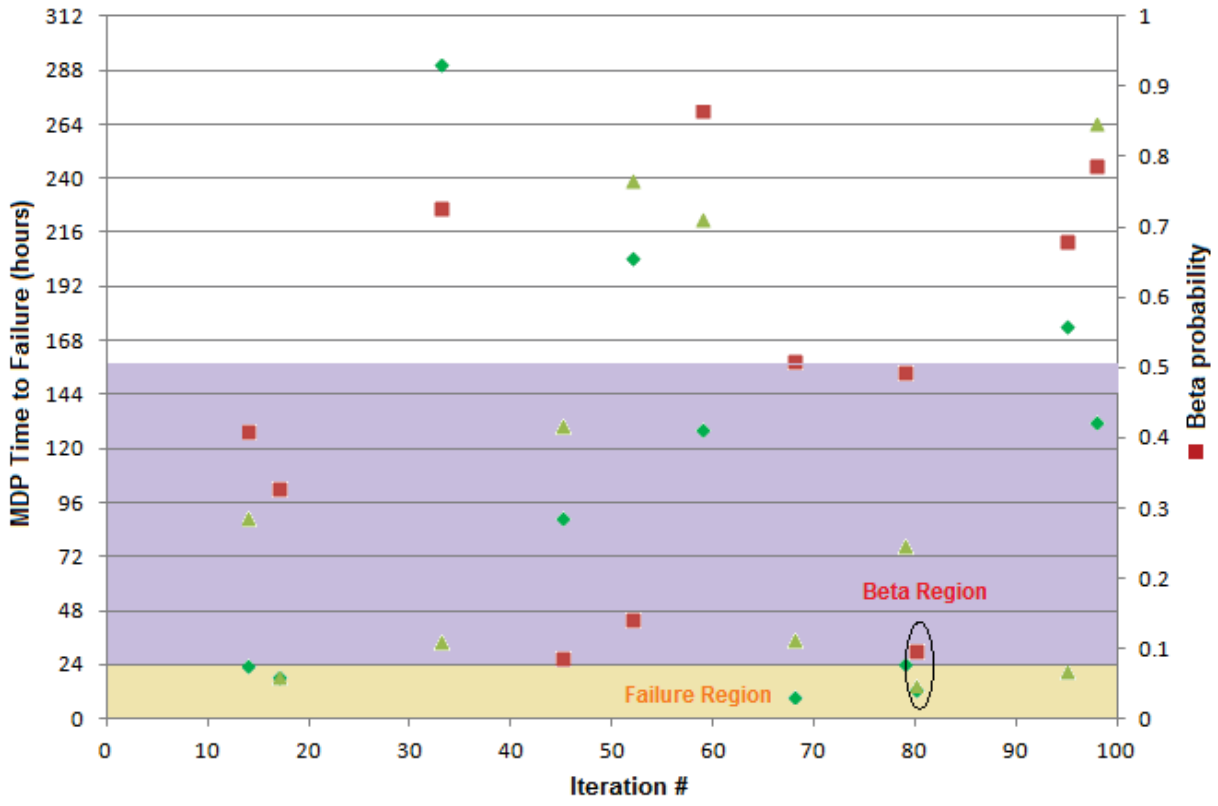

Figure 2-11. Simulation results of mitigating system failing to operate for 24 hours.

Lastly, there are combinations of pump train 1 failing to start and pump train 2 failing to run for the required mission time (and vice versa). This simulation process is the same as that discussed above. There was only one time out of the eleven initiating events that the system failed to operate for the full 24 hours. Figure 2-12 shows the operating times for both pumps given the system successfully started.

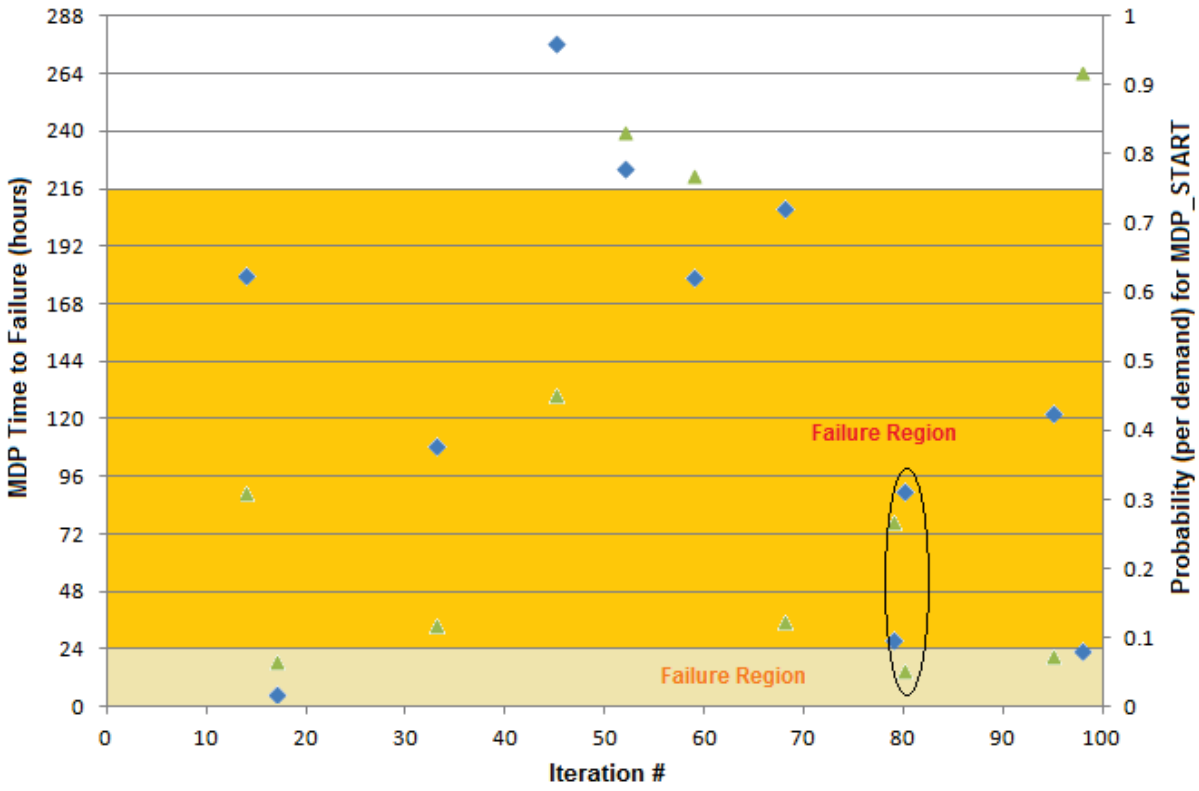

Figure 2-12. Simulation results of mitigating system, MDP1 failing to operate for 24 hours and MDP 2 failing to start.

Now we are at the point in the process where we need to pull all of the simulation information together and provide a description of the risk perspective of the RISMC process to account for one of the pumps being unavailable. The information is broken down into the two different simulations. A comparison will be performed in order to see the effect of a pump train being unavailable. This comparison should be performed along with the evaluated reactor physics. For this example only the change in frequency will be used.

Table 2-2 provides the results of the base result assuming that one of the two pump trains is sufficient to remove decay heat given the initiating event occurred. Table 2-3 provides the results for the simulation process assuming that one pump train is unavailable part of the year.

Table 2-2. Baseline results for the simulation example.

Scenario (outcome)	LOMFW Term	MDP_START Term (CCF and independent)	MDP_RUN Term (CCF and independent)	MDP_RUN and MDP_START	Frequency (per year)
1 (OK)	= 9/100 year	7/9 successes	7/9 successes	9/9 successes	(9/100)(7/9)(7/9)(9/9) = 0.054
2 (CD)	= 9/100 year	7/9 successes	7/9 successes	0/9 failures	(9/100)(7/9)(7/9)(0/9) = 0.0
3 (CD)	= 9/100 year	7/9 successes	2/9 failures		(9/100)(7/9)(2/9)= 0.016
4 (CD)	= 9/100 year	2/9 failures	n/a		(9/100)(2/9) = 0.02
5 (no LOMFW)	= 91/100 year				(91/100) = 0.91

Looking at the simulation data, the following can be extracted:

- The frequency of LOMFW leading to complete loss of decay heat removal (LOMFW + decay heat removal) given core damage is 0.036 per year (determined by adding 0.0 + 0.016 + 0.02).
- The frequency of no damage is 0.964 per year.

Table 2-3. Configuration results for the example given one pump train is unavailable.

Scenario (outcome)	LOMFW Term	MDP_START Term (CCF and independent)	MDP_RUN Term (CCF and independent)	MDP_RUN and MDP_START	Frequency (per year)
1 (OK)	= 11/100 year	8/11 successes	10/11 successes	10/11 successes	(11/100)(8/11)(10/11)(10/11) = 0.066
2 (CD)	= 11/100 year	8/11 successes	10/11 successes	1/11 failures	(11/100)(8/11)(10/11)(1/11) = 0.0066
3 (CD)	= 11/100 year	8/11 successes	1/11 failures		(11/100)(8/11)(1/11)= 0.0073
4 (CD)	= 11/100 year	3/11 failures	n/a		(11/100)(3/11) = 0.03
5 (no LOMFW)	= 89/100 year				(89/100) = 0.89

The results from simulation for this configuration are:

- The frequency of LOMFW leading to complete loss of decay heat removal (LOMFW + decay heat removal) given core damage is 0.044 per year (determined by adding 0.03 + 0.0073 + 0.0066).

- The frequency of no damage is 0.956 per year.

Based on this simple example, the change in core damage is 0.008/yr (calculated by taking 0.0439/yr - 0.036 /yr). This simple simulation just related the change in core damage frequency and did not evaluate the actual safety margin, since no reactor physics evaluations were performed. An output from the SAPHIRE risk monitor would look like Figure 2-13 given the example information was feed into the software. This output used the case study inputs and provided the output, which is the change in core damage frequency. This change is just the difference between the base core damage frequency subtracted from the configuration core damage frequency.

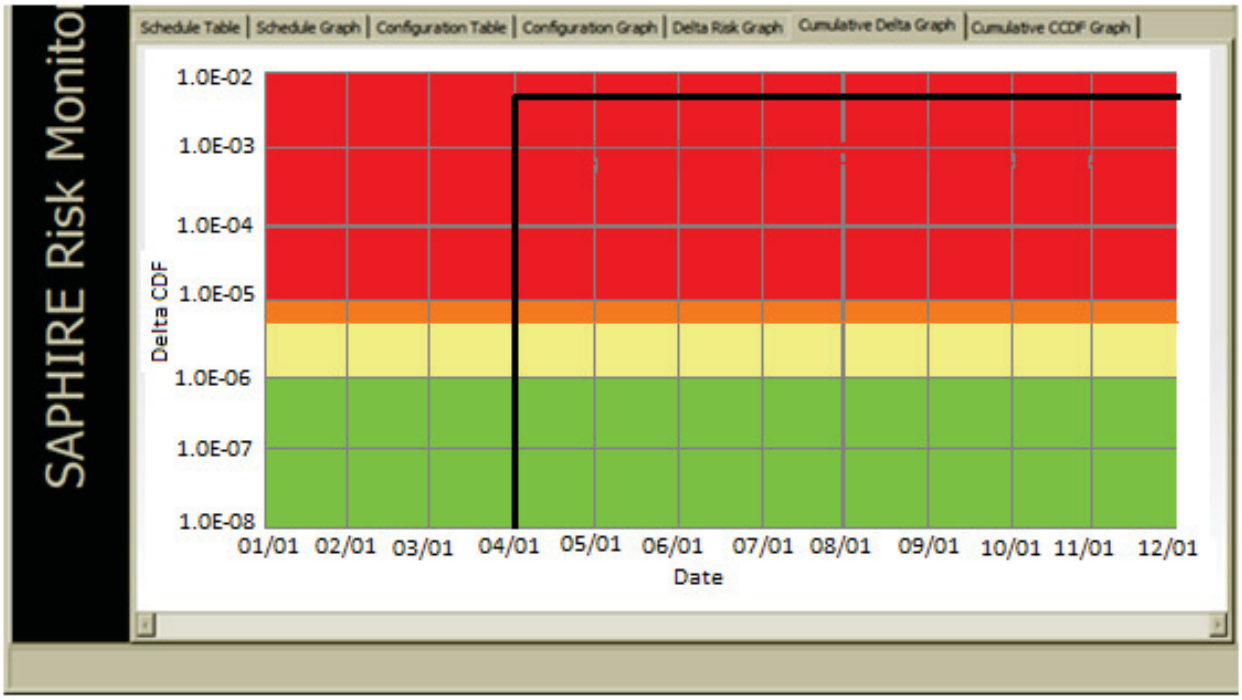

Figure 2-13. Example result of the configuration risk (showing delta CDF).

The same configuration evaluation was performed using the traditional PRA process shown in Section 2.1.2. The core damage frequency based on the configuration of pump train 2 being unavailable for 75 percent of the year is 0.048 per year. This gives a delta core damage frequency of 0.048/yr – 0.033/yr = 0.015/yr. This result is almost *double* that determined from the simulation.

In the next section, we will describe technical issues that need to be understood as part of the RISMC methodology. For example, we will show why the traditional approach is conservative (by almost a factor of 100%) over performing the same calculation using simulation.

3. TECHNICAL FEATURES AND ISSUES

The purpose of this section is to identify technical features and issues from using the RISMC process to evaluate configuration risk. The RISMC process uses some of the same models that have a strong influence on the traditional PRA process. These include common cause failure adjustments and human error adjustments. However, by directly coupling the plant physics with the probabilistic representation of the plant response and by simulating scenarios directly, some technical issues are not as problematic as with the traditional PRA.

3.1 Common Cause Failure

Common cause failure adjustment is an important issue when risk evaluations are performed. (Refer to Appendix B for a more detailed discussion on common cause failure assessment.) This adjustment needs to be considered whenever a component is unavailable to perform its intended function. Sometimes when evaluating different configurations, just the component is set to unavailable and the common cause failure event is left as is. But, in many cases, an adjustment needs to be performed on the common cause failure event in order to represent the conditional degradation. This adjustment depends on how the common cause failure probability is calculated and the type of configuration.

Most common cause models use the idea of parsing up the failure data into the different categories, i.e., independent or dependent failures, in order to capture the different ways a component could fail. The combined data that gets calculated is termed the total probability.

Nominally, the total probability (e.g., probability to start of 0.2) is used by the individual components as part of the simulation. This probability; however, includes both the independent failure probability and dependent failure probability. To illustrate, let us assume that the failure probability of the MDP failing to start has a total failure probability of 0.02. This failure probability can be separated into its independent part and its dependent part. Within common cause failure modeling, a conditional probability is a parametric way to account for dependent failures. To show how this dependent failure is captured in our model, a simple alpha-factor method will be used. The alpha-factor model splits the total probability up into the two parts as

$$Q_T = Q_I + Q_D = \alpha_1 Q_T + \alpha_2 Q_T$$

The total probability, Q_T, is the probability that is used in PRAs and simulation. Depending on the nature of the component that is removed either for maintenance activity or failed, the common cause failure probability will be adjusted in different ways. These two different ways a component can be unavailable to perform its intended function has a potential impact of the common cause failure probability adjustment. The following example will illustrate common cause failure adjustment for a two-train system given:

- One train removed for maintenance activities
- One train fails

3.1.1 CCF adjustment due to test and maintenance activity

For this configuration example, a two train system will be used and one of the components will be removed for testing or maintenance activities. The probabilistic modification is straight forward based on this configuration. The train that is unavailable is just removed from the logic model or simulation – thus the two train system becomes a single train system. However, the probability adjustment when common cause failure is modeled needs extra consideration. The adjustment to the common cause failure probability must account for the information available.

If a component is unavailable due to testing and maintenance activities is there still a potential common cause failure (on the remaining train). The assumption here that is advocated is that even though one of the components is removed for maintenance activities, there is still a potential shared-cause that may result in a failure. How this can be accounted for depends on how probabilities have been allocated in the risk model. If the probability assigned to a component is only its independent probability, Q_I, then the common cause portion of the probability needs to be left unchanged (so the two pieces will sum up to the total failure probability). However, if the allocated probability is the total failure probability, Q_T, then the common cause failure event is set to 0.0 since this part is already included in the total failure probability.

3.1.2 CCF adjustment due to failure

For this configuration example of a two train system, one of the components will be assumed failed. This type of adjustment is for the SDP process where a component is found to be inoperable. In this case, the train that has failed is removed from the logic structure or simulation and the two train system becomes a single train system. However, the probability adjustment when common cause failure is modeled needs to be adjusted.

If a component has failed, the failure mechanism needs to be determined. The determined failure can have an impact on the overall common cause failure probability adjustment. In general, two cases are considered, "independent" or "shared causes."

- If the failure was determined to be independent, i.e., no shared potential, then the common cause failure probability is set to 0.0. This implies that the failure mechanism that causes the component to fail does not have the potential to cause the other component to fail.

- If the failure was determined to be of a shared cause, then the common cause failure probability is adjusted to its *conditional* failure probability. In the case of a two-train system, the conditional failure probability is represented by the α_2 term. The α_2 term accounts for the conditional probability that if one component fails the other component is likely to fail at an increased failure probability.

During the RISMC simulation approach when we see a failure of a component, the new conditional common cause failure probabilities will be simulated to account for a specific plant configuration. For example, the working component is simulated and, if it fails independently, the system is failed since the second component is unavailable. If the working component does not fail independently, the simulation process will also use the conditional failure probability of both components due to common cause.

Recommendation #2

When performing failure analysis or configuration risk management, the common cause failure probability needs to be adjusted based on the configuration being evaluated using the applicable conditional failure probability.

3.2 Human Error Probability

Human errors can affect the overall result of sequence simulation. The affect can be positive, i.e., increase in safety margin, since the simulation process allows for the operator actions to be represented at the time required based on the operating procedures of the event in progress which may be expansive for a particular iteration. The human error probability associated with the operator action can vary depending upon time of required response and other key factors. The use of the SPAR-H PSFs can be fully utilized as part of RISMC simulation process. Note other PSF-based models may also be used as part of the simulation.

For example, if a mitigating system failed to start, then the time required for the operator to perform a required procedure would be immediate since the system did not operate at all. Now if the mitigating system started but failed at some later time prior to successful mission, the operator response will now be adjusted based on this time to respond and the decay heat level calculated using the T-H calculations that are being performed. The human error probability will be different based on these two different failures of the same mitigating system. This enhanced realism is a distinct advantage of the RISMC process over traditional PRA, since in traditional PRA there is no distinction between how the system failed either due to starting or running and at what time did it fail during operation.

The traditional PRA determines the human error probability based on procedures and assumed timing factors on when the procedures will be implemented in the sequence of interest. Therefore, this human error probability is a fixed probability and does not get re-evaluated depending upon the failure at the beginning (fails to start), early (fails within a couple hours of the event) or late (failed later into the sequence).

To help illustrate this potential change, the SPAR-H methodology has a quantification approach that accounts for variations in different PSFs. We will evaluate an example that will look at just the one PSF – timing of the operator to perform an activity. There are a total of six different timing levels that can be used to update the nominal human error probability. The different timing levels and their multiplier (PSF) are:

- inadequate time (probability of 1.0)
- barely adequate time (x10.0)
- nominal time (x1.0)
- extra time (x0.1)

- expansive time (x0.01)
- insufficient information (x1.0)

Depending upon the timing level, the multiplier is used to adjust the nominal probability.

For the example, let us assume the nominal probability that is used in a traditional PRA is 1.0E-03 based on understanding of procedures and the average timing that is governing a sequence of interest. Under the RISMC simulation process, the mitigating system of interest may fail at the beginning of it being initiated (failed during starting). The operator action should be re-evaluated based on this new set of information since the *actual* time is different than the *average* time for this activity. The human error probability should now be adjusted upwards (increased) due to the failure of the mitigating system early and less time is available for the operator to perform the necessary steps. The same philosophy can be used but in an opposite direction when the mitigating system failed while in operation at a later time in the scenario. This failure at a later time in the sequence may impact the heat level to be removed from the reactor (since decay heat is a function of time) and allow for additional time for the operator to perform the necessary steps in the procedure. Therefore, under this condition the human error probability would be lowered.

The RISMC simulation process provides a real time capability in allowing for the calculation of the human error probabilities. By simulating the timing of each sequence and the timing of component failure, allows for human error probability adjustments. A nominal probability is used to start the simulation, but depending upon time of failure and decay heat level, this probability can be adjusted and have an impact on the final safety margin.

Recommendation #3

When using the RISMC simulation-based approach for scenario generation, the human error probabilities related to operator actions should be evaluated in the context of scenario-specific performance shaping factors instead of assumed conditions.

3.3 Plant Reactor Physics

The RISMC process allows for the coupling of the reactor physics (e.g., T-H) to the configuration of the plant. This direct coupling allows for timing of plant response and operator response to be calculated based on this information. The RELAP series of T-H system codes may be used to calculate the key plant variables. These plant variables (i.e., temperature, pressure, flow rate) can have a direct link to important safety equipment. The direct link of the plant physics to mitigating systems can be evaluated or assessed from the standpoint of traditional PRA assumptions or degradation and aging affects.

A traditional PRA evaluation looks at the mitigating systems required to perform their intended function based on the scenario of interest. The mitigating system is quantified to see if it failed to start or failed during operation. Failure of the components within the mitigating system in the traditional PRA approach is based on the applicable failure probability or rate.

In a simulation, we can represent failures both by the probabilistic behavior and the performance behavior. For example, assume a mitigating system contains two pump trains that can provide 150 gpm of flow each and one of the two pumps is required to provide sufficient flow given a transient event. The RISMC process could simulate the failure probability of the pump trains and, if a failure occurred, it is assumed the pump could no longer provide sufficient flow. Alternatively, the failure could be simulated by representing degradations in the flow rate, where the flow rate may go to zero flow in the case of a complete failure. Once both pumps have failed, a new mechanistic calculation will be performed to determine the status of the plant and if damage had occurred.

A degraded flow rate of the pump needs to be simulated to see if it is providing some flow (less than what is required for success) or completely failed. If some flow is being provided, i.e., a degraded condition, this flow rate can be used in the RELAP calculations. In probabilistic space, both (or all) trains within a system could be deemed failed because the individual flow rates are below the required PRA flow rate for success. This combination in traditional PRA space would have the system failed; however, this degraded condition of both pumps may still meet the minimum required flow for success.

By accounting for degradation of components (e.g., flow rates) and aging affects (e.g., increase in failure rate or decrease in flow rates over time), a better representation of when damage does occur can be realized.

Recommendation #4

When using the RISMC simulation-based approach for calculating plant physics, accounting for degraded conditions and aging affects can have an impact on when damage occurs. Degraded conditions and aging effects of mitigating systems should have a direct link to plant physics calculations.

3.4 Delta Risk Calculations

The RISMC simulation process will calculate a safety margin and risk metric (core or fuel damage frequency) based on the configuration of interest. These calculated risk metrics can be used directly (as an absolute measure) or they need to consider changes (i.e., increases) relative to the nominal risk levels. Each of these methods will be discussed.

The first calculation type is related to the example performed in Section 2.1. This calculation took a delta change in core damage frequency. The delta type of calculation needs to be performed whenever a SDP assessment is required. The reason a delta calculation is performed stems from the NRC regulations where, as part of the SDP, the NRC is tasked to evaluate just the degradation that is experienced by the plant. The NRC recognizes that the configuration of interest (condition of plant) could have occurred while other routine testing or maintenance activities were being performed. The SDP evaluation is, however, only concerned about the degraded condition. Therefore, this type of evaluation will look at the plant risk to determine when core damage occurs conditioned on the degraded condition. This result is one part of the calculation. The other part of the calculation is the simulation of the plant under nominal conditions. Then, the nominal result will be subtracted from the degraded condition to provide a delta

change (or risk increase) in core damage frequency. This change in risk will be compared to the risk thresholds listed in Section 1.2.

The second calculation of concern will be to evaluate the plant configuration of interest during testing or maintenance activities to determine the safety margin and core damage frequency. The configuration of interest is based on potential plant configurations given certain testing and maintenance activities that are planned to be performed. This calculation should not worry about the *change* in risk since the evaluation is determining what the safety margin is given that condition. This type of evaluation should just use the absolute risk result that is determined from the analysis.

In the RISMC simulation approach, the plant conditions represents actual (based on plant physics being calculated) plant parameters and what is the safety margin. By only simulating the plant systems that play a role in the increase in risk, the calculation time will decrease.

Recommendation #5

When using the RISMC simulation-based approach for calculating safety margin and core damage frequency, two different results can be evaluated, an absolute and a change in safety margins. If the evaluation is for SDP, then the process must evaluate the degraded condition and compare this to the nominal plant condition. If the evaluation is for configuration risk management, then the absolute safety margin should be used to determine if the planned activity should proceed.

3.5 Convolution Factors

If we revisit the simulation example, we had two components with exponentially distributed failure times with a failure rate of 0.01/hr. These two MDPs (train A and train B) were working in parallel with one required for success, as shown in Figure 3-1. With the assumptions that the standby component cannot fail while in standby and that the failure times of the two components are independent, we can determine the failure distribution of the system.

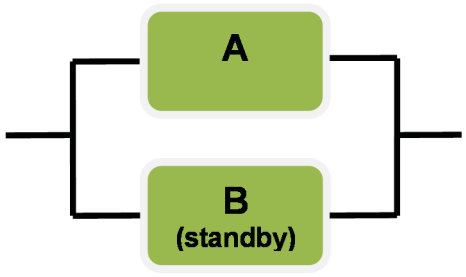

Figure 3-1. Two component parallel system with one required for success.

From a reliability point of view, component A operates for a random time period T_1, after which component B takes over (in a "switched" manner) for a random time period T_2. The operational time of

the MDP system is $T = T_1 + T_2$. In order to quantify an accident scenario, we want the probability that the system does not function, or when T ≤ t, where t will be the mission time of the system. Note that this probability is equivalent to the system unreliability.

Since T_1 and T_2 are exponential random variables, for *i*=1, 2, the density function for each individual failure time is given by

$$f_i(t_i) = \lambda_i \exp(-\lambda_i t_i) \quad , t_i \geq 0$$
$$f_i(t_i) = 0 \quad , t_i < 0$$

The time-dependence in this example comes from the fact that we do not know when component A will fail, which implies that we do not know how long component B will need to operate. Another way to look at this is that the "mission time" for component B is a random variable. Note that the simulation based approach provides an exact result for this calculation, but as we saw earlier, the traditional PRA result was too large. We can evaluate this problem by noting:

1. The system is represented by an AND gate (both components have to fail).
2. The components fail independently
3. The standby failure rate is zero
4. The probability of the fail to switch to component B is zero

The density function for T is given by the **convolution** of T_1 and T_2:

$$f(t) = \int_0^t f_1(t-y) f_2(y) dy = \int_{0`}^t f_1(y) f_2(t-y) dy$$
$$= \int_0^t \lambda_1 \exp[-\lambda_1 (t-y)] \lambda_2 \exp(-\lambda_2 y) dy$$
$$= \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1} [\exp(-\lambda_1 t) - \exp(-\lambda_2 t)]$$

The cumulative distribution is the integral of this equation:

$$F(t) = 1 - \frac{\lambda_2 \exp[-\lambda_1 t] - \lambda_1 \exp[-\lambda_2 t]}{\lambda_2 - \lambda_1}$$

For the special case where $\lambda_1 = \lambda_2 = \lambda$, the pdf is:

$$f(t) = \int_0^t \lambda^2 \exp(-\lambda y) dy = \lambda^2 t \exp(-\lambda t)$$

The cumulative distribution becomes what amounts to the Poisson probability of at least two failures during the interval (0, t):

$$F(t) = 1 - \exp(-\lambda t) - \lambda t \exp(-\lambda t)$$

In the traditional PRA case, we approximate failure probability as:

$$F_{approx}(t) = [1 - \exp(-\lambda t)][1 - \exp(-\lambda t)]$$

To illustrate the numerical difference between the exact and approximate results, let us return to our example using the MDPs. In that example, the failure rate has a value of 0.01/hr and the mission time (t) is 24 hours. We then calculate the exact results (i.e., what is produced via simulation) and approximate results for this example:

Exact result = 0.025

Approximate result = 0.046

In this case the approximate calculation that is used in traditional PRA is too large by a factor of almost two. Note that some traditional PRAs append a convolution-based "factor" (which would be the ratio of the exact to approximate results, or 0.54 in this example) to the specific minimal cut sets containing the failure combination described above. However this adjustment factor – while making a correction in the probability – causes other technical quantification issues such as impacts to importance measures (e.g., does the factor apply to MDP A, MDP B, or both?) and uncertainty analysis.

The result that was obtained in the example for the change in risk (i.e., delta core damage frequency) using the traditional PRA approach was found to be 0.015/yr. Multiplying this value by the adjustment factor (0.015 * 0.54) gives the result of 0.008/yr – this is the answer that was obtained directly by the RISMC simulation approach.

Recommendation #6

If traditional PRA methods are used to produce the configuration risk management probabilistic analysis, convolution-based factors should be applied to time-dependent failure combinations in order to approximate an exact result. Preferentially, the RISMC simulation-based approach to scenario generation should be used since it automatically addresses the time dependence between components and alleviates the need for adjustment factors.

3.6 Success States

In traditional PRAs, it is sometimes necessary to consider scenarios events that represent successes in addition to failures. When these PRAs are used (containing success events) then it is considered as a "non-coherent" failure model. Further, quantification of either coherent or non-coherent results typically employ approximations such as the minimal cut set upper-bound. However, these quantification approximations can be very inaccurate. Consequently, different approaches to efficiently and accurately solve non-coherent logic models have been studied.

Currently, non-coherent logic is encountered in practical applications such as the generation and quantification of scenarios. Cases where a system or component is failed or unavailable, such as in configuration risk management, typically cause failure probabilities of associated systems to increase,

thereby acerbating the use of quantification approximations (many of which rely on low failure probabilities to be accurate).

The primary area where success events are found in static logic models is through event tree accident sequences, with lesser use of complemented events and/or gates in fault trees. In traditional PRA, accident sequences are defined a priori by developing event trees, where the sequence logic is the list of systems that succeed or fail during this accident sequence, hence the arrival of success terms (potentially). Note that in the simulation-based approach, the nature of failures and successes are treated directly (not a priori) as part of the simulation and are determined as the analysis evolves over time.

To evaluate the issue of success states, and their impact on traditional PRA versus simulation-based analysis, we will use a slightly more complex example than what was used in Section 2. For this example, we start with an event tree containing a single initiating event and two top events (for a total of four sequences) as shown in Figure 3-2.

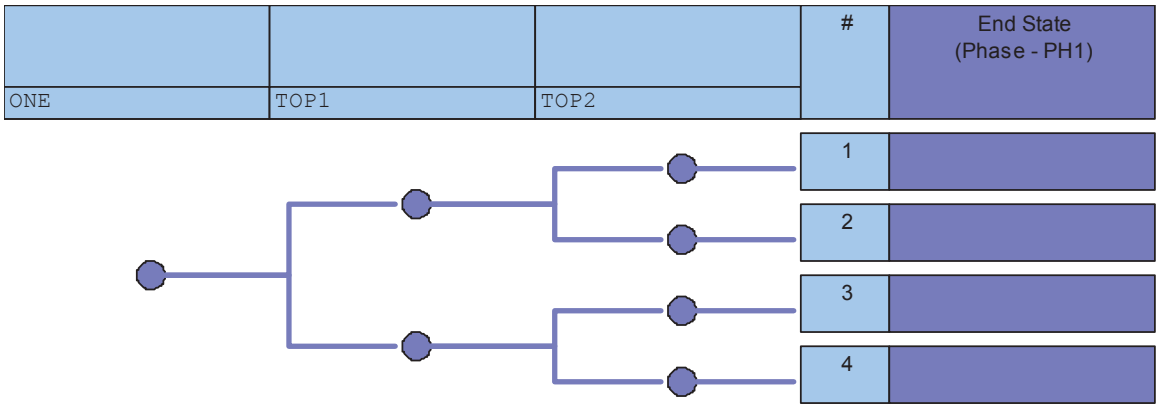

Figure 3-2. Event tree for example #3.

The two associated fault trees are shown below.

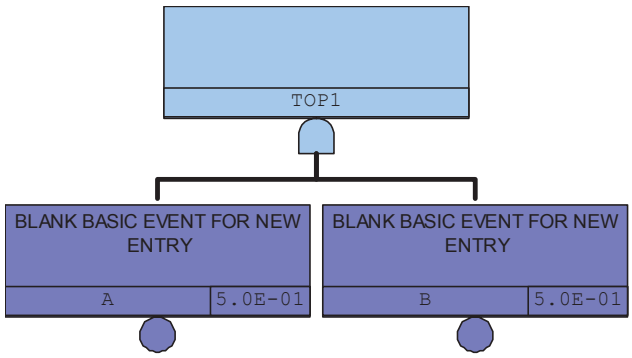

Figure 3-3. TOP 1 fault tree.

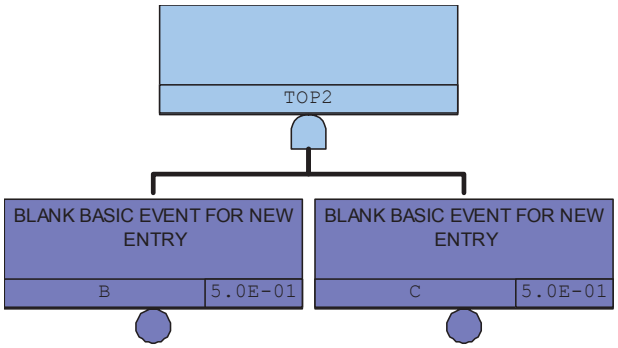

Figure 3-4. TOP 2 fault tree.

First, we will use the traditional PRA approach by solving the cut sets for "core damage" sequences. Let us assume that sequences 1 and 3 are OK, and 2 and 4 are core damage. Solving the sequences show the following results:

Table 3-1. Cut set generation results

Sequence	Cut Set(s)	Quantification
1 OK	<PASS>	1.000
2 CD	**B C**	**0.250**
3 OK	A B	0.250
4 CD	**A B C**	**0.125**

Adding sequence 2 to 4 gives a value of 0.375, which is too high since the exact value should be 0.125+0.125 = 0.250. The primary reason this analysis is too conservative is that the default analysis approach in most PRA codes ignores the probability contribution of the "/A" term in sequence 2.

Simulating both sequence 2 and 4 provides a numerical result of 0.25, which is the correct answer.

Recommendation #7

If traditional PRA methods are used to produce the configuration risk management probabilistic analysis, sequences that include success states or branches should be adjusted to account for success terms. Preferentially, the RISMC simulation-based approach to scenario quantification should be used since it automatically addresses success of components and systems.

4. CONCLUSIONS

The INL has carried out a demonstration of the RISMC approach for the purpose of configuration risk management. We have shown how improved accuracy and realism can be achieved by simulating changes in risk – as a function of different configurations – in order to determine safety margins as the plant is modified.

In order to carry out configuration risk management, a coupling of mechanistic and probabilistic calculations are performed. Within this process, several technical issues are encountered. We described the various technical issues that play a role in these configuration-based calculations with the intent that future applications can take advantage of the analysis benefits while avoiding some of the technical pitfalls that are found for these types of calculations. The technical areas that are addressed are:

- Common Cause Failure
- Human Error Probability
- Plant Reactor Physics
- Delta Risk Calculations
- Convolution Factors
- Success States

For each technical issue, specific recommendations have been provided with the intention of improving the safety margin analysis and strengthening the technical basis behind the analysis process. By following the overall RISMC approach described in this report *and* applying the recommendations made herein, a technically-sound safety margin characterization for configuration risk management can be realized.

5. REFERENCES

Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. (2005). *The SPAR-H Human Reliability Analysis Method.* NRC.

Idaho National Laboratory. (2011). *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8.* Rockville, MD: NRC.

Idaho National Laboratory. (n.d.). *The Advanced Test Reactor (ATR)*. Retrieved August 2012, from https://inlportal.inl.gov/portal/server.pt/gateway/PTARGS_0_1646_9670_0_0_18/atr.pdf

Mosleh, A., Rasmuson, D., & Marshall, F. (1998). *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.* NRC.

Rasmussen, J., Nixon, P., & Warner, F. (1990). Human Error and the Problem of Causality in Analysis of Accidents [and Discussion]. *Philosophical Transactions of the Royal Society Biological Sciences, 327*(1241), 449-462.

Reason, J. (1990). The Contribution of Latent Human Failures to the Breakdown of Complex Systems. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences, 327*(1241), 475-484.

RELAP5 Code Development Team. (2012). *RELAP5-3D Code Manual.* INL.

Smith, C., Rabiti, C., & Martineau, R. (2012). *Risk Informed Safety Margins Characterization (RISMC) Pathway Technical Program Plan.* Idaho National Laboratory.

APPENDIX A

A.1 Dynamic Simulation Model Generation from a Static PRA Model

A.1.1 Overview

The traditional method of risk assessment has been the development of static models of a system (i.e. nuclear power plant) based on initiating events, event trees, fault trees and basic event probabilities. Over the years vary sophisticated models have been created the help in understanding the risk of system failure. This method of analysis has worked well in quantifying risks using probabilistic derived data.

However, there are certain issues that static modeling do not adequately quantify. Some of these issues are how time of system component failures might affect risk. A dynamic simulation model of the system can take into account the timing of accident events.

Considering the completeness of current static PRA models including the probabilistic information that is contained, it is very advantageous to use these PRA models to auto-generate to the complexity of the system in a dynamic simulation model. This section describes a methodology to generate a dynamic model from the static PRA models of a traditional code such as SAPHIRE.

A.1.2 Dynamic Simulation Model

The dynamic simulation model is based on a modeling technology known as Discrete Event Simulation. This simulation model maintains a dynamic list of events in time that are processed during the course of the modeling. The timeline events are created from analysis of stochastic variables that describe possible events in terms of a probabilistic distribution.

The simulation model is based on several interconnected data objects. These data objects include:

- Simulation Object – A simulation object is a subsystem, component, action or entity that makes up the modeled system. These modeled objects can be interconnected through parameter or attribute values. They become the basis of the modeling effort as each are evaluated for changes in state.
- Simulation States – Each simulation object is further defined as to the possible states that the object can be in. These object states could be simple such as On, Off or Failed or might contain a complex series of states that might describe a decision path example.
- Simulation Events – Events define a transition from one object state to another. This event transition is defined using various types of probabilistic distributions, object parameter trigger points or dependencies on other events. It is these events that are evaluated along the simulation timeline.
- Simulation Outcomes – A simulation state might be associated with outcomes of interest in the system model. Certain outcomes might terminate the simulation. Recorded outcomes over several simulation runs become the basis of risk assessment and evaluation.

- Other Simulation Data Objects – There are several other data objects that define things like required resources, variates and equations that support the simulation process and provide a way to conduct "what-if" types of studies.

A.1.3 Static PRA Model

The static PRA models in SAPHIRE consist of initiating events, event trees, fault trees, end states and basic events. Initiating events define a transient producing event that might have a negative impact on the modeled system. These initiating events are given frequency of occurrence which in a risk sense is hopefully very small. Each initiating event is the first node of an event tree that defines the top level events as a success or failure of safety systems or actions that are in place to protect the modeled system from damage. Each top level event in the tree is evaluated using fault trees that use Boolean logic of associated basic events to define the success or failure of a system. The basic events are defined in terms of probabilistic equations. Every logical path through the event trees is assigned an end state which in many models is binary in nature expressing a success or failure of the modeled system.

In all cases risk is a mathematical calculation expressing the probability that a specific success or failure path can occur. Critical failure paths can then be determined. This modeling method is a static calculation where time is not considered except as evaluated over a total mission time. Thus events that might be defined as a mean time to failure for example are reduced to a probability that it might fail during the time of the mission. When it failed during the course of the transient is not necessarily considered.

A.1.4 Generation of a Dynamic Model from a Static PRA Model

Key to the success of using the dynamic modeling approach defined above will be the automatic generation of a dynamic model from the established and validated static models. The following concepts were discussed as a way to accomplish the model transition.

1. Initial events will be the basis of constructing a simulation. Initial considerations for the development and testing of this process will limit the simulation model to only one initial event but in general that limit could be removed during later development efforts. The initial event will also be the initial simulation event that will change its state at the start of the simulation.
2. The initial event defines an event tree and the event tree's top events will represent other simulation objects in the dynamic model. The initial state of each top event will be considered "Standard Operational State".
3. Simulation states will be defined for each simulation object defined from the event tree's top events will include a "Demand" state that indicates that a successful operation of the object is required to respond to the incident. The event that causes this transition will be dependent on the event logic path and transition states of those prior simulation objects.
4. The other simulation states for a top event object will be derived from a collapsed representation of the fault tree associated with the top event. Since the dynamic modeling is only different from

the static model in its way of handling basic events that include time in the evaluation of probability of occurrence, all other events will be collapsed into a single state and event for that transition.

5. All time dependent events will be retained as a state and transition event that will be placed as needed on the event timeline.
6. Boolean logic of the fault tree will be maintained in the generation of the collapsed tree as a representation of the simulation states for that top event or simulation object. See Figure 1 for a visual representation the collapsed tree concept.
7. Variates will be defined and linked with transition events where appropriate. Functions will also be derived from those already in the SAPHIRE model definition of combined events. By placing these as separate records and linking them to events, the model once established would be easier to change for different modeling efforts.
8. Sequence end states will be used to define the simulation outcomes that can be tracked and reported internally. These outcomes will be augmented with the path information that resulted in reaching that outcome. Because of the collapsed nature of the state diagrams, the path information will necessarily be a collapsed version of the sequences derived from the static model. Path statistics will also be available for reporting.

The handling of house events from the PRA still needs to be evaluated and defined in the context of a dynamic modeling effort. The Figure A-1 illustrate the model transition described above.

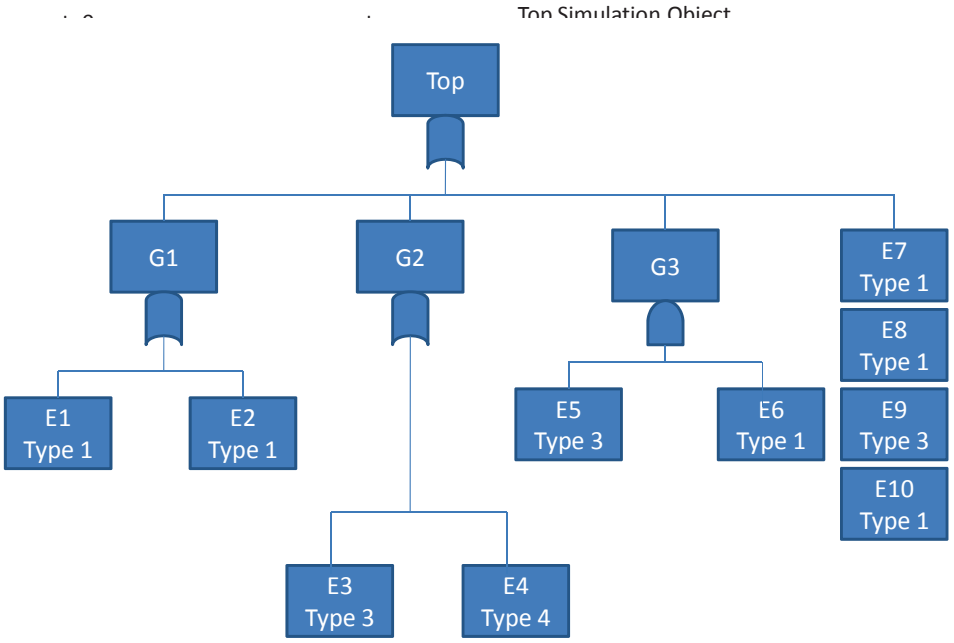

Figure A-1. The types of transitions from the DEMO project.

In terms of the event tree that this example might be representing, the transitions to success states and/or failure states might be external events that move other systems into a "Demand" state. The actual failure state might be a negative outcome only if it is a state that leads to an end state in the event tree of the static model. If the time of transition is beyond the time of simulation defined then the simulation will not record this as a transition because it is outside the time range of interest.

A.2.1 Simulation Analysis Example

In this example, we will compare a cut set based method to the simulation method. This comparative analysis uses a demonstration model created in SAPHIRE called the DEMO project. The DEMO project includes one initiating event (LOSP) defined with a frequency of 2.3 per year. The associated event tree (see Figure A-2) resolves to three possible end states (OK, SMALL-RELEASE and LARGE-RELEASE). The event tree has two top events (ESC and CCS) that success or failure is determined using a corresponding fault tree. The fault trees are comprised of several logic gates and events.

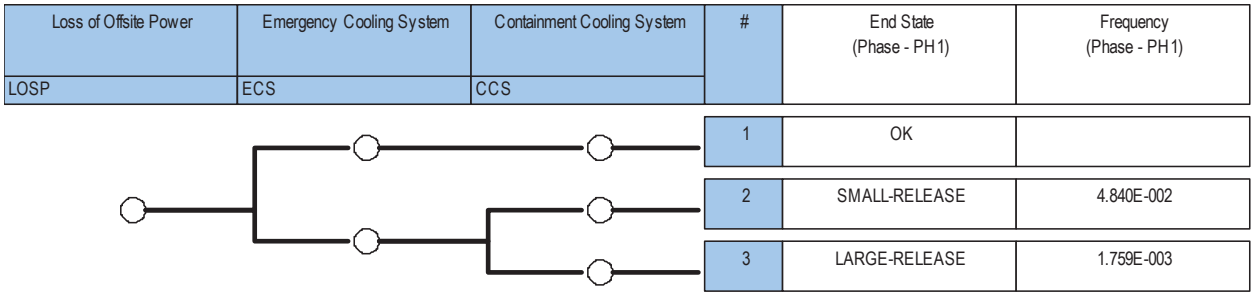

Figure A-2. The LOSP event tree from the DEMO project.

The simulation model was created from the SAPHIRE DEMO project. The simulation uses an event-based model that has simulation objects from the top events of the LOSP event tree above. The event-based model is shown in Figure A-3. The **IE Generator** object simulates the initiating event (just LOSP in this case) needed to evaluate the model. Specifically, what this node does is represent the occurrence (in time) of the next LOSP event randomly.

Each node from the SAPHIRE event tree becomes a state in the simulation model with the associated fault tree becoming a series of "complex" and "basic" events in the simulation model (see Figure A-4 and Figure A-5). We use a random number generation method to simulate complex-events to determine the next simulation state.

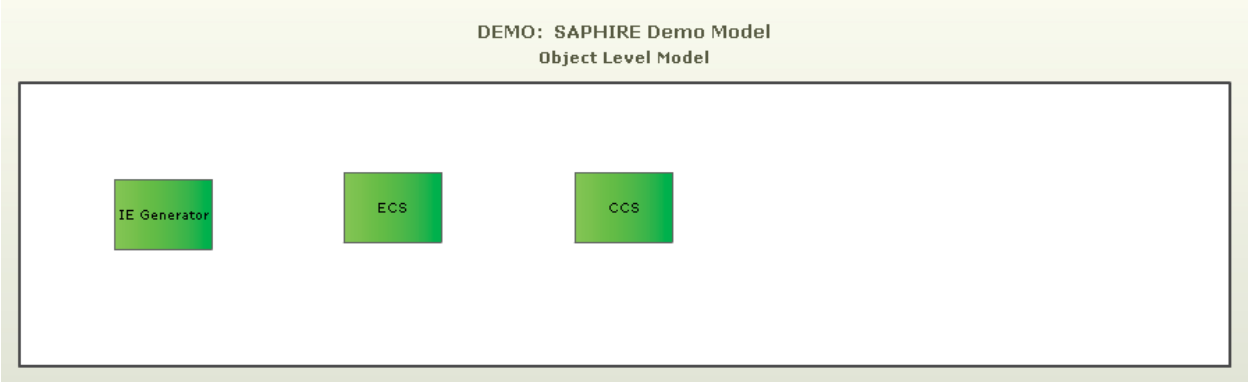

Figure A-3. Simulation model objects as seen in the browser window.

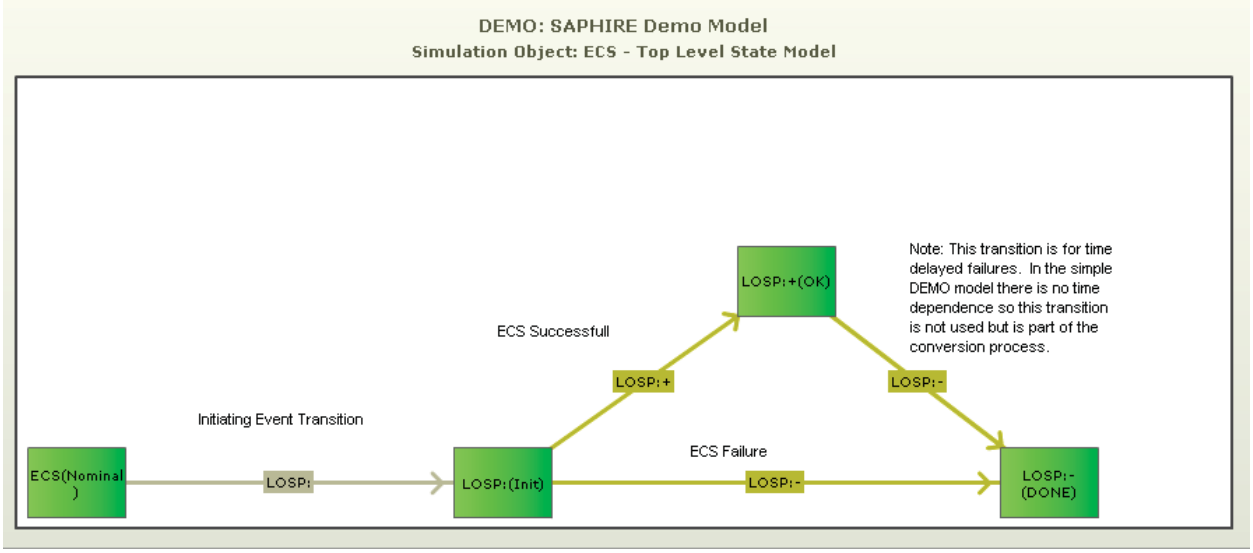

Figure A-4. The simulation state and transition model for ECS.

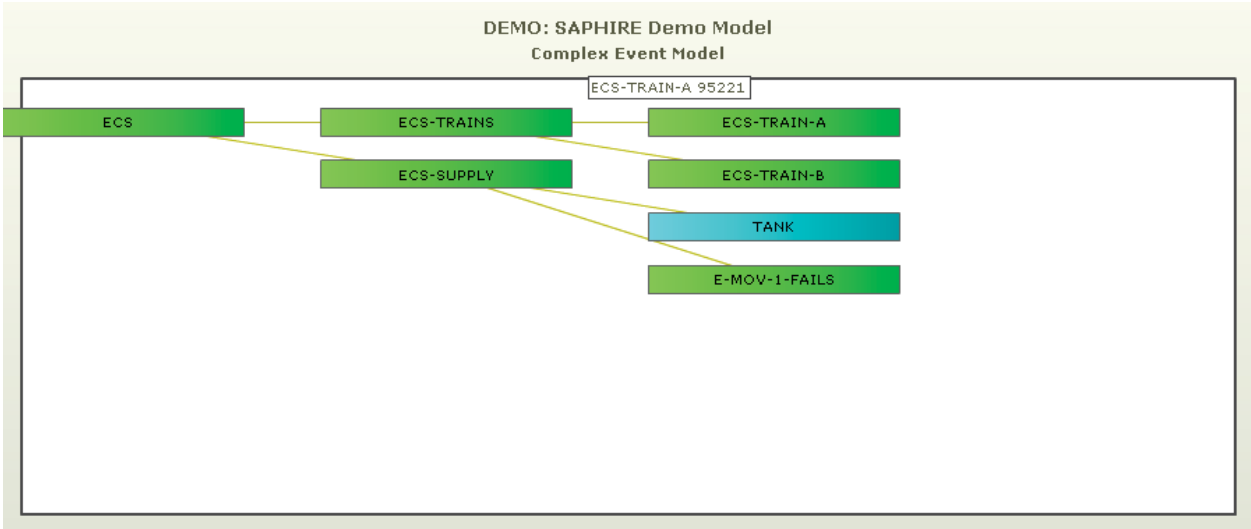

Figure A-5. The simulation complex-event model for ECS down to the basic event level (partial view).

The analysis shown in this section will compare the SAPHIRE calculated frequency values of the possible end states to the frequency of the three possible simulation sequences observed from a large number of simulation iterations of the simulation model.

A.2.2 Simulation Analysis Results

The SAPHIRE results are shown in Figure A- as being 4.84E-2 for a SMALL-RELEASE and 1.759E-3 for a LARGE-RELEASE. This frequency includes the initiating event frequency which is 2.3 per year.

Simulation analysis shown in Table A-1 (for SMALL-RELEASE) and Table A-2 (for LARGE-RELEASE) were calculated conditional upon seeing a LOSP. To compare the simulation results to the SAPHIRE calculation, we need to multiply the conditional simulation results by the LOSP frequency. This comparison is shown in Table A-3. While the use of simulation to determine failure frequency will vary due to Monte Carlo issues, the overall results match fairly well the result calculated by SAPHIRE.

Table A-1. Simulation analysis results (for the SMALL_RELEASE end state).

	Number of Simulation Iterations	**SMALL-RELEASE Sequence Count**	**SMALL-RELEASE probability given LOSP**
Test Run 1	384,516	7,895	2.053E-2
Test Run 2	1,157,603	23,612	2.040E-2
Summation	1,542,119	31,507	2.043E-2

Table A-2. Simulation analysis results (for the SMALL_RELEASE end state).

	Number of Iterations	**LARGE-RELEASE Sequence Count**	**LARGE-RELEASE probability given LOSP**
Test Run 1	384,516	277	7.204E-4
Test Run 2	1,157,603	892	7.771E-4
Summation	1,542,119	1169	7.580E-4

Table A-3. Simulation analysis results and comparison with SAPHIRE.

	SMALL-RELEASE	**LARGE-RELEASE**
Simulation	4.70E-2/year	1.74E-3/year
SAPHIRE	4.84E-2/year	1.76E-3/year

Appendix B

B.1 Simulation CCF Adjustments Following a Component Failure

One of the technical issues that needed to be considered during a scenario simulation is for the case where one component in a group of redundant components fails. If failures in the group were statistically independent, then we could simply simulate the other components failures in a straight-forward fashion. However, we know from risk assessment practices that dependent failures are possible and results in common-cause failure (CCF) modeling. Consequently, when a component fails in a group of redundant components, we need to determine the conditional failure of the remaining components – this section describes the approach to calculate the conditional failure probability to be used in the simulation approach.

Assume the failure combinations for a two train system (labeled A for train A and B for train B) with two failure modes (S = started; R = run) are:

$$S = \left\{A_I^R\ B_I^R,\ A_I^S\ B_I^S,\ A_I^R\ B_I^S,\ A_I^S\ B_I^R,\ C_{AB}^R, C_{AB}^S\right\}$$

A simulation model would need to consider all of these potential failure combinations. Note that the definition of "A total" represents the failure probability (from any cause) of train A and is given by:

$$A_t^S = A_I^S \cup C_{AB}^S$$

where "C" represents a CCF type of failure and the A_I represents individual (not dependent) failures. Consequently, the term C_{AB} represents a CCF of both train A and train B.

Now, when we run a simulation, we may see the failure of a component, say for example, train A. Specifically, assume that we see a failure to start of train A – this implies that we need to condition on "A total" (or the failure of train A). Using the definition of a conditional probability, we see that the conditional probability of failure for the second train (train B) given failure of the first is:

$$Pr(S|A_t^S) = \frac{Pr(S \cap A_t^S)}{P_r(A_t^S)}$$

where, for a two-train system with two failure modes $S \cap A_t^S = \left\{A_I^S\ B_I^S,\ A_I^S\ B_I^R,\ C_{AB}^S\right\}$

$$\therefore\ Pr(S\big|A_t^S) = \frac{Q_1^{(S)^2}}{Q_t^S} + \frac{Q_1^S Q_1^R}{Q_t^S} + \frac{Q_2^S}{Q_t^S}$$
$$= \propto_1^S Q_1^S + \propto_1^S Q_1^R + \propto_2^S \approx\ Q_1^S + Q_1^R + \propto_2^S$$

where we have defined the failure probabilities (Q) in terms of the Basic Parameter Model typically used to quantify CCF models and are using the alpha factor model as defined in (Mosleh, Rasmuson, & Marshall, 1998). As can be seen in the results above, the conditional failure probability of the second train is approximately equal to $\propto_2$ since this term is generally much larger than either of the "Q" terms.

Thus, when simulating failures, the correct conditional term (above) should be used rather than assuming components failure independently.

B.2 Calculation for the Two-train Example

In the previous section, we defined a conditional probability:

$$P(X|Y) = \frac{P(Y \cap X)}{P(Y)}$$

where the symbols X and Y represent any "event." For example, event X could represent EDG_A failing and Y represents EDG_B has failed. To illustrate the types of calculations we are performing for the system simulation, we will focus on the possible states a two train EDG system (Trains A and B), as shown in Figure B-1.

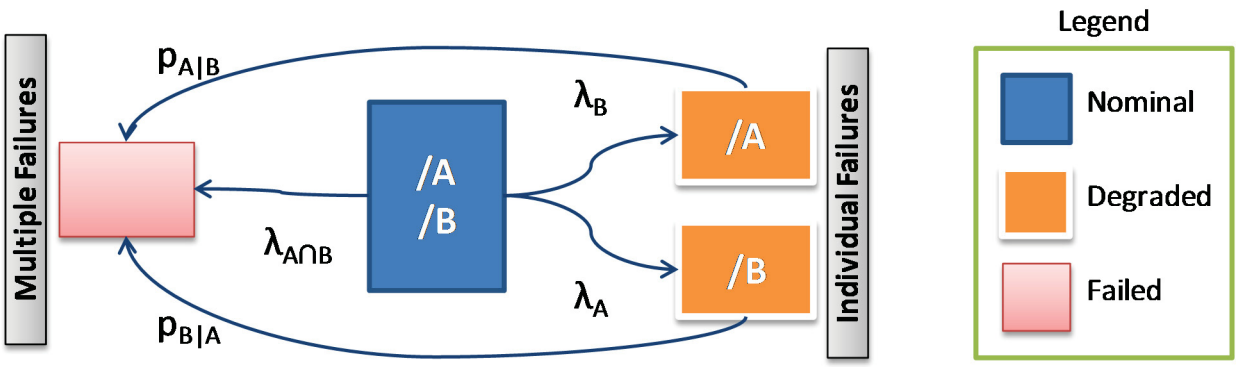

Figure B-1. Illustration of the success, degraded, and failure states of a two-train system.

To evaluate the model above, we need to know the EDG failure rates λ_A, λ_B, and $\lambda_{A\cap B}$ and the conditional probabilities $p_{A|B}$ and $p_{B|A}$. Note that this model assumes that repair is not possible (at least in a short time, say 24 hours).

We can determine the rates using the **non-staggered** alpha-factor model:

$\lambda_A = \lambda_B = \lambda_1 = (\alpha_1 \lambda_{total}) / \alpha_t = (\alpha_1 \lambda_{total}) / (\alpha_1+2\alpha_2)$

Assuming the following values for α are applicable:

$\alpha_1 = 0.9$ $\alpha_2 = 0.1$

and the EDG total failure rate is:

λ_{total} = 6E-5/hr

we can find that $\lambda_A = \lambda_B = \lambda_1$ = 4.9E-5/hr. This is the failure rate of an **individual** train. We now know that the dependent failure rate is:

$\lambda_{A\cap B} = \lambda_2 = (2\alpha_2\,\lambda_{total}) / (\alpha_1+2\alpha_2) = 1.1E\text{-}5/hr$

Next, we need to determine the conditional probabilities. Using $P_{system} = p_{A|B} * p_B$ and the definition of conditional probabilities to find:

$$p_{system|B} = p(p_B \cap p_{system})/p_B$$

The term p_B can be written as two probabilities, an individual failure probability and a dependent failure probability, or (in terms of the **non-staggered** alpha-factor model):

$$p_B = p_{ind} + p_{ccf} = Q_1 + Q_2 = [1-\exp(-(\alpha_1/(\alpha_1+2\alpha_2)) *\lambda_{total}\, t)] + [1-\exp(-(2\alpha_2/(\alpha_1+2\alpha_2))* \lambda_{total}\, t)]$$

The conditional probability is then:

$$p_{system|B} = (\{[1-\exp(-(\alpha_1/(\alpha_1+2\alpha_2)) *\lambda_{total}\, t)] + [1-\exp(-(2\alpha_2/(\alpha_1+2\alpha_2))* \lambda_{total}\, t)]\} \cap p_{system})/p_B$$

Since $p_{system} = Q_1^2 + Q_2 = ([1-\exp(-(\alpha_1/(\alpha_1+2\alpha_2)) *\lambda_{total}\, t)])^2 + [1-\exp(-(2\alpha_2/(\alpha_1+2\alpha_2))* \lambda_{total}\, t)]$, we can show (after some algebra):

$$p_{system|B} = (\alpha_1/\alpha_t)^2[1-\exp(-\lambda_{total}\, t)] + 2\alpha_2/\alpha_t$$

Thus, $p_{A|B} = p_{B|A} = 0.18$ (when the mission time t = 24 hours)

Now that we have all of the applicable terms, we can quantify the model described in Figure.

The ways for the system to fail are:

1. EDG A fails (with rate λ_A) then EDG B fails (with conditional probability $p_{B|A}$)
2. EDG B fails (with rate λ_B) then EDG A fails (with conditional probability $p_{A|B}$)
3. Both EDGs fail (with rate $\lambda_{A\cap B}$)

In words, the three scenarios represent (in order):

- Train A fails with rate λ_A then Train B fails with conditional probability (in 24 hours) of $p_{B|A}$
- Train B fails with rate λ_B then Train A fails with conditional probability (in 24 hours) of $p_{A|B}$
- Both trains fail with a dependent rate $\lambda_{A\cap B}$

We describe these three scenarios in terms of two parts, an initiating event part (any term with a "λ") and a mitigating part (any term with a "p"). Quantifying these yields:

Cut Set	Terms	Value
1	4.9E-5/hr * 0.18	8.8E-06/hr
2	4.9E-5/hr * 0.18	8.8E-06/hr
3	1.1E-5/hr	1.1E-05/hr
Total		2.9E-05/hr

Now, during the simulation, we may see a failure, for example EDG B might fail. This implies we have changed our system boundary conditions to represent the failure of train B – the model changes to that shown in Figure B-2. The rate of failure for this system is now

$\lambda_A + \lambda_{A \cap B} = 4.9E\text{-}5/hr + 1.1E\text{-}5/hr = 6.0E\text{-}5/hr$.

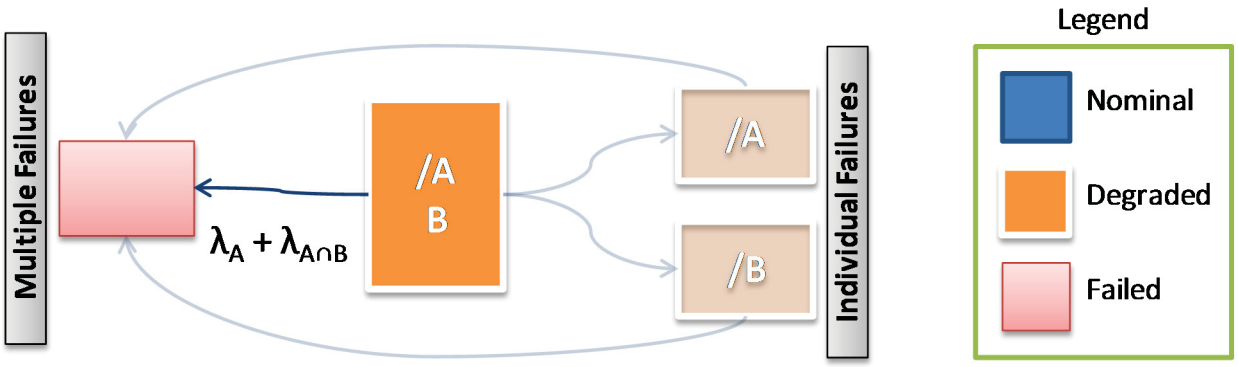

Figure B-2. Illustration of the degraded and failure states of a two-train system when EDG B is failed.