INL/EXT-12-27015
Revision 0

Light Water Reactor Sustainability Program

Risk Informed Safety Margin Characterization (RISMC) Advanced Test Reactor Demonstration Case Study

August 2012

DOE Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, do not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXT-12-27015
Revision 0

Light Water Reactor Sustainability Program

Risk Informed Safety Margin Characterization (RISMC) Advanced Test Reactor Demonstration Case Study

Curtis Smith
David Schwieder
Cherie Phelan
Anh Bui
Paul Bayless

August 2012

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

EXECUTIVE SUMMARY

Safety is central to the design, licensing, operation, and economics of Nuclear Power Plants (NPPs). Consequently, the ability to better characterize and quantify safety margin holds the key to improved decision making about light water reactor design, operation, and plant life extension. A systematic approach to characterization of safety margins and the subsequent margins management options represents a vital input to the licensee and regulatory analysis and decision making that will be involved.

The purpose of the Risk Informed Safety Margin Characterization (RISMC) Pathway research and development (R&D) is to support plant decisions for risk-informed margins management with the aim to improve economics, reliability, and sustain safety of current NPPs. Goals of the RISMC Pathway are twofold: (1) Develop and demonstrate a risk-assessment method coupled to safety margin quantification that can be used by NPP decision makers as part of their margin recovery strategies. (2) Create an advanced "RISMC toolkit" that enables more accurate representation of NPP safety margin.

In order to carry out the R&D needed for the Pathway, the Idaho National Laboratory is performing a series of case studies that will explore methods- and tools-development issues. One of the initial case studies that has been proposed is to demonstrate the RISMC approach using the Advanced Test Reactor (ATR) as a test. This report describes the RISMC methodology demonstration for the ATR. As part of the demonstration, we describe how both the thermal-hydraulics and probabilistic safety calculations are integrated and used to quantify margin management strategies.

Completing the ATR case study has pointed to several additional areas of promising R&D related to risk-informed margin management. First, the current NRC Significance Determination Process is focused on core damage frequency, but we showed how the concept of safety margin provided additional information, both from a quantitative aspect but more importantly from an engineering physics understanding. Further, additional applications seem to be possible including NPP risk monitor enhancements; a general decision support capability for operational decisions; and an integrated and holistic framework to account for aging effects during the NPP lifetime.

Several successful outcomes have resulted from performing the ATR case study, including the development of an improved plant physics approach and an enhanced risk-analysis capability featuring a unique suite of simulation methods that builds upon traditional PRA approaches. The approach and lessons learned from this case study will be included in future Technical Basis Guides produced by the RISMC Pathway. These guides will be the mechanism for developing the specifications for RISMC tools and for defining how plant decision makers should propose and evaluate margin recovery strategies.

CONTENTS

FIGURES

TABLES

ACRONYMS

CDF	core damage frequency
DOE	Department of Energy
EDG	emergency diesel generator
INL	Idaho National Laboratory
LCP	loss of commercial power
LOOP	loss of offsite power
LOP	loss of power
LWR	light water reactor
LWRS	light water reactor sustainability
MOOSE	Multiphysics Object-Oriented Simulation Environment
NPP	nuclear power plant
PRA	probabilistic risk assessment
R&D	research and development
RISMC	Risk Informed Safety Margin Characterization
SSC	system, structure, and component
T-H	thermal-hydraulics

Risk Informed Safety Margin Characterization (RISMC) Advanced Test Reactor Demonstration Case Study

1. BACKGROUND

1.1 RISMC Pathway Background

Safety is central to the design, licensing, operation, and economics of nuclear power plants (NPPs). As the current light water reactor (LWR) NPPs age beyond 60 years, there are possibilities for increased frequency of systems, structures, and components (SSC) degradations or failures that initiate safety-significant events, reduce existing accident mitigation capabilities, or create new failure modes. Plant designers commonly "over-design" portions of NPPs and provide robustness in the form of redundant and diverse engineered safety features to ensure that, even in the case of well-beyond design basis scenarios, public health and safety will be protected with a very high degree of assurance. This form of defense-in-depth is a reasoned response to uncertainties and is often referred to generically as "safety margin." Historically, specific safety margin provisions have been formulated primarily based on engineering judgment backed by a set of conservative engineering calculations.

The ability to better characterize and quantify safety margin holds the key to improved decision making about LWR design, operation, and plant life extension. In a sense, contemplation of LWR operation beyond 60 years does represent a kind of "beyond design basis" operation. A systematic approach to characterization of safety margin and the subsequent margin management options represents a vital input to the licensee and regulatory analysis and decision making that will be involved. In addition, as research and development (R&D) in the LWR Sustainability (LWRS) Program and other collaborative efforts yield new data, sensors, and improved scientific understanding of physical processes that govern the aging and degradation of plant SSCs (and concurrently support technological advances in nuclear reactor fuels and plant instrumentation and control systems) needs and opportunities to better optimize plant safety and performance will become known. This interaction of degradation understanding and potential impacts to plant margins is shown in Figure 1-1. To support decision making related to economics, readability, and safety, the RISMC Pathway provides methods and tools that enable mitigation options known as margins management strategies.

The purpose of the RISMC Pathway R&D is to support plant decisions for risk-informed margin management with the aim to improve economics, reliability, and sustain safety of current NPPs. As the lead Department of Energy (DOE) Laboratory for this Pathway, the Idaho National Laboratory (INL) is tasked with developing and deploying methods and tools that support the quantification and management of safety margin and uncertainty.

Goals of the RISMC Pathway are twofold:

1. Develop and demonstrate a risk-assessment method coupled to safety margin quantification that can be used by NPP decision makers as part of their margin recovery strategies.

2. Create an advanced "RISMC toolkit" that enables more accurate representation of NPP safety margin.

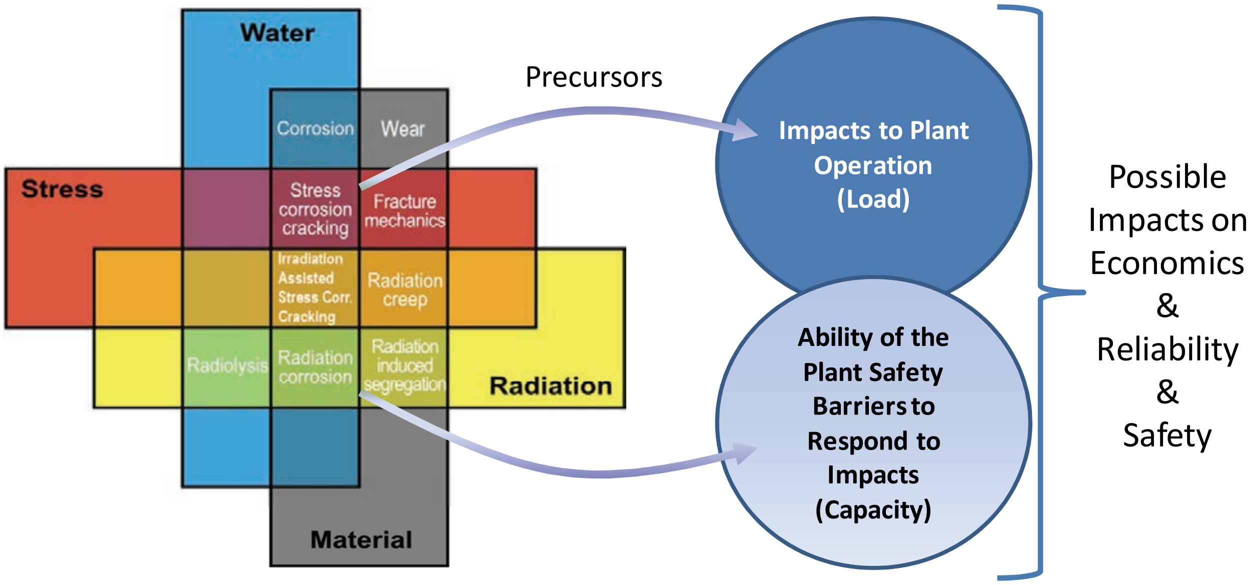

Water
Corrosion
Wear
Stress
Stress corrosion cracking
Fracture mechanics
Irradiation Assisted Stress Corr. Cracking
Radiation creep
Radiolysis
Radiation corrosion
Radiation induced segregation
Radiation
Material
Precursors
Impacts to Plant Operation (Load)
Ability of the Plant Safety Barriers to Respond to Impacts (Capacity)
Possible Impacts on Economics & Reliability & Safety

Figure 1-1. Representation of the interaction of degradation mechanisms that may impact plant operations and safety barriers if left unmitigated.

In this report, the word "safety" represents the freedom from those hazards that can cause death; injury; illness; damage to or loss of equipment or property; or adversely affects the environment.

One of the primary items inherent in the goals of the Pathway is the ability to propose and evaluate margin recovery strategies (i.e., proposed changes to SSCs or plant procedures that work to mitigate margin degradation due to aging or plant modifications). If a margin such as a plant safety is degraded, the RISMC methods and tools will serve to model, measure, and maintain margins for active and passive SSCs for normal and off-normal conditions. Moving beyond current limitations in safety analysis, the Pathway will develop techniques to conduct analysis using simulation-based studies of safety margins where "margin" go beyond the typical engineering margins concept. For example, licensing margins as a part of the plant's design basis are not the only ones protecting the public; plant safety depends on margins that are not necessarily analyzed in licensing.

While simulation methods in risk and reliability applications have been proposed for several decades, the availability of advanced mechanistic and probabilistic simulation tools have been limited. But, as noted by researchers such as Zio, (Zio, 2009) "…simulation appears to be the only feasible approach to quantitatively capture the realistic aspects of the multi-state system stochastic behavior." Consequently, the approach we are using for the RISMC Pathway is to use simulation of plant behavior as it relates to safety margins.

In order to carry out the research and development needed for the RISMC Pathway, INL, along with the Electric Power Research Institute (EPRI), has proposed a series of case studies that will explore methods- and tools-development issues. One of the initial case studies that have been proposed is to demonstrate the RISMC approach using the Advanced Test Reactor (ATR) as a test. Several reasons exist for this choice, including:

- ATR has a modern, full-scope, and updated probabilistic risk assessment (PRA) in the INL-developed analysis tool SAPHIRE.

- ATR has a realistic T-H input deck using RELAP5.
- ATR uses its PRA to make risk informed decisions (but not safety-margins based).
- Details for a variety of ATR information, including access to ATR engineering staff, are available to the RISMC Pathway researchers.

1.2 Advanced Test Reactor (ATR) Background

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. (Wikipedia)

An example of the reactor core, vessel, experimental piping, and control systems is shown in Figure 1-2. A line diagram (also known as a piping-and-instrumentation diagram) is shown in Figure 1-3 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 (see Figure 1-4 for an example of the RELAP5 nodalization used in these calculations). 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. For example, in Figure 1-5, we see that RELAP5 successfully captures the plant pressure behavior during a normal pump coast-down scenario.

In addition to the RELAP5 T-H input deck (which is used for both PRA and other safety-related calculations), 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)

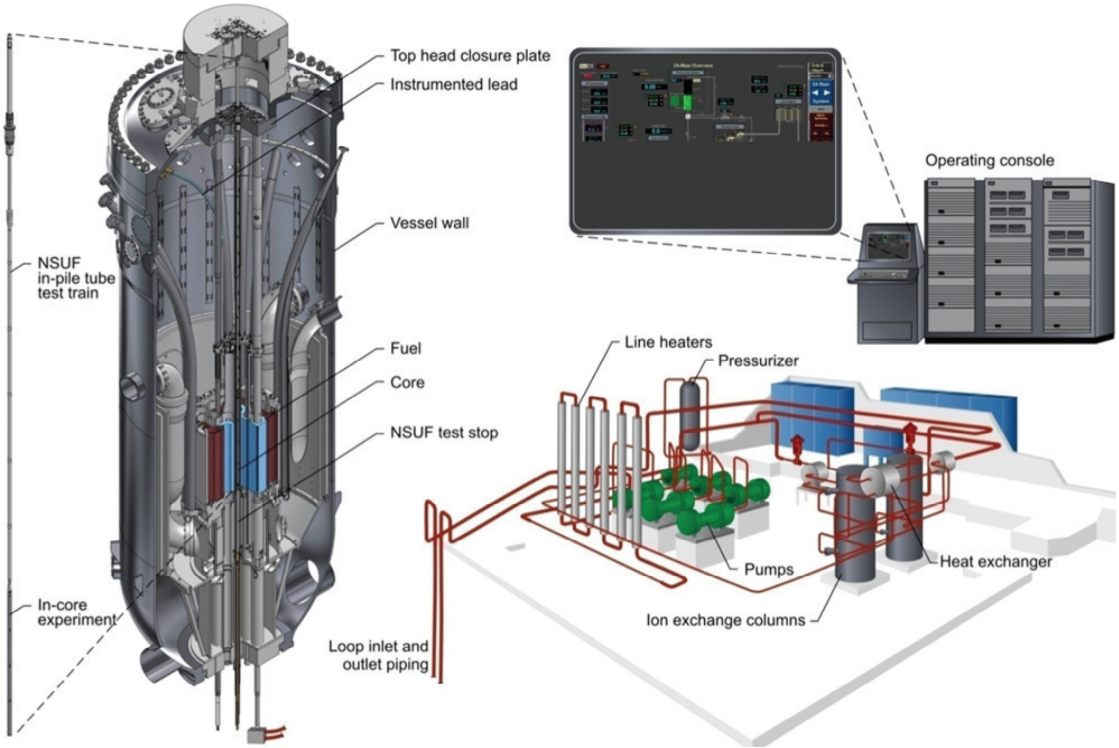


Figure 1-2. ATR experiment loop schematic representation.

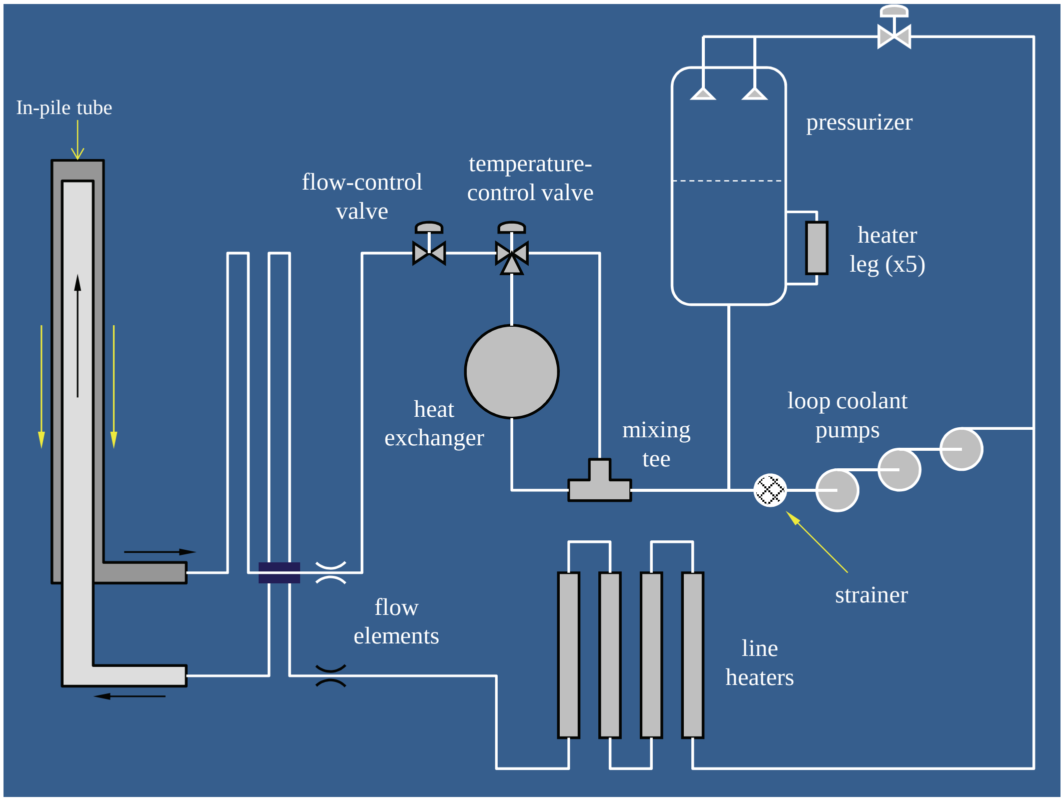


Figure 1-3. Component line diagram for an ATR experiment loop.

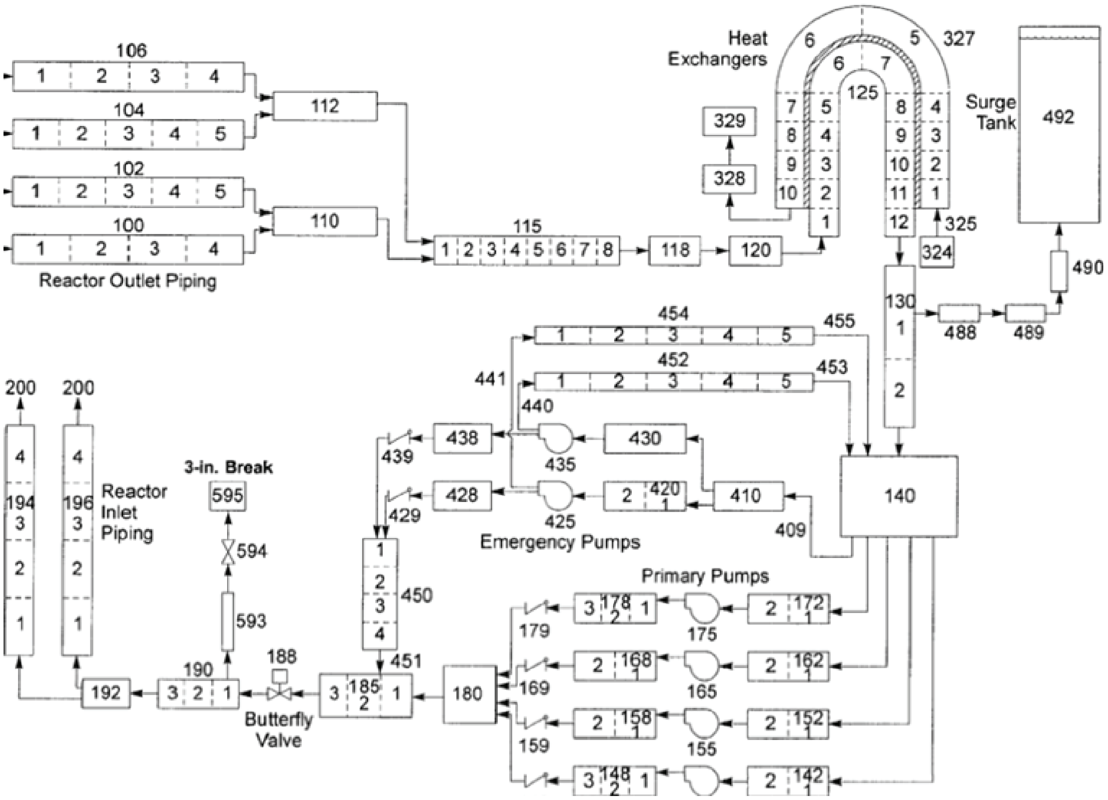


Figure 1-4. ATR RELAP5 input nodalization for main components in the primary coolant system.

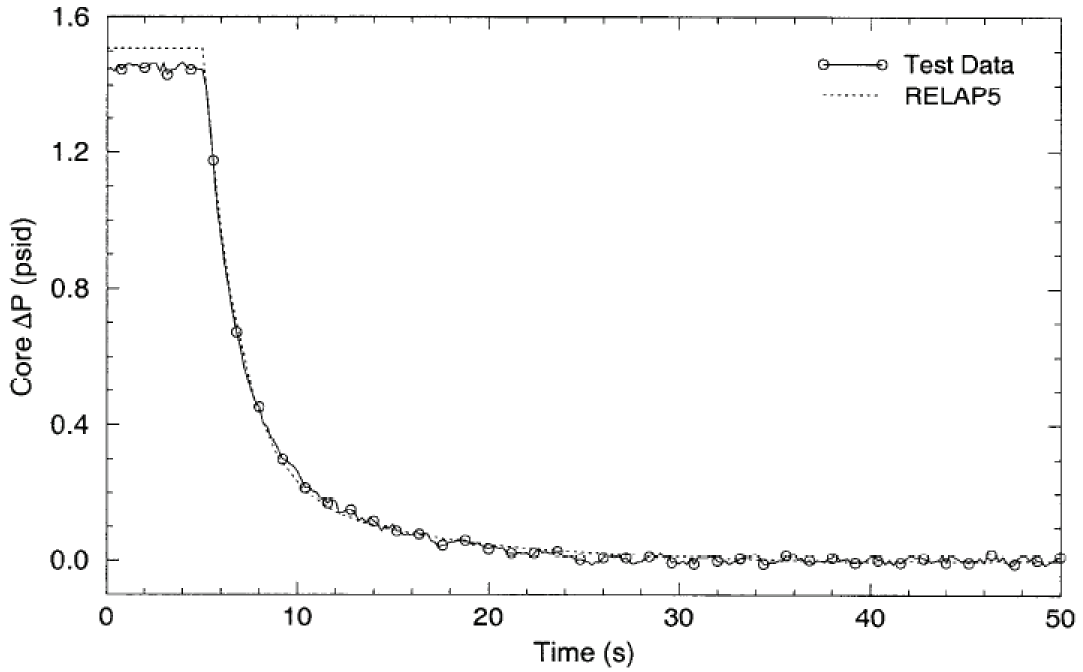


Figure 1-5. RELAP5 calculation comparison with test data for an ATR pump coast-down situation.

As part of the RISMC demonstration, we successfully coupled the risk assessment simulation to the T-H analysis (using RELAP5). As part of this analysis where we integrate probabilistic elements with mechanistic calculations, we are able to determine the plant physical T-H response. With the knowledge of the plant response, we still need to determine whether or not a particular outcome is “success” (meaning no fuel damage) or “failure” (meaning fuel damage). In the PRA, these categories are defined as the prevention or realization of significant core fuel damage that releases fission products, respectively.

The ATR PRA notes that fuel damage sufficient to release significant fission products may be in the form of:

- Cladding melting (or burnout) due to fuel over temperature
- Cracking or plate buckling due to fuel plate overstress
- Mechanical failures due to manufacturing errors or direct contact damage.

As part of this case study, we only considered cases where the fuel experienced an over temperature event. Further, for this analysis, we assumed that any event that saw a peak cladding temperature of 725 F (658 K) was a fuel damage outcome.

An example of what is determined to be fuel damage (from the T-H) is shown in Figure 1-6. In this figure, the ATR RELAP5 model simulates the calculated peak cladding temperature from two accident scenarios. The initiating event is a loss of power that results in the loss of the primary and emergency coolant pumps, the secondary coolant system pumps, and the pressurizing pumps. In the first transient, one reactor vessel vent valve is opened by the operators, allowing the reactor to depressurize. With the depressurization, the firewater injection system becomes available to inject water to the system, providing adequate core cooling and slowly reducing the fuel temperature. In the second transient, the reactor vessel vent valves remain closed. The system pressure increases until the safety relief valves begin cycling, thereafter maintaining a relatively high pressure. With no method of heat removal, the water in the reactor vessel continues to heat up, eventually reaching saturation and starting to boil. With no available high pressure coolant injection, a slow boiloff ensues. When sufficient water has been lost, the core begins to uncover, near 36 h in the simulation, and the fuel begins to heat up, quickly exceeding the melting temperature of about 930 K.

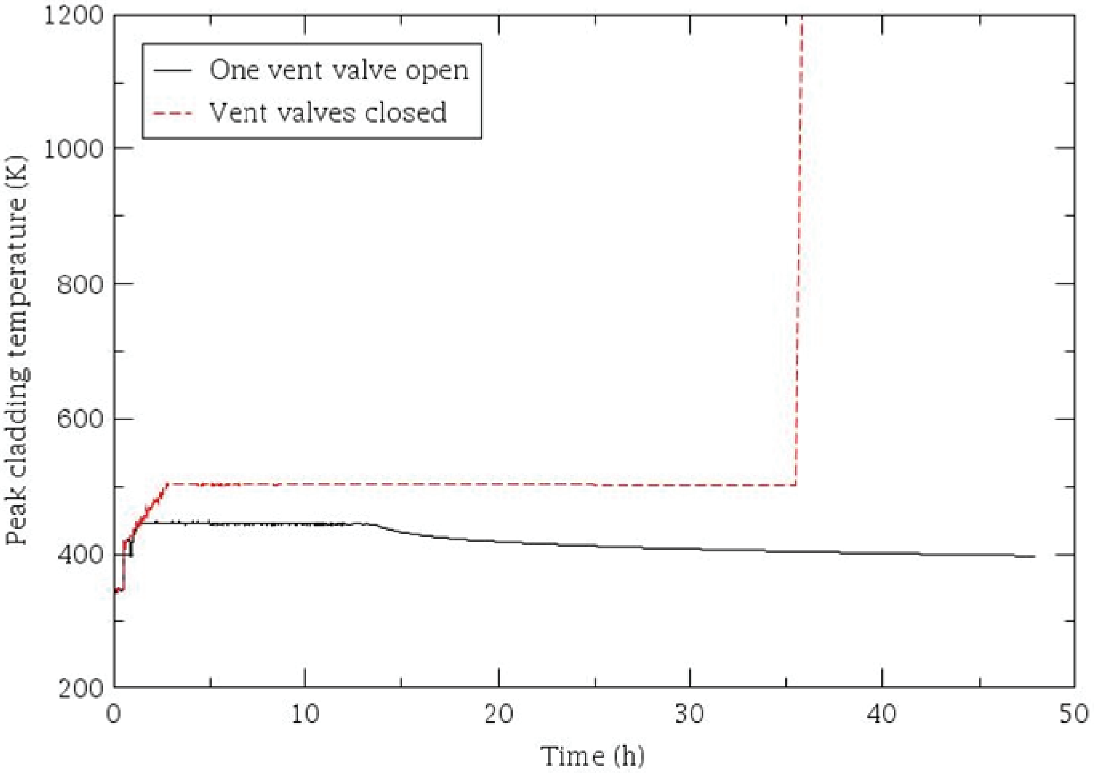


Figure 1-6. Simulated scenario leading to fuel damage (when venting is not available).

2. OVERVIEW OF THE ATR CASE STUDY

2.1 Case Study Purpose

The purpose of the RISMC ATR case study is to demonstrate the RISMC approach using realistic plant information, including both real PRA and T-H models. As part of this case study, we evaluated emergency diesel generator (EDG) issues since recently ATR has investigated how to change emergency backup power at the plant. Historically, ATR has had a continually-running EDG as a backup power supply which is different than all commercial NPPs in the U.S. (commercial plants have their EDGs in standby). The reason that ATR was designed to originally have an EDG constantly running (as the primary backup) was that commercial power at the INL (then called the National Reactor Testing Station) was somewhat unreliable. (Duckwitz, 2011)

Margin Recovery Strategies under consideration include:

- Keep the emergency power system as is (EDG running, one in standby, commercial power as backup)
- Redundant commercial power as primary backup, single new EDG as backup
- Redundant commercial power as primary backup, two existing EDGs as backup

For the different strategies, we would simulate the plant behavior both probabilistically (a EDG or commercial power might fail, for example) and mechanistically (the T-H behavior under off-normal conditions). To perform this simulation, we need to use the existing PRA and T-H information (e.g., SAPHIRE probabilities, RELAP5 input). We will then define the simulation for different scenarios and different strategies, and then run a large number of iterations to determine overall safety margins.

2.2 Details of the RISMC Case Study Approach

What differentiates the RISMC approach from traditional PRA is the concept of a safety margin. In PRA, a safety *metric* such as core damage frequency (CDF) is generally estimated using static fault- and event-tree models. However, we do not know how close we are to physical safety limits (say peak clad temperature) for most accident sequences described in the PRA. Further, as found in other research (Sherry & Gabor, 2011), there may be some scenarios that are considered to be "ok" (i.e., not core damage) that are close to or exceed safety limits. In the RISMC approach, what we want to understand is not just the frequency of an event like core damage, but how close are we (or not) to this event and how might we increase our safety margin through Margin Management Strategies.

In general terms though, a "margin" is usually characterized in one of two ways:

- A *deterministic* margin, defined by the ratio (or, alternatively, the difference) of an applied capacity (i.e., strength) to the load. For example, we test a pressure tank to failure where the tank design is rated for a pressure **C**, it failed at pressure **L**, thus the margin is (**L – C)** (safety margin) or **L/C** (safety factor).

- A *probabilistic* margin, defined by the probability that the load exceeds the capacity. For example, we model failure of a pressure tank where the tank design capacity is a distribution f(**C**), its loading condition is a second distribution f(**L**), the probabilistic margin would be represented by the expression Pr[f(**L**) > f(**C**)].

A **probabilistic safety margin** is a numerical value quantifying the probability that a key safety metric (e.g., for an important process observable such as clad temperature) will be exceeded under specified accident scenario conditions.

The RISMC Pathway uses the probabilistic margin approach to quantify impacts to economics, reliability, and safety. Further, we use this approach in risk-informed margins management to present results to decision makers as it relates to Margin Recovery Strategies, as will be described in Section 3.

As an example of the type of results that are generated via the RISMC method and tools, we show a simple hypothetical example in Figure 2-1. For this example, we suppose that a NPP has two alternatives to consider:

Alternative #1 – retain an existing, but aging, component as-is

Alternative #2 – replace the aging component with a new one

Using the RISMC analysis methods and tools (described in Section 3), we run 30 simulations where this component plays a role in plant response under accident conditions. For each of the 30 simulations, we calculate the outcome of a selected safety metric – say peak clad temperature – and compare that against a capacity limit (assumed to be 2200°F in this example). However, we have to run these simulations for both alternative cases (resulting in a total of 60 simulations).

The results of these simulations are then used to determine **the probabilistic margin**:

Alternative #1: Pr(Load exceeds Capacity) = 0.17

Alternative #2: Pr(Load exceeds Capacity) = 0.033 (note lower values are better)

In this example, the “load” is the blue and red boxes shown in Figure 2-1 (measured by the peak clad temperature for each simulated scenario) and the “capacity” is the 2200°F 10 CFR50.46 limit.

If the safety margin characterization were the only decision factor, then Alternative #2 would be preferred (its safety characteristics are better) since we only realized one case where we exceeded our 2200°F safety limit.

Note though that the safety margin insights are only part of the decision information that would be available to the decision maker, for example the costs and schedules related to the alternatives would also need to be considered. In many cases, multiple alternatives will be available to the decision maker due to level of redundancy and several barriers for safety present in current NPPs.

Because one LWRS objective is to develop technologies that can improve the reliability, sustain safety, and extend the life of the current reactors, any safety margin focus would need to consider more realistic load and capacity implications for operating NPPs. For example, the notional diagram shown in Figure 2-2 illustrates that safety, as represented by a load distribution, is a complex function that varies from one type of accident scenario to the next. However, the capacity part of the evaluation may not vary as much from one accident to the next because the safety capacity is determined by physical design elements such as fuel and material properties (which are common across a spectrum of accidents) or regulatory safety limits (such as the 10 CFR 50.46 limit in Figure 2-1).

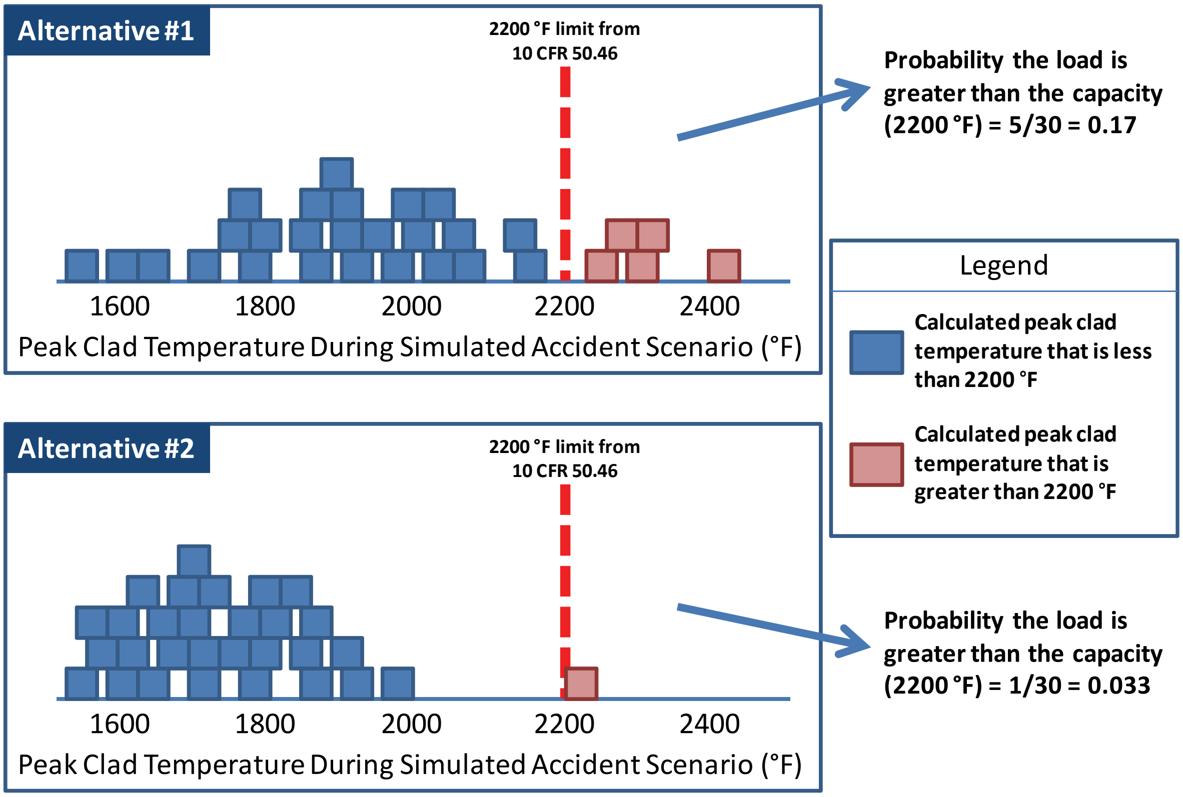


Figure 2-1. RISMC example when evaluating alternatives for risk-informed margins management.

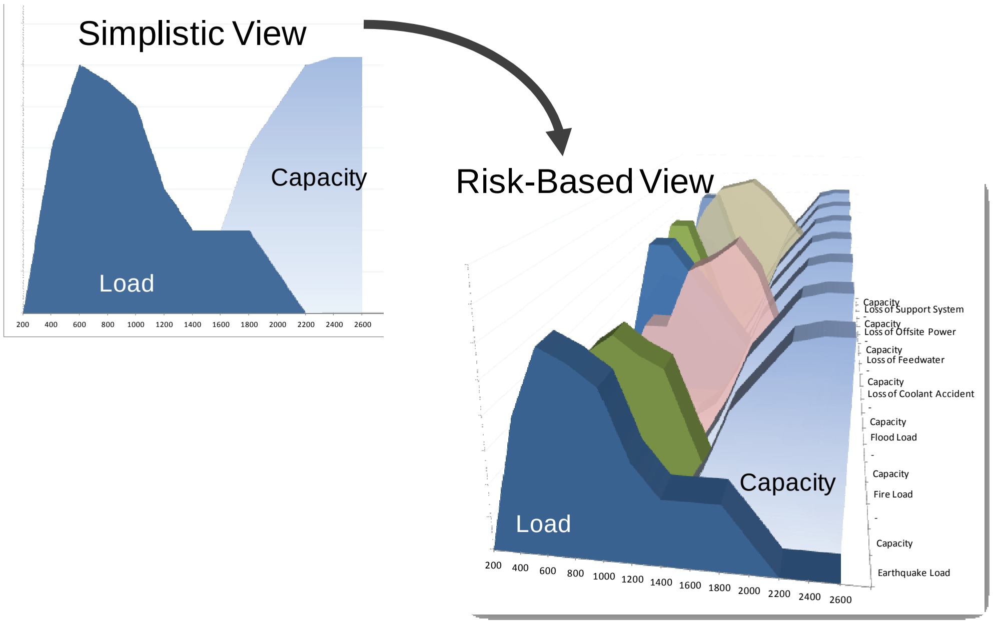


Figure 2-2. Family of load and capacity distributions representing different accident conditions.

To successfully accomplish the goals described in Section 2.1, the RISMC Pathway will define and demonstrate the risk-informed safety margin approach using a series of case studies. The determination of a quantitative safety margin requires an understanding of risk-based scenarios. Within a scenario, an understanding of plant behavior (i.e., operational rules such as technical specifications, operator behavior, and SSC status) and associated uncertainty will be required to interface with a systems code (i.e., RELAP-7 as part of the RISMC Toolkit). Then, to characterize safety margin for a specific safety performance metric[a] of consideration (e.g., peak clad temperature), the plant simulation will determine time and scenario-dependent outcomes for both the load and capacity. Specifically, the safety margin approach will use the physics-based plant results (the "load") and contrast these to the capacity (for the associated performance metric) to determine if safety margins have been exceeded (or not) for a family of accident scenarios.

The RISMC Pathway will also develop a significantly improved plant physics code (i.e., RELAP-7) and a suite of simulation methods for driving RELAP-7 to analyze safety margin as part of the RISMC Toolkit. These tools will use advanced computational techniques to simulate the behavior of NPPs in a way that develops more comprehensive safety insights and enables a more useful risk-informed analysis of plant safety margin than can be done using existing tools. RELAP-7 is a systems code, meaning it will simulate behavior at the plant level (i.e., it will address a broad range of phenomena at a level of detail that is feasible and appropriate for a plant scale of modeling) as opposed to analyzing highly localized phenomena in great detail at every point in the plant (which is still infeasible today).

2.3 Benefits of the RISMC R&D

As previously noted, the purpose of the RISMC Pathway is to support plant decisions for risk-informed margins management with the aim to improve economics, reliability, and sustain safety of current NPPs. As one of the Pathways in the LWRS Program, there are a variety of benefits to be realized from the RISMC Pathway, including:

- The RISMC Pathway
    - Provides to decision makers the safety case, based upon Technical Guides, in order to select operational alternatives as part of Margin Management activities.
    - Develops a significantly improved plant physics (including T-H and neutronics) codes.
    - Greatly improves the U.S. risk analysis capabilities by creating a unique suite of simulation methods that builds upon traditional probabilistic risk assessment (PRA) approaches.
    - Creates an integrated approach to coupling component aging and damage evolution to the risk analysis models so that material degradation can be quantified.
    - Replaces traditional static fault- and event-tree models by merging NPP scenario simulation with improved plant physics to determine outcomes of key physical process variables.

[a] Safety performance metrics may be application-specific, but in general are engineering characteristics of the NPP, for example as defined in 10 CFR 50.36, "safety limits for nuclear reactors are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain of the physical barriers that guard against the uncontrolled release of radioactivity."

3. CASE STUDY DETAILS AND RESULTS

The purpose of this section is to describe the ATR case study and results of the analysis.

To better understand the approach to determine safety margins, we first describe the two types of analysis used in this pathway (see Figure 3-1), probabilistic and mechanistic quantification. Note that in actual applications, a blended approach is used where both types of analysis are used to support any one particular decision. For example, the approach could be either mostly probabilistic, mostly mechanistic, or both.

Types of Analysis Used in Safety Margin Evaluations

PROBABILISTIC	MECHANISTIC
Pertaining to stochastic (non-deterministic) events, the outcome of which is described by a probability.	Pertaining to predictable events, the outcome of which is known with certainty if the inputs are known with certainty.
Probabilistic analysis uses models representing the randomness in the outcome of a process. Because probabilities are not observable quantities, we rely on models to estimate probabilities for certain specified outcomes.	Mechanistic analysis (also called “deterministic”) uses models to represents situations where the observable outcome will be known given a certain set of parameter values.
An example of a probabilistic model is the counting of *k* number of failures of an operating component in time *t*: Probability(k=1) = $\lambda e^{-\lambda t}$.	An example of a mechanistic model is the one-dimensional transfer of heat (or heat flux) through a solid: $q = -k\partial T/\partial x$.

Figure 3-1. Types of analysis that are used in the RISMC Pathway.

The use of both types of analysis, probabilistic and mechanistic, is represented in Figure 3-2. Probabilistic analysis is represented by the risk analysis while mechanistic analysis is represented by the plant physics calculations. Safety margin and uncertainty quantification rely on plant physics (e.g., T-H and reactor kinetics) coupled with probabilistic risk simulation. The coupling takes place through the interchange of physical parameters (e.g., pressures and temperatures) and operational or accident scenarios.

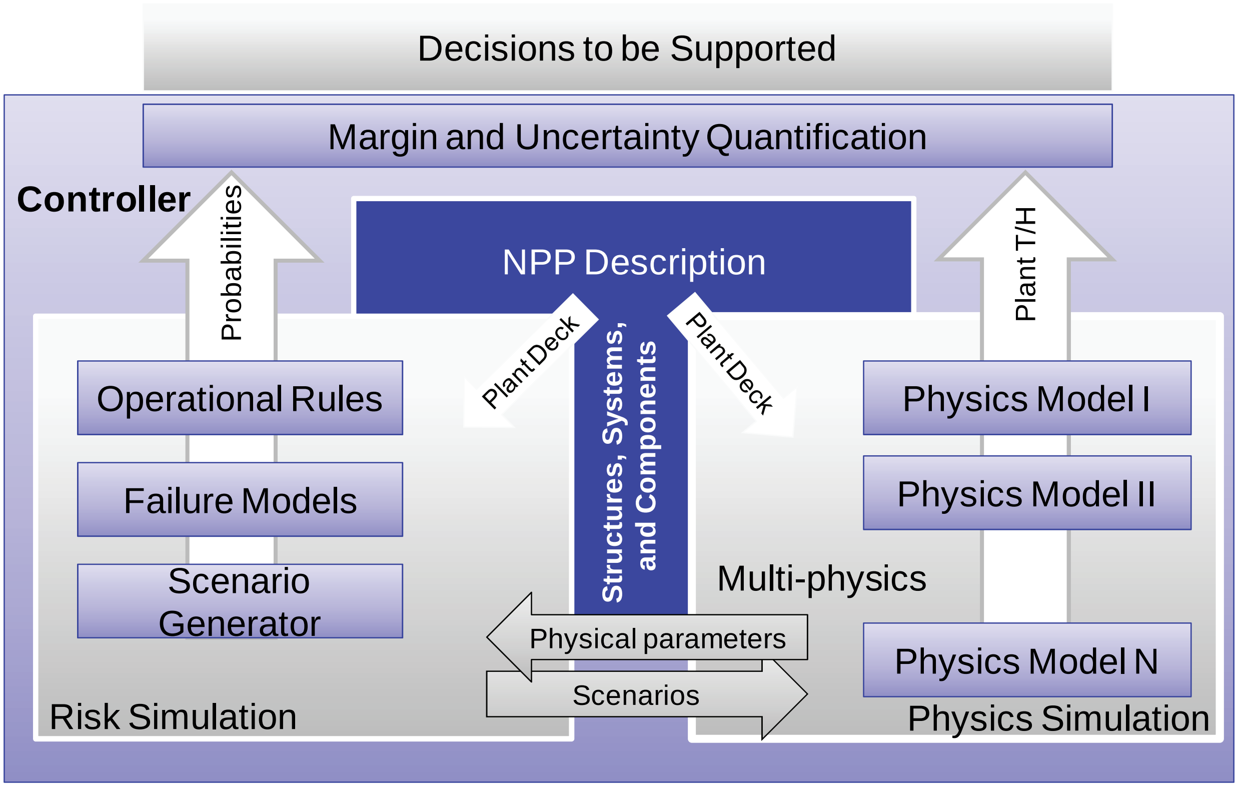


Figure 3-2. Attributes of the RISMC approach for supporting decision-making.

3.1 The Case Study Approach

3.1.1 ATR Case Study Purpose

The purpose of the ATR case study is to provide a demonstration of the RISMC method supporting safety margin management. The technical basis for safety margins management is captured in what is known as the "safety case." While definitions may vary in detail, the safety case essentially means the following:

> *A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is adequately safe for a given application in a given environment.(Bishop & Bloomfield, 1998)*

The realization of a safety case for the ATR is an output when applying the RISMC method. The safety-margin claims do the following:

- Make an explicit set of safety margin claims about the ATR facility and SSCs of interest (e.g., emergency backup power components such as diesel generators).

- Produce qualitative and quantitative evidence that supports the claims above.

- Provide a set of safety margin management options (i.e., margin recovery strategies) that link the claims to the probabilistic and mechanistic evidence.

- Make clear the assumptions, models, data, and uncertainties underlying the arguments.

- Allow different viewpoints and levels of detail in a graded fashion for decision making.

3.1.2 RISMC Process Steps

The mechanics to conduct margins analysis, including a methodology for carrying out simulation-based studies of safety margin, are described in this section. For the ATR case study, we used the following RISMC-specific process steps (also shown in Figure 3-3):

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 (the key parts of which are illustrated in Figure 3-4).

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.

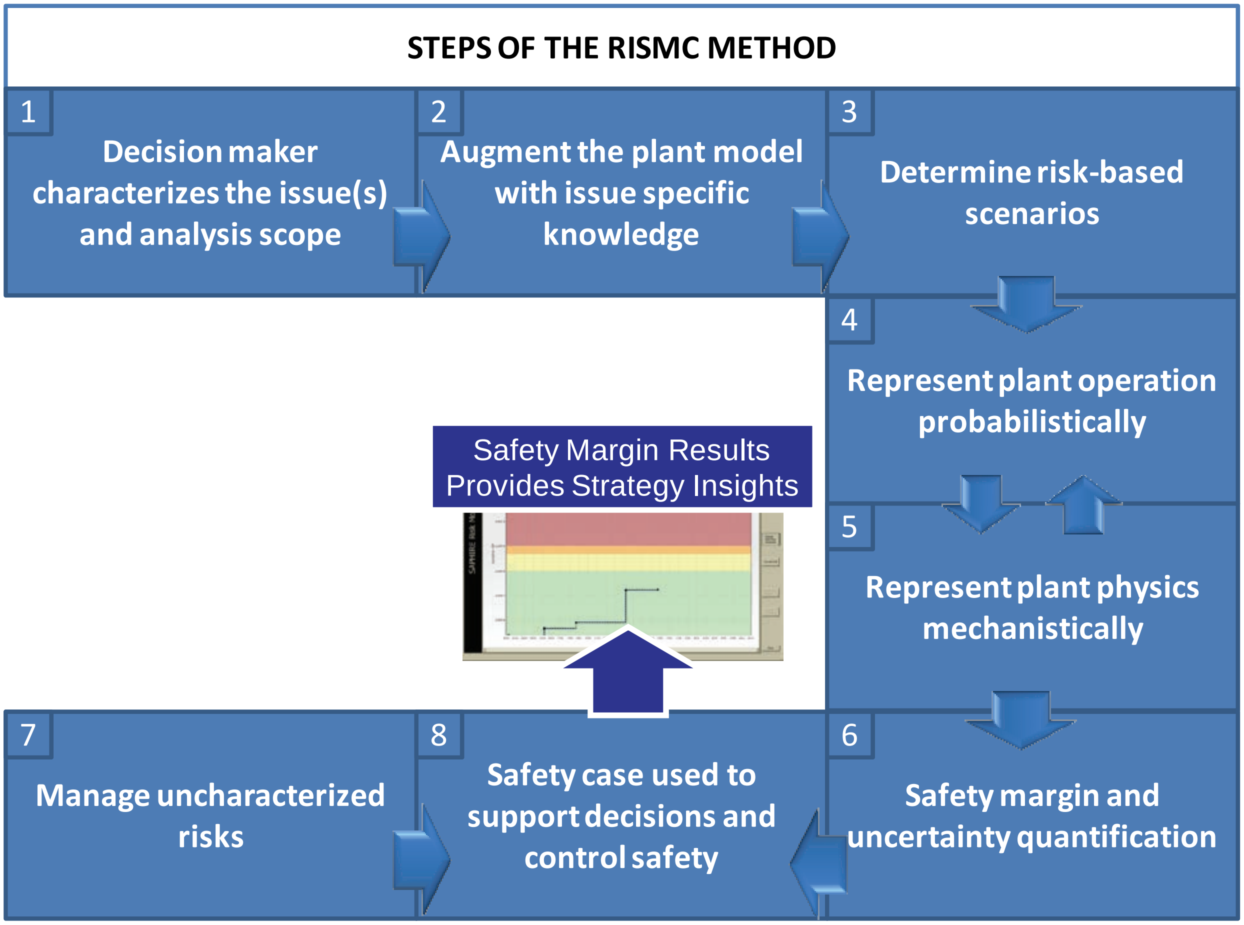

STEPS OF THE RISMC METHOD
1
Decision maker characterizes the issue(s) and analysis scope
2
Augment the plant model with issue specific knowledge
3
Determine risk-based scenarios
4
Represent plant operation probabilistically
5
Represent plant physics mechanistically
6
Safety margin and uncertainty quantification
7
Manage uncharacterized risks
8
Safety case used to support decisions and control safety
Safety Margin Results Provides Strategy Insights

Figure 3-3. Depiction of the high-level steps required in the RISMC method.

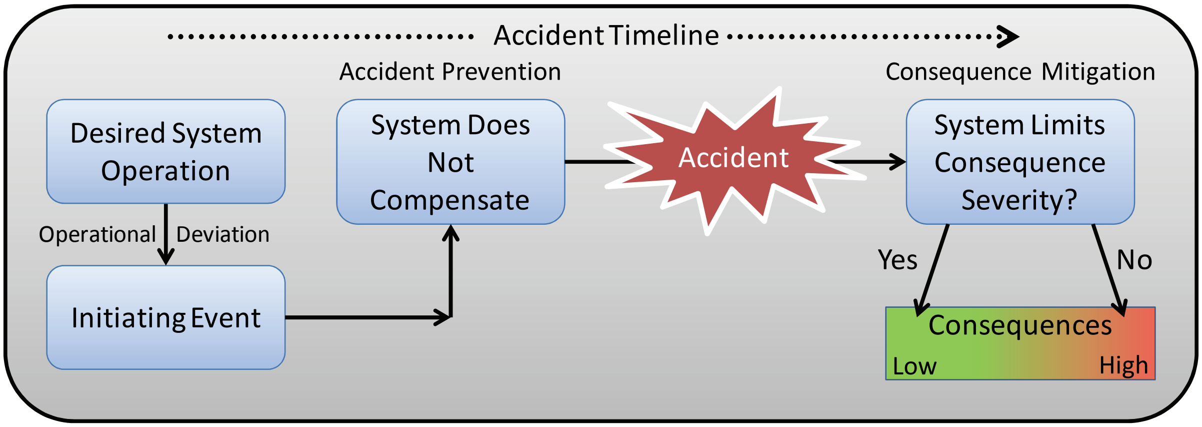


Figure 3-4. Accident scenario representation.

Note that for the ATR case study demonstration, we applied the RISMC steps to different degrees of detail. For example, Step 7 of the process, managing uncharacterized risks, was not explored in detail while Step 4, representing the plant operation probabilistically, was evaluated in detail based upon the ATR PRA. Nonetheless, all eight steps and the results of the RISMC method are described in the following subsections.

3.2 Characterizing the Issue and Analysis Scope

The purpose of this step is to characterize the issue to be resolved in a way that explicitly scopes the modeling and analysis to be performed. For the safety metrics of interest, we need to determine where hazards exist and what scenarios might lead to experiencing the hazards.

Note that not all deviations from a desired system operation lead to mishaps or accidents; but, if operational intent is specified appropriately, all mishaps and accidents will be found to correspond to one or more deviations from desired operation. Specification of operational intent therefore implies categories of hazards, and provides cues to the identification process. Further, these hazards typically are considered for the various *possible* safety impacts shown in Figure 3-5, especially when considering an "all hazards" integrated model. For the ATR Case Study, we focused on fuel melt scenarios (a thermal energy issue) as highlighted in Figure 3-5.

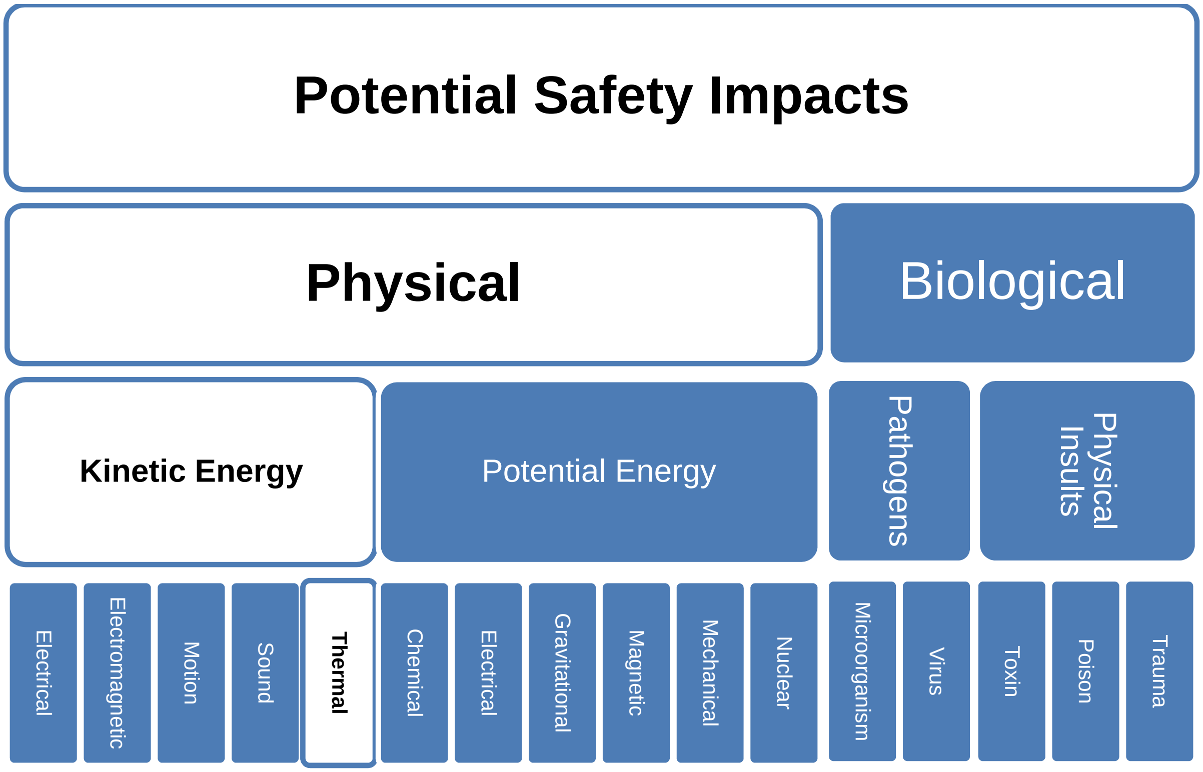


Figure 3-5. Examples of type types of hazards that may lead to safety impacts.

For the case study under consideration, we include the margin management strategies of:

I. Keep the emergency power system as is (an EDG running, one in standby, commercial power as backup).

II. Redundant commercial power as primary backup, single new EDG as backup.

III. Redundant commercial power as primary backup, existing EDGs as backup.

The types of results of the analysis (the output of Step 8 of the RISMC approach) are illustrated in Figure 3-6, where we are able to calculate the changes in safety margin using a risk-informed approach that accounts for consequences and frequency of undesired outcomes. For each strategy identified above, we will calculate the probabilistic margin for fuel melt scenarios and will compare the different strategies against each other in order to effectively manage safety related to this case study.

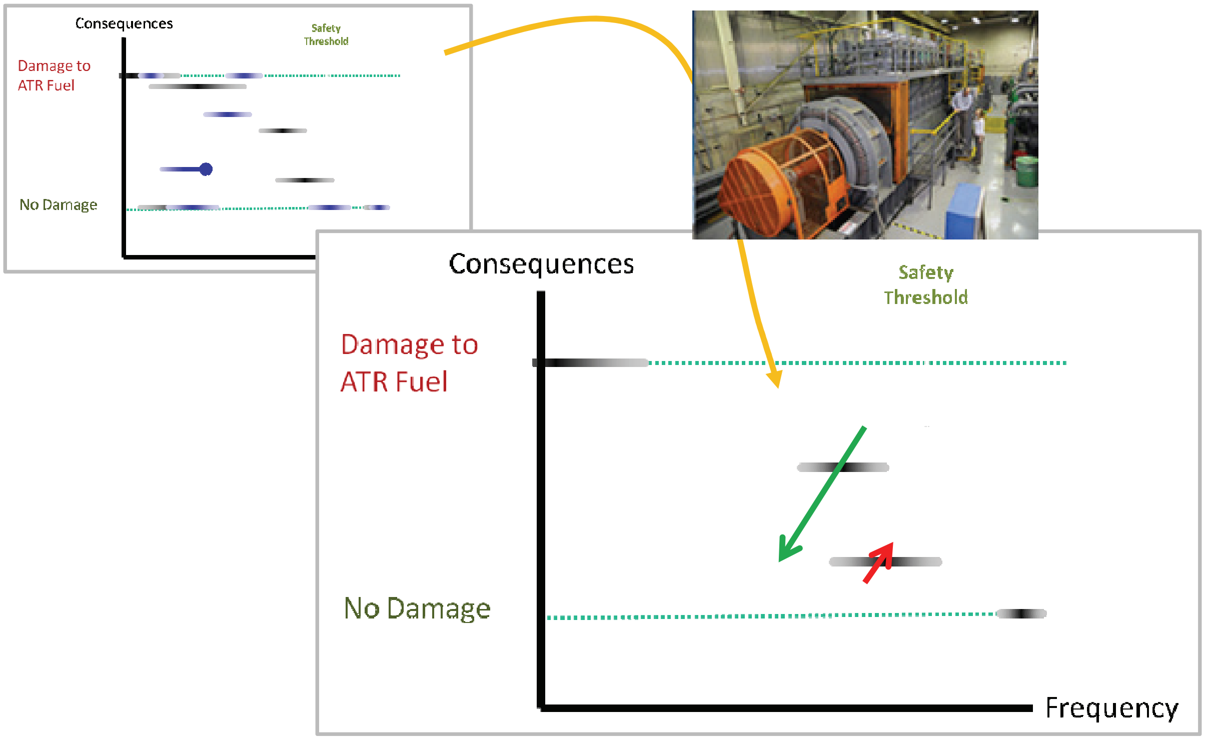


Figure 3-6. Representation of Margin Management Strategies where plant changes can reduce or maintain safety.

3.3 Issue Specific Knowledge

The purpose of this step is to quantify the decision-maker and analyst's state-of-knowledge (uncertainty) of the key variables and models relevant to the issue. In general though, for the ATR case study, we need to:

- Represent initiating events. While the ATR PRA considers approximately 30 initiating events, the analysis for this case study considered only 10 different initiating events. Included in the represented initiating events are loss of power, routine shutdowns, and small break loss of coolant transients.

- Incorporate information specific to EDG modifications. We considered the implication of changes to the plant related to backup power variations.

- Extract PRA information. We (as described in the next section) used the ATR PRA as the starting point for all of the probabilistic information used in the scenario simulation step.

During the development of the case study, we consulted with ATR domain knowledge experts both on the PRA and the T-H simulation as needed.

3.4 Risk-Based Scenarios

The purpose of this step is to determine issue-specific, risk-based scenarios and accident timelines (as were shown in Figure 3-4). Simulation-assisted risk assessment provides a framework for integrated mechanistic/probabilistic treatment of physical processes and system reliability. As such, it exercises a tight coupling between phenomenology (represented by process parameters in codes such as RELAP) and reliability (i.e., failure of systems/components).

Simulation encompasses a variety of rules and models that describe plant control and operator behavior, such as:

- Rules
  - Operating rules (e.g., technical specifications, emergency operating procedures, maintenance practices, core management)
  - External factors (e.g., grid and regulatory consideration)
- Models
  - Occurrence of an initiating event
  - Failure of a component
  - Dependencies that impact multiple SSCs

By combining these rules and models, the resulting "physics-based reliability" engine gives an enhanced capability to identify and assess plant vulnerability. Further, this engine then provides the mechanism for coupling with the plant physics models.

The approach to solving accident sequences is designed to be able to explore both the success portions and failure parts of the operational space since, for the majority of the time, the system is in the success state. For example, a common simulation approach is that where state transitions are generated probabilistically (see Appendix A for additional details on this type of simulation approach). In this approach, a time-of-transition is calculated (via the simulation). However, for most scenarios in NPPs, the normal situation is that the plant is functioning properly for most of the time. In the case of ATR, this represents the situation where the plant is at power and experiments are taking place during the testing cycle. Nonetheless, we need to consider both success and failure space for operation, and when in failure space, evaluate the potential consequence outcomes (as shown in Figure 3-7).

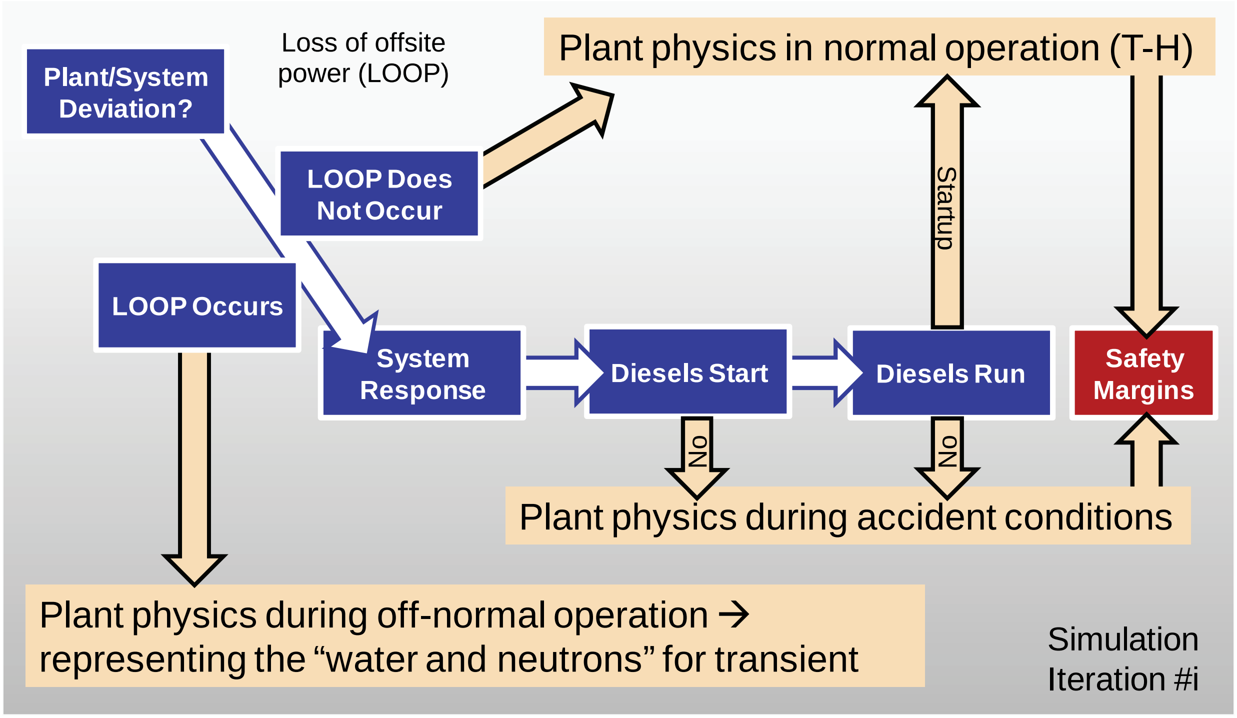

Plant/System Deviation?
Loss of offsite power (LOOP)
Plant physics in normal operation (T-H)
LOOP Does Not Occur
Startup
LOOP Occurs
System Response
Diesels Start
Diesels Run
Safety Margins
No
No
Plant physics during accident conditions
Plant physics during off-normal operation → representing the "water and neutrons" for transient
Simulation Iteration #i

Figure 3-7. Representation of the scenario considerations during a single simulation iteration.

For the ATR Case Study, a probabilistic simulation model used was created based upon the ATR PRA. We used an existing discrete event simulation modeling tool where the model consists of simulation objects that transition through various states to describe a plant-response scenario to an off-normal condition.

The SAPHIRE PRA uses initiating events, basic events, event trees, and fault trees to define all of the possible scenarios for normal and off-normal plant conditions. The conversion process identifies initiating events of interest (ten were chosen for the ATR Study of which two, LOP-Loss of Electrical Power and S12-Small Loss of Coolant Accident were studied in detail). Each initiating event is associated with several event trees that define the plant's possible response to the event. The event tree (see Figure 3-8 for an example of an event tree) consists of several "top events" (LCP representing loss of commercial power, DGPIE representing loss of EDG power, etc.). The conversion defines each top event as a simulation object (see Figure 3-9).

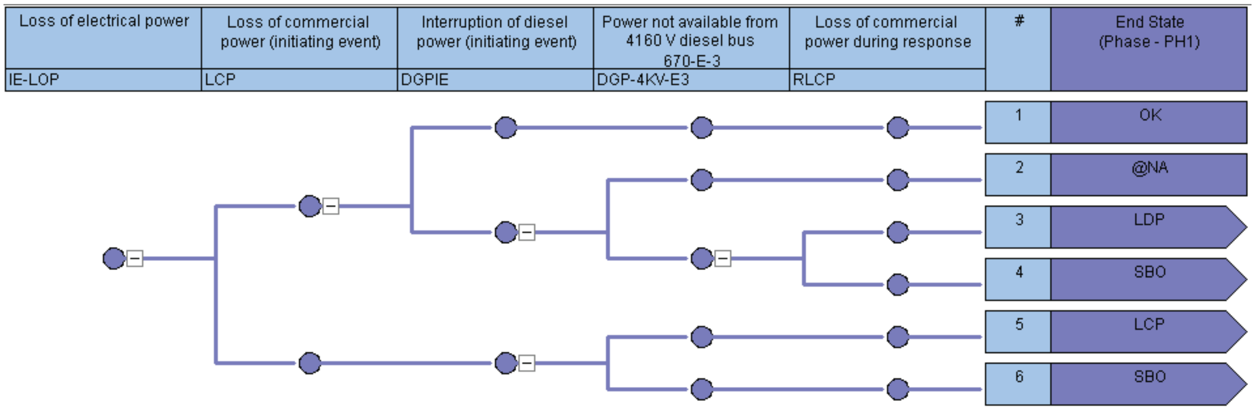

Loss of electrical power
Loss of commercial power (initiating event)
Interruption of diesel power (initiating event)
Power not available from 4160 V diesel bus 670-E-3
Loss of commercial power during response
#
End State (Phase - PH1)
IE-LOP
LCP
DGPIE
DGP-4KV-E3
RLCP
1
OK
2
@NA
3
LDP
4
SBO
5
LCP
6
SBO

Figure 3-8. ATR SAPHIRE initial event tree for the LOP initiating event.

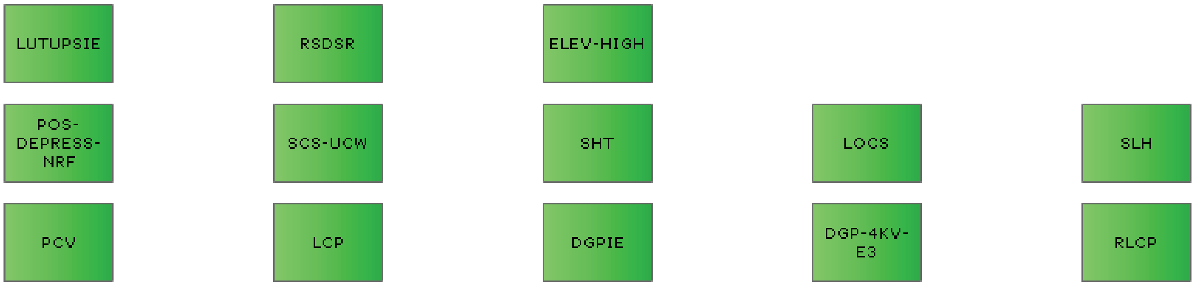


Figure 3-9. ATR simulation objects (a partial set).

Each top event can be in multiple states but for the ATR PRA these states are usually binary (failure or success). In the PRA, a fault tree is used to define the probability of transitioning to another possible state. The approach we used for the ATR case study was to define four object states and four state transition events for each top event (see Figure 3-10):

- The first state is the nominal or default operating state of the simulation object.
- The next two states represent a successful (upper) or failed (lower) state. The transition to either one of these states is based on the system structure as defined in the original PRA fault tree. For example, if a EDG had a fault tree that included cooling is required to maintain proper operation of the EDG, then the simulation would also include this cooling function. If the system state evaluation results in an immediate failure (at time zero), the object transitions directly to the failed state. Otherwise it transfers to the success state.
- For the last possible state, we represented the case where a time-delayed failure is detected. For example, if the EDG started but failed in three hours, then this time-delayed failure would be triggered in the simulation. When this trigger is enacted, a transition (including its time) is entered into a simulation queue.

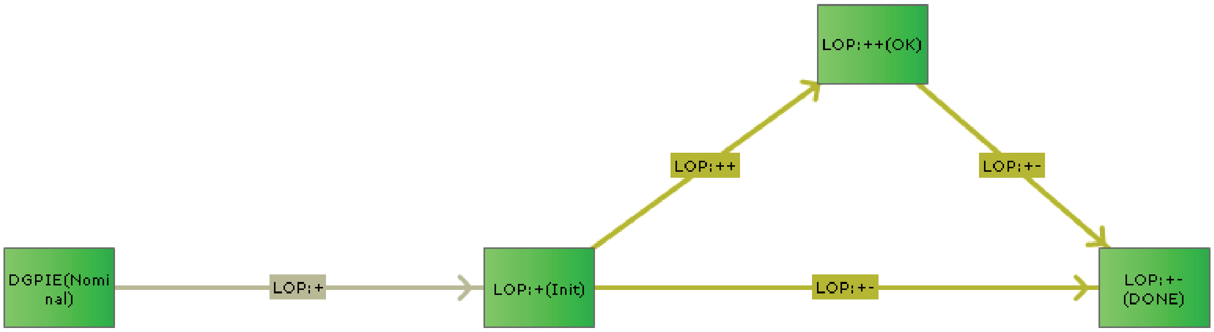


Figure 3-10. Object state and transition model diagram.

For all of the systems, the associated SAPHIRE fault tree structure is converted to a similar linked structure of complex and basic events representing a state table for the system. Note that the "complex events" are similar to the fault tree gates with a count that defines the number of failures needed to fail the complex event. For example, the ATR has two emergency pumps (components 435 and 425 as seen in Figure 1-4). For this system to fail, both pumps have to fail, for a failure count of two.

To better illustrate how the system state approach works in the simulation we have developed, we show an example EDG system in Figure 3-11 where failure of the system is experienced when any two of the EDGs fail. For example, a failure of the system occurs when both the A and B EDGs fail. The state table used in the simulation for this example system is shown in Table 3-1. During the simulation, we check to see if any of the three EDGs (A, B, or C) have failed. If one or more has failed, we then check to see if the system is failed by using the state table.

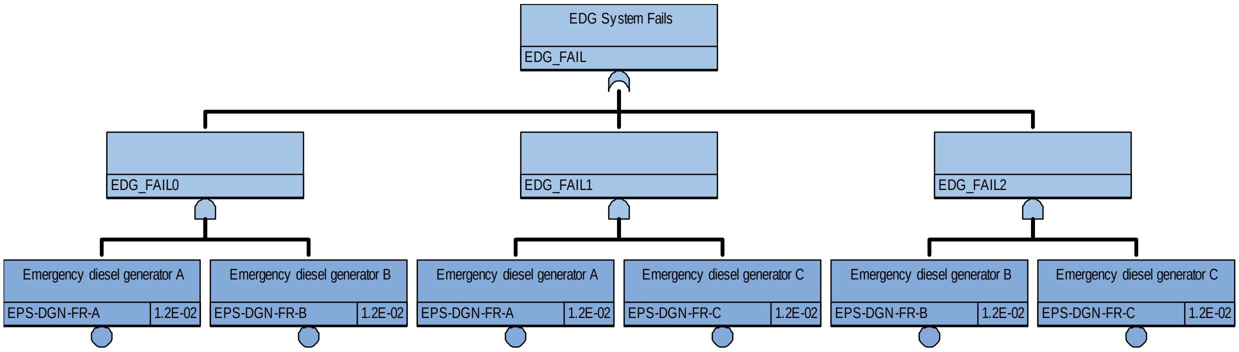

EDG System Fails
EDG_FAIL
EDG_FAIL0
EDG_FAIL1
EDG_FAIL2
Emergency diesel generator A
EPS-DGN-FR-A
1.2E-02
Emergency diesel generator B
EPS-DGN-FR-B
1.2E-02
Emergency diesel generator A
EPS-DGN-FR-A
1.2E-02
Emergency diesel generator C
EPS-DGN-FR-C
1.2E-02
Emergency diesel generator B
EPS-DGN-FR-B
1.2E-02
Emergency diesel generator C
EPS-DGN-FR-C
1.2E-02

Figure 3-11. Example EDG system consisting of three divisions of diesels.

Table 3-1. State table for the example EDG system shown in Figure 3-11.

EDG Fails		
Complex Event EDG_FAIL0	Complex Event EDG_FAIL1	Complex Event EDG_FAIL2
Failure Count = 2 EDG A fails, EDG B fails	Failure Count = 2 EDG A fails, EDG C fails	Failure Count = 2 EDG B fails, EDG C fails

Note that the “children” of a complex event in a system state table can be other complex events or basic events. The complex event can also fail due to a common cause failure. A common cause failure probability is stored in the complex event that is a “parent event” to related component failure events (for example, for a group of redundant components). One technical issue that was considered for the system simulation was how to represent dependent failures, for example how to calculate the probability of pump 435 to fail when pump 425 has failed. To solve this issue, we used the definition of conditional probabilities and thereby force transitions during the simulation based upon their specific conditional probabilities. The details of this calculation are described in Appendix B.

3.5 Probabilistic Plant Operation

Representing plant operation probabilistically using the scenarios identified in Step 3 of the RISMC approach is next. As part of operational scenario generation, plant “rules” (e.g., operator procedures, technical specifications, maintenance schedules) are used to provide realism. 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.

3.5.1 Example of simulating probabilistic operations

To better understand the approach of simulating plant operation using probabilistic concepts, we first describe a simplistic simulation example. In this example, we have a possible scenario where a plant may experience a loss of offsite power (which challenges the safety systems), an EDG may fail to start, or an EDG may fail to run (if it starts successfully). In this example, we can define models for the plant observable events, specifically:

- Loss of offsite power – LOOP ~ Poisson(λ=0.1/yr)
- Failure of a EDG to start – DG_START ~ Binomial(p=0.2/demand)
- Failure of a EDG to run – DG_RUN ~ Poisson(λ=0.01/hr)

where the symbol “~” means “defined as the probabilistic distribution.”

We then create a simulation (which we did in Excel) and run N number of iterations of this simulation. First, we check to see if an initiating event has occurred in the mission time of the next year. Since the average rate of initiating events is once every 10 years (or 0.1 per year), we would only expect to see events occurring once in every 10 iterations (on average). The results of the initiating event part of the simulation for the first 50 iterations are shown in Figure 3-12, where an iteration represents a single year of plant operation. These results are used to determine whether (or not) an initiating event has occurred.

Any case where we “saw” a LOOP in a calendar time of less than one year indicates that an initiating event (i.e., the LOOP) has occurred. In this example, we can see that a LOOP has occurred **six times** in the 50 iterations (they are shaded red in Figure 3-12). In other words, we have just simulated 50 years of plant operation, and during those 50 years, we have seen six LOOP events. We used this approach to simulate the ten different initiating events from the ATR PRA. However, for the ATR case study, we were able to simulate millions of years of (virtual) plant operation probabilistically.

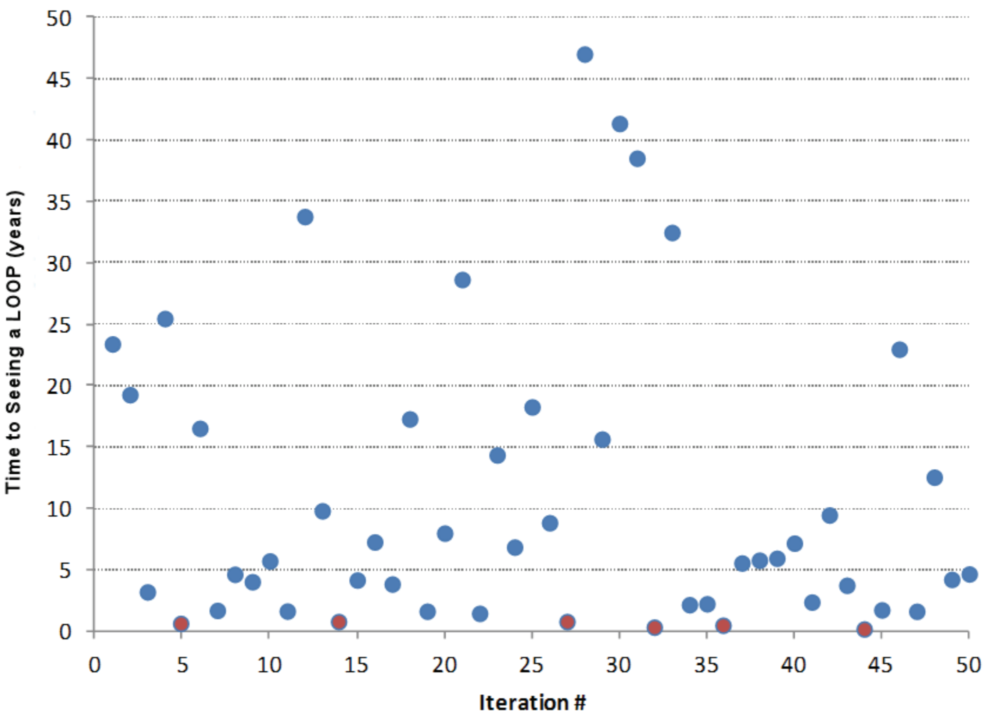


Figure 3-12. Simulation results (50 iterations) for the event LOOP.

For the example described in this section, we see that we have simulated 50 years of operation, where 44 years *did not* see an initiating event, and six years did see an initiating event (a LOOP). However, at a NPP, it takes more than just an initiating event to result in accident conditions.

The second part of the simulation is to check, for each time we see a LOOP, what happens with the system response, in our case the EDGs. The starting of the diesels was defined to have a probability model where each time it is demanded, they fail with probability of 0.2. The results of this part of the simulation are shown in Figure 3-13, where any outcomes in the shaded region (less than 0.2 probability) are considered to be failures. In the first 50 iterations, we saw six initiating events, and following these six events, we see a total of two times that the EDG represented by DG_START failed (on iteration 27 and iteration 44). In other words, in year 27 of the simulation, we saw a LOOP followed by the EDG failing to start. We saw this same event occur during year 44 of the simulation.

Lastly, we need to consider the scenario when a diesel starts but then fails to run. The event for DG_RUN follows a Poisson model with a failure rate of 0.01/hr. To determine what is failure and success, we need to define a mission time for this system. For this example, we assumed that the system must function for 24 hours (after 24 hours, the decay heat is low enough to preclude fuel damage), so any predicted failure times *longer* than 24 hours are considered to be a success (i.e., a failure occurs *after* 24 hours). In each case of the analysis, we simulated the diesels operating, once for each LOOP occurrence. The results of this part of the simulation are shown in Figure 3-14, where we can see that the system failed to run for 24 hours one time out of the six tries. In other words, in year 5 of the simulation, we saw a LOOP followed by the EDG starting, but then failing to run for 24 hours after the initiating event.

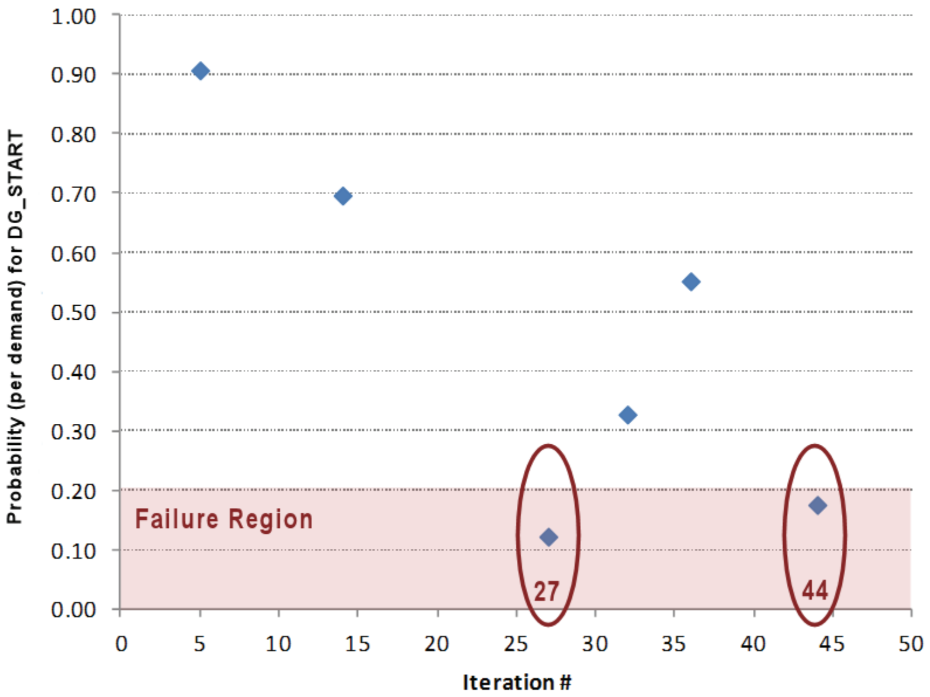


Figure 3-13. Simulation results (50 iterations) for the diesel generators failing to start (or not).

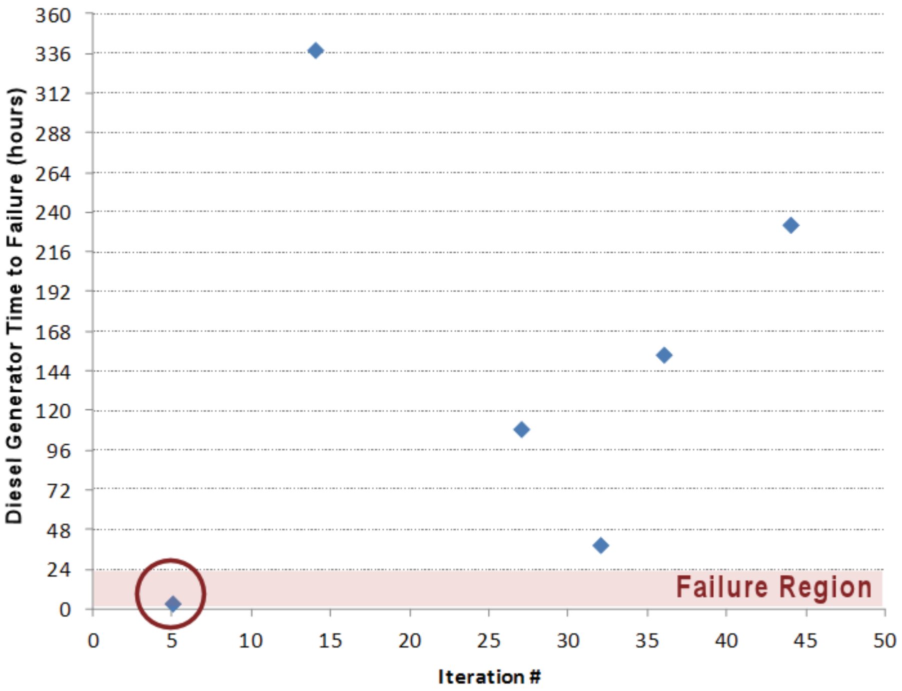


Figure 3-14. Simulation results (50 iterations) for the diesel generators failing to run (or not).

We can now put all of the simulation pieces together to make a coherent picture about all of the scenarios, including those with success events. However, we note that running 50 iterations is not sufficient to provide a very precise quantification result for this (or most any) simulation. Further, we note that only a few trials were calculated for DG_START and DG_RUN, but we could have just as easily simulated 50 iterations of each to have additional statistical results.

In this EDG example, we calculated the results shown in Table 3-2.

Table 3-2. Results of the EDG simulation example.

Scenario (outcome)	**LOOP Term**	**DG_START Term**	**DG_RUN Term**	**Frequency (per year)**
1 (OK)	= 6/50 year	4/6 successes	3/4 successes	(6/50)(4/6)(3/4) = 0.06
2 (CD)	= 6/50 year	4/6 successes	1/4 failures	(6/50)(4/6)(1/4) = 0.02
3 (CD)	= 6/50 year	2/6 failures	n/a	(6/50)(2/6) = 0.04
4 (no LOOP)	= 44/50 year			(44/50) = 0.88

Exploring the simulation data (from the 50 iterations) reveals:

- The frequency of LOOP leading to station blackout (LOOP + EDG failure) giving core damage is 0.06 per year (determined by adding 0.02 to 0.04).

- The frequency of no damage is 0.94 per year.

- The frequency of just LOOP is 0.12 per year, which is slightly higher than what we would expect (it should be 0.1 per year, on average). The difference in this case is the result of statistical variation.

- It is twice as likely, if we see core damage, to have it happen due to the diesels failing to start compared to them failing to run (0.04 versus 0.02).

For the simulation approach, we do not need to perform any special manipulations related to success or failure terms since the simulation **directly traces outcomes** of a process, including success outcomes. Further, one of the optimization designs related to simulation routines is coupled with the fact that most iterations of a simulation routine end in success, consequently the routine may be able to quickly calculate these success end states and then focus more of the scenario computation on other sequences of events.

The scenario generation process must consider a variety of controls, processes, and models, as illustrated in Figure 3-15. Once the scenario specifics are determined, then the scenario generation process interfaces with systems physics codes such as RELAP in order to determine the safety margin based upon the plant physics.

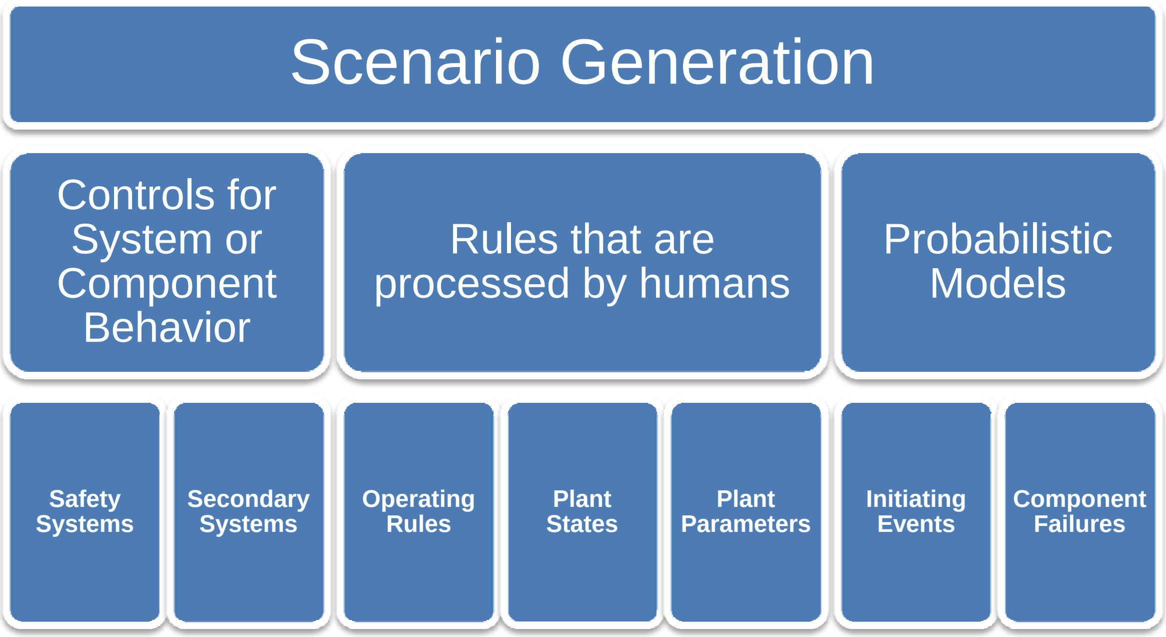


Figure 3-15. Items that are considered during the scenario generation step.

3.5.2 ATR Plant Simulation

The ATR case study modeling uses discrete event simulation to probabilistically create a scenario of a plant's operation. Since the model contains operational data as well as the probability of components failing, it can represent a possible operational outcome. When multiple possible outcomes are analyzed by iterating through the model, then an understanding of the safety margin can be analyzed.

A discrete event simulation maintains an event queue ordered by simulation time. Events are created and entered into the queue. The simulation engine pulls the next event off of the queue and processes that event. During event processing, a simulation time is set, simulation parameter values are changed, simulation object states change, and other events are created and inserted into the event queue. After the event processing is complete, the next event is pulled from the queue and processing continues until the event queue is empty.

For example, using the ATR PRA model described in section 3.3 and evaluating the loss of electrical power initiating event (LOP) over a ten-year period, we simulated 11 LOP events in the queue (see Figure 3-16).

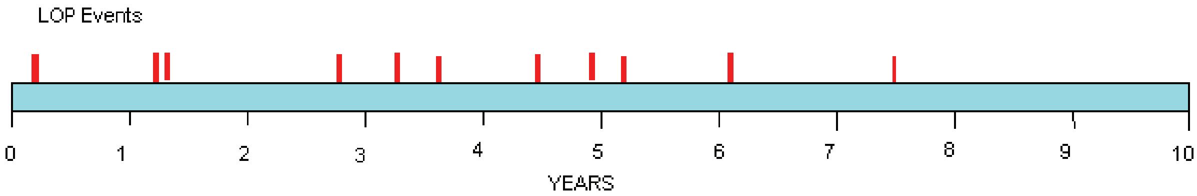


Figure 3-16. Illustration of a discrete event time line of LOP events.

The first event is pulled from the queue and the simulation time advances to 0.2 years. During processing, an event, Loss of Commercial Power (LCP), is added to the queue at 0.2 years and the first event terminates. The LCP event is pulled from the queue and the simulation time remains at 0.2 years. The LCP represents the probability that the loss of power is from loss of commercial power and occurs (based upon historical INL data) about 77% of the time. In this case the LCP event is considered "failed" and the LCP object moves to that state. The next step in the simulation checks the EDGs for operation so the "diesel system event" is placed in the queue at 0.2 years. This type of processing continues until an end state in the evaluation is reached – this indicates that the probabilistic scenario is complete. However, we will not know exactly if fuel damage occurs for this scenario, thus we will create a T-H calculation event that will perform the mechanistic analysis (this is described in the next section).

The processing of an initiating event creates a sequence based on the evaluation results of all of the subsequent created scenarios in that process. During an extended evaluation where the simulation scenario is iterated through many times, unique sequences are generated. For example, we used the ATR case study to simulate 1000 iterations, each 10 years long of simulation time. From this simulation, unique sequences were created from a total of 10,022 LOP events. For each LOP event, we question the failure/success of each safety system using the state table approach described in Section 3.4.

Nuclear plants like ATR are designed to avoid core damage situations. Thus, in order to evaluate the safety margin, an analysis requires a large numbers of initiating events to be simulated. However, one of the advantages of simulation is that we can force a specific type of event to occur – for example if small break loss-of-coolant accidents are of interest, we can simply simulate that event occurring numerous times. As a test, we performed two such evaluations, where 524,700 initiating events (representing loss of electrical power) were evaluated. First we considered cases where just the loss of electrical power is seen, and then we considered the same case but with no backup EDGs. The results are shown in Table 3-3, where we can clearly see that a strategy where the EDGs are not available (or are unreliable) results in a reduction in the safety margin.

Table 3-3. Results of 524,700 conditional ATR initiating event simulations.

Case	Cases where the peak clad temperature exceeds 725 °F	Safety Margin, or the Pr(Load > Capacity)
Loss of electrical power	92	$1.8x10^{-4}$
Loss of electrical power (EDGs are failed)	4,629	$8.8x10^{-3}$

3.6 Mechanistic Plant Physics

This step in the RISMC approach represents the plant physics mechanistically and is performed by systems codes such as the RELAP series. The plant systems-level code will be 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 of the RISMC approach. Because there is a coupling between Steps 4 and 5, they each can impact the other. For example, a calculated high loading (say from a high temperature level) in an SSC may disable a component, thereby impacting an accident scenario.

For the ATR case study, the initial properties used in the RELAP5 input deck for the plant are:

- Reactor power: 230 MW
- Inlet temperature T: 325 K
- Outlet temperature T: 343 K
- Inlet pressure P: 2.66 MPa
- Core delta pressure ΔP: 0.689 MPa
- System flow rate: 3.124 m^3/s

We use these values just as a starting point for scenarios. Upset conditions, such as a transient, changes the plant physics depending on the specifics of the scenario. Ultimately, we track pressures and temperatures through the piping loops at ATR as illustrated in Figure 3-17. Once we are given a scenario (from the PRA simulation), we can then call the RELAP5 code in order to represent the plant's physical phenomena. To couple a scenario to the T-H calculation, we have to customize the T-H code model (or input deck if using a legacy code) specific to the scenario. For example, in Figure 3-18, we show a portion of the input deck that is used by the RELAP5 code. Some of the lines of text in this input deck would need to be customized to each scenario in order to determine, for the simulation, what are the plant responses such as the peak clad temperature.

As an example, we may have a scenario in which one of the pumps fail, for example, emergency coolant pump ECP M-11. In this case, we need to determine how to represent this failure in RELAP5. In the RELAP5 deck, this pump is referenced under the "name" of 435. However, in the ATR PRA, this pump appears under several logic gates including:

- PCS-MDP-1M-M11 – Loss of ECP M-11: 1 minute
- PCS-MDP-30M-M11 – Loss of ECP M-11: 30 minutes
- PCS-MDP-LT-M11 – Loss of ECP M-11: long term
- PCS-MDP-STBY-M11 – Failure of ECP M-11 to start from standby
- DCS-M11-FTS – Emergency primary coolant pump M-11 fails to start due to DCS faults

If the scenario has a failure of this pump, we need to modify the RELAP5 input deck (for this one scenario). The code to change the input deck looks like:

```
0000504  time  0  ge  timeof  505  1800.0  l * start on M-10 failure, 30 min. battery
```

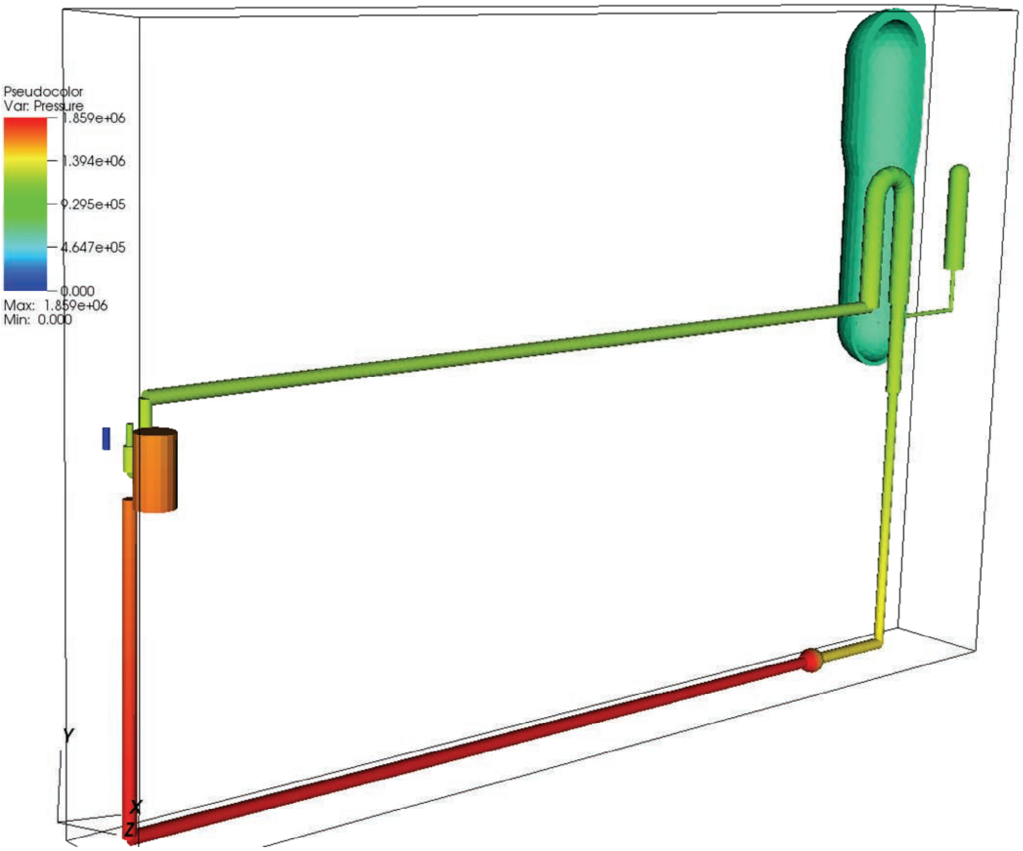


Figure 3-17. Illustration of the flow loop represented by the RELAP5 model for ATR.

```
$======================================================================$
* Emergency Coolant Pump Trips
*
$======================================================================$
0000503 time 0 ge null 0 1.0e6 l * em pmp 425 (M-10)
0000504 time 0 ge null 0 0.0   l * em pmp 435 (M-11)
* start M-11 ECP on low recirculation flow
0000505 cntrlvar 385 lt null 0 90.0 l
* stop M-11 ECP 1800 s after it starts
*0000504 time 0 ge timeof 505 1800.0 l
0000715 -504 and 505 n
$======================================================================$
* Pipe Break Trip *
$======================================================================$
0000507 time 0 ge null 0 1.0e6 l
$======================================================================$
```

Figure 3-18. Example of the parameters found in a typical RELAP5 input deck.

To run the scenario where pump ECP M-11 fails, we would insert the applicable RELAP5 line into the ATR input deck, and then call the RELAP5 code to run and produce the pressure, flow, and temperature output. We have determined the needed modifications for the components of interest (see Figure 1-4) in the RELAP5 input deck and their ties to the PRA. These ties are shown in Table 3-4.

The T-H model in RELAP is a representation of the physical properties of a plant. For each simulation iteration, we generate scenarios which are organized into a relational database with a table containing the RELAP5 inputs identified by its unique number and a second table containing the relationship between the PRA basic events and gates. Thus, when a component fails in the simulation (as described in the previous section) a RELAP5 input is also generated that mimics the failure. During the simulation run, any of the special events or gates identified that fail are saved along with the initiating event. Post processing of all of these events produces the final RELAP5 input deck for any one scenario.

Once all the iterations of the simulation have been completed, the results of the simulation are stored and the interface files to RELAP5 are generated. During the generation of the files, each of the initiating events from all the iterations of the simulation is examined and the sequence of RELAP5 inputs (or cards) that would be generated by the failures of each initiating event is generated.

Since we have the original ATR PRA, we are able to compare a scenario from the PRA against the same scenario as evaluated via RELAP5 to see if they both have the same outcome such as fuel damage. Generally we would expect that fuel damage scenarios from the PRA would also result in fuel damage from the RELAP5 calculation (i.e., peak clad temperature > 725°F). Further, we would expect “ok” scenarios from the PRA to not see elevated temperatures during the transient. However, it may be possible that discrepancies exist.

For the RELAP5 calculations, the type of results that are produced is shown in Figure 3-19. In this case, we simulated an “ok” scenario where we had a small break loss-of-coolant transient, but emergency pumps (and other systems) were available.

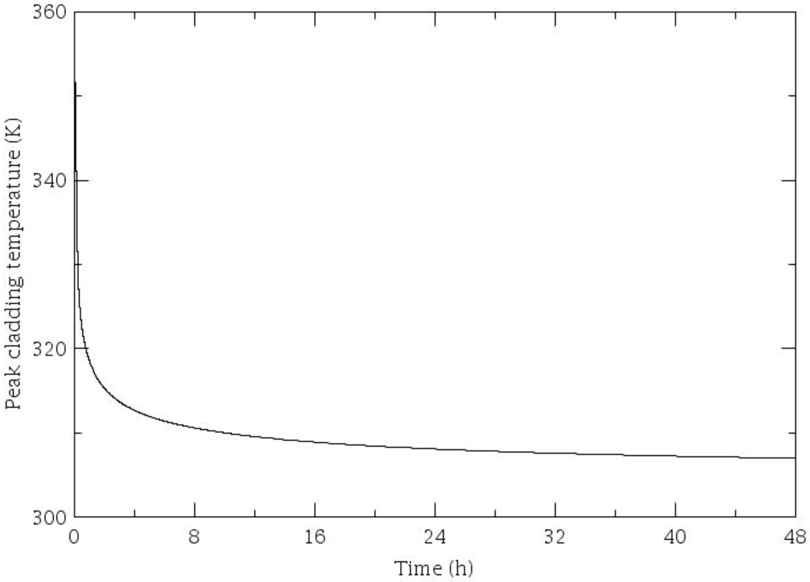


Figure 3-19. Peak clad temperature during a small break loss-of-coolant transient when safety systems are available.

Table 3-4. Mapping of components to the RELAP5 and PRA events and gates.

Component	RELAP 5 Name	PRA Basic Event or Gate
Emergency Coolant Pump	425	PCS-MDP-LT-M10, PCS-MDP-30M-M10, PCS-MDP-1M-M10, PCS-MDP-STBY-M10, DCS-M10-FTR, DCS-M10-FTS
	435	PCS-MDP-1M-M11, PCS-MDP-30M-M11, PCS-MDP-LT-M11, PCS-MDP-STBY-M11, DCS-M11-FTS
ECP Discharge Check Valve	429	PCS-CKV-FO-00CK1A17-0000
	439	PCS-CKV-FO-00CK1A20-0000
Primary coolant system (PCS) pump	145	PCS-MDP-1M-M-6, PCS-MDP-30M-M-6, PCS-MDP-LT-M-6
	155	PCS-MDP-1M-M-7, PCS-MDP-30M-M-7, PCS-MDP-LT-M-7
	165	PCS-MDP-1M-M-8, PCS-MDP-30M-M-8, PCS-MDP-LT-M-8
	175	PCS-MDP-1M-M-9, PCS-MDP-30M-M-9, PCS-MDP-LT-M-9
PCS Discharge Check Valve	149	PCS-MOV-SC-000GT1A3-0000, PCS-MOV-SC-000GT1A3-0001, PCS-MOV-SC-000GT1A3-0030
	159	PCS-MOV-SC-000GT1A6-0000, PCS-MOV-SC-000GT1A6-0001, PCS-MOV-SC-000GT1A6-0030
	169	PCS-MOV-SC-000GT1A9-0000, PCS-MOV-SC-000GT1A9-0001, PCS-MOV-SC-000GT1A9-0030
	179	PCS-MOV-SC-00GT1A12-0000, PCS-MOV-SC-00GT1A12-0001, PCS-MOV-SC-00GT1A12-0030
Secondary Coolant Sys Pumps	325	SCS, SCS-DG, UCW-SCS, UCW-SCS-SBK
Safety Relief Valve	805	PCS-SRV-FC-000SFA71-0000 (fails to close when needed)
		PCS-SRV-FO-000SFA71-0000 (fails to open when needed)
	805	PCS-SRV-FC-000SFA72-0000 (fails to close when needed)
		PCS-SRV-FO-000SFA72-0000 (fails to open when needed)
Rx Vessel Vent Valve	815	PCS-AOV-FO-000GB231-0000, PCS-SOV-CA-0GB231&2-0000
Pressurizing Pump	511	DCS-FCV-1-8A-FO-12, DCS-M14-FTS, DCS-M14-PT-01-19, DCS-M14-FTS, DCS-M14-PT-01-19, PCS-MDP-1M-M14, PCS-MDP-30M-M14, PCS-MDP-LT-M14, PCS-MDP-MLXI-M14, PCS-MDP-STBY-M14
	516	DCS-FCV-1-8A-FO-19, DCS-M15-FTS, DCS-M15-PT-01-19, DCS-M15-FTS, DCS-M15-PT-01-19, PCS-MDP-1M-M15, PCS-MDP-30M-M15, PCS-MDP-LT-M15, PCS-MDP-MLXI-M15, PCS-MDP-STBY-M15
EFIS (bottom head)	532	EISNF200ALL, EISNF100T, EISNF100S, EISNF100L, FWS-RXBH
EFIS (upper vessel)	572	EISNF101, FWS-RXUV

One of the ideas we considered for this case study but did not implement is the idea of physics emulators for the T-H. A T-H emulator is a computer program that is “trained” using T-H code runs (knowing both the specific scenario inputs and the plant phenomena that results) and is then able (with some uncertainty) to produce plant phenomena (e.g., temperature, as seen in Figure 3-20) very rapidly for many related but different scenarios. The benefit of a T-H emulator is to allow for a large number of scenarios to be evaluated while minimizing the computational expense.

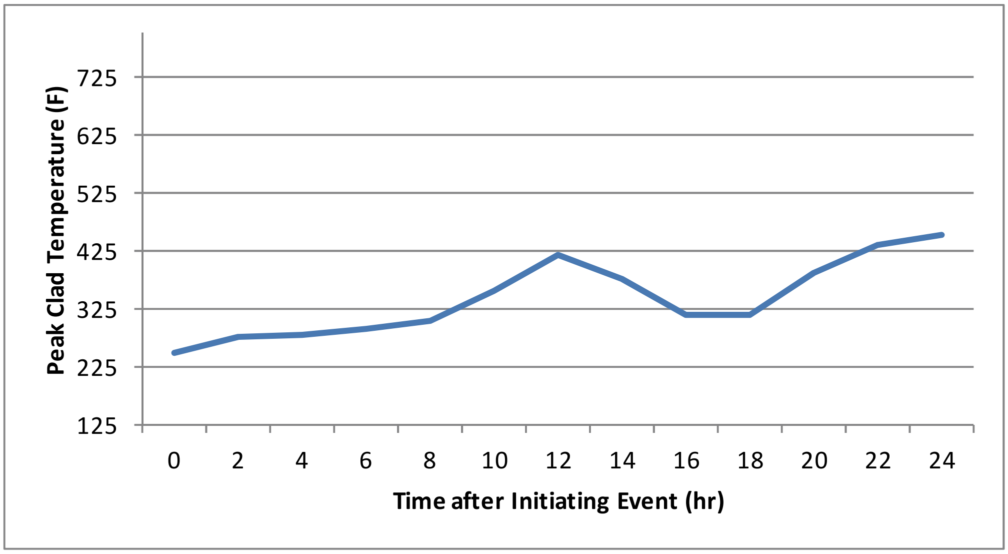


Figure 3-20. Peak clad temperature as predicted by a T-H emulator.

3.7 Safety Margin and Uncertainty Quantification

The purpose of this step is to construct and quantify the probabilistic load and capacity distributions using the information generated from the previous steps in the RISMC approach. Once the load and capacity information is known, it is possible to then determine the probabilistic safety margin.

It should be noted that while the focus of this study was on a safety margin determination, other considerations are generally a part of decision making for complex issues. For example, the types of performance measures that may be evaluated for decisions related to long-term operations of NPPs are shown in Figure 3-21 (where the safety margin performance measure is highlighted). The point of these multi-dimensional decision criteria is that safety is not the only factor that has to be considered, but for the ATR case study it was the sole focus of our evaluation.

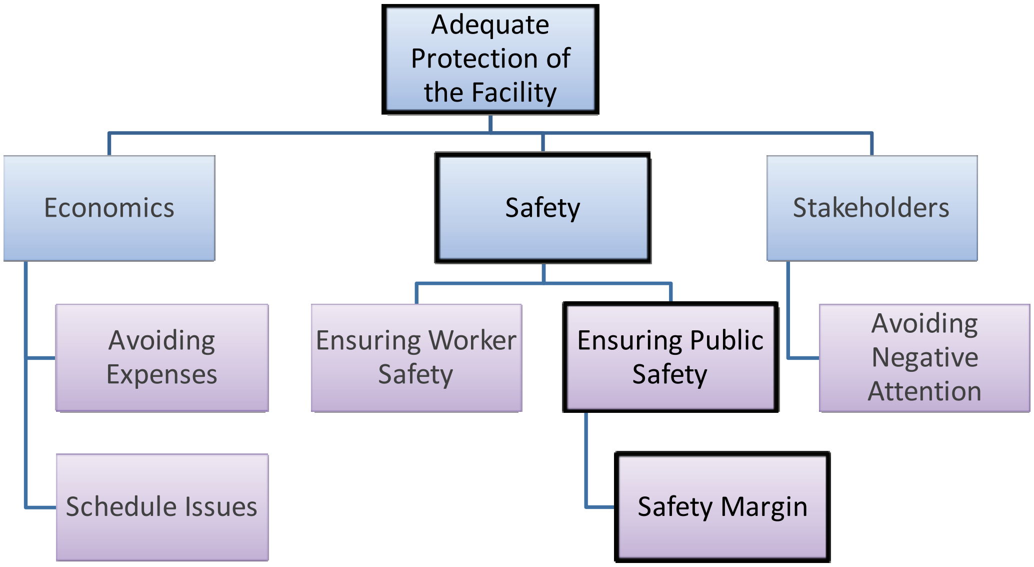


Figure 3-21. Types of decision performance measures typically considered.

3.7.1 Safety Margins

Recall that we initially proposed three alternative cases:

I. Keep the emergency power system as is (an EDG running, one in standby, commercial power as backup).

II. Redundant commercial power as primary backup, single new EDG as backup.

III. Redundant commercial power as primary backup, existing EDGs as backup.

For this step in the RISMC analysis, we need to gather the results of the integrated probabilistic (scenarios, specifically the risk analysis) and mechanistic (physics, specifically the T-H) calculations and determine the safety margin for each alternative. For the ATR case study, the safety margin was given by the number of simulations where the peak clad temperature exceeds 725 °F – in other words any simulation case that results in fuel damage is defined as having "depleted" the safety margin. Since this safety margin is a quantitative value (and is a probability) the following attributes of the margin are evident:

- A safety margin of 1.0 would indicate that a particular strategy would *always* result in fuel damage. The value of 1.0 is an absolute (and unrealistic) upper bound on the safety margin calculation.

- A safety margin of 0.0 would indicate that a particular strategy would *never* result in fuel damage. The value of 0.0 is an absolute lower-bound on the safety margin calculation.

- Lower values of the safety margin metric are preferred over higher values.

After evaluating the proposed Margin Management Strategies, the results will indicate which of the associated safety margins are most preferential. For example, the results may be displayed as illustrated in Figure 3-22. In this figure, we see that Case III would be preferred over the other two strategies when using safety as the sole decision factor.

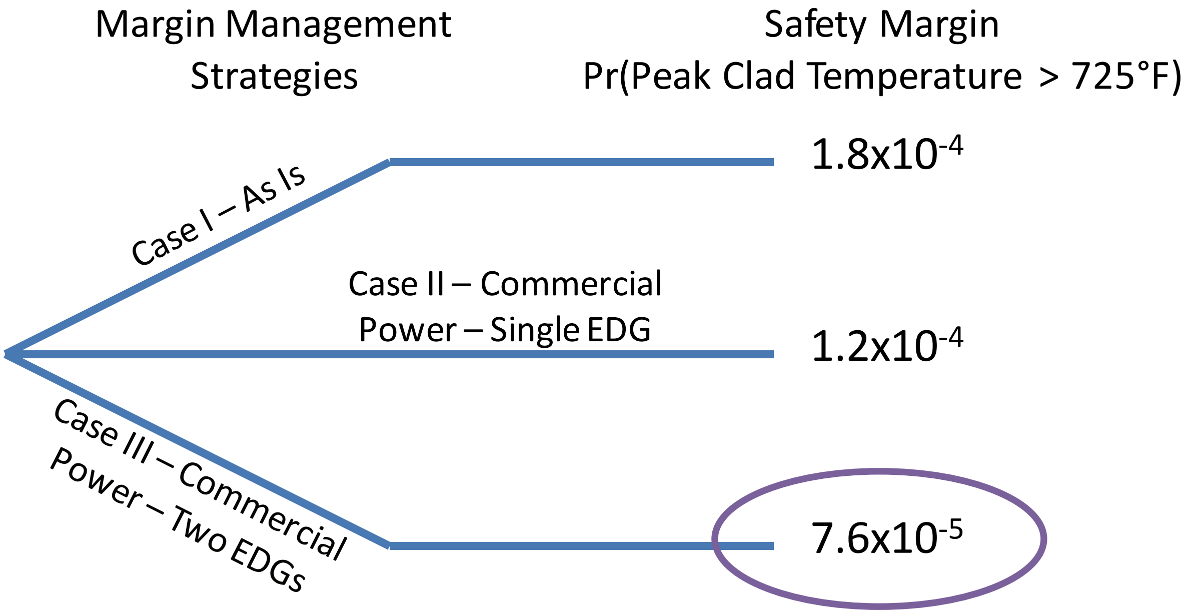


Figure 3-22. Notional safety margin results for the three Margin Management Strategies.

Once we have an integrated risk-informed safety margin model with both probabilistic and mechanistic aspects, we have the ability to vary factors (such as core power) in order to see if our decisions change. For example, we illustrate a hypothetical case in Figure 3-23, where we see that the preferred Margin Management Strategy might change depending on specifics of the plant. In this example, we see that if we increase the ATR core power to its maximum (250 MW) then it is possible that Case III is preferred over Case II, depending on the reliability of commercial power. Further, if it becomes known that the reliability of commercial offsite power is somewhat unreliable (availability of less than 0.8) then the Case I strategy may be preferential, depending on the ATR core power level.

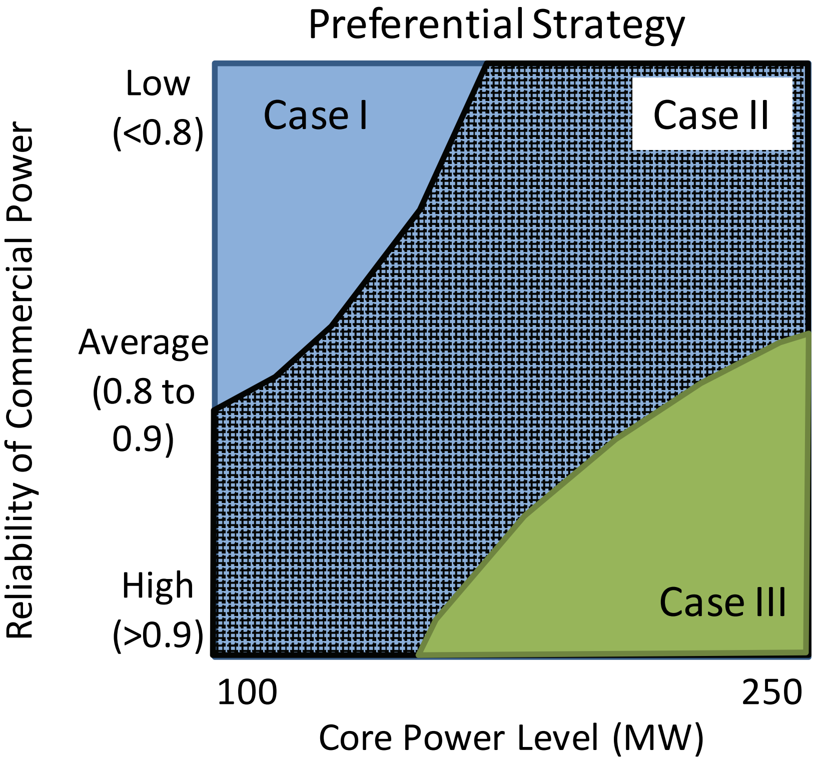


Figure 3-23. Example of decision preferences when key plant factors change.

In addition to the safety margin values that are calculated, we have available for each simulation scenario the frequency and consequences associated with that scenario. This allows us to determine the *characteristics* of the safety margin. For example, in Figure 3-24, we show a notional case where most of the scenarios for Case III have low frequency (in the "green" region on the frequency axis[b]) and have low consequences (have low peak clad temperature). However, some scenarios exceed the fuel damage temperature limit and some scenarios get close to the "green/white" frequency threshold. This type of consequence-frequency information is useful in order to determine situations when a safety margin might be relatively low (compared to other alternatives) but where the risk-information is near either (or both) a consequence or frequency edge. While the degree of "closeness" to these edges can be quantified, we did not perform this calculation for this case study but will investigate this approach in a future case study.

[b] Note that we show the frequency limits as described in the NRC Inspection Manual Chapter 0609, the Significance Determination Process. The ATR is considering use of these limits in risk-informed applications.

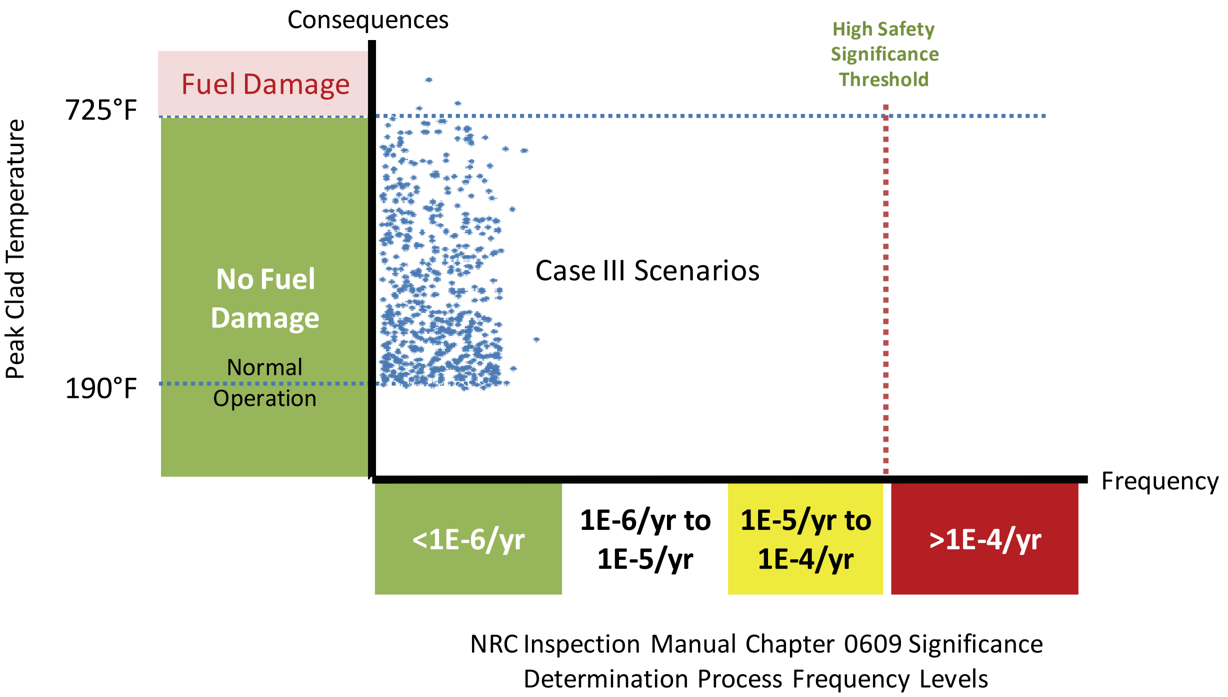


Figure 3-24. Frequency and consequence results showing probabilistic nature of risk-informed scenarios.

3.7.2 Uncertainty Determination

As part of the ATR case study, we used the uncertainty analysis code DAKOTA as a test to capture uncertainty related to the probabilistic and mechanistic calculations. An example of a DAKOTA analysis using a pressurizer failure scenario with different levels of uncertainty (either treating 6 or 21 uncertainty parameters) is shown in Figure 3-25. Ultimately, we would need to consider the uncertainty on the results presented in the previous section during actual plant decisions.

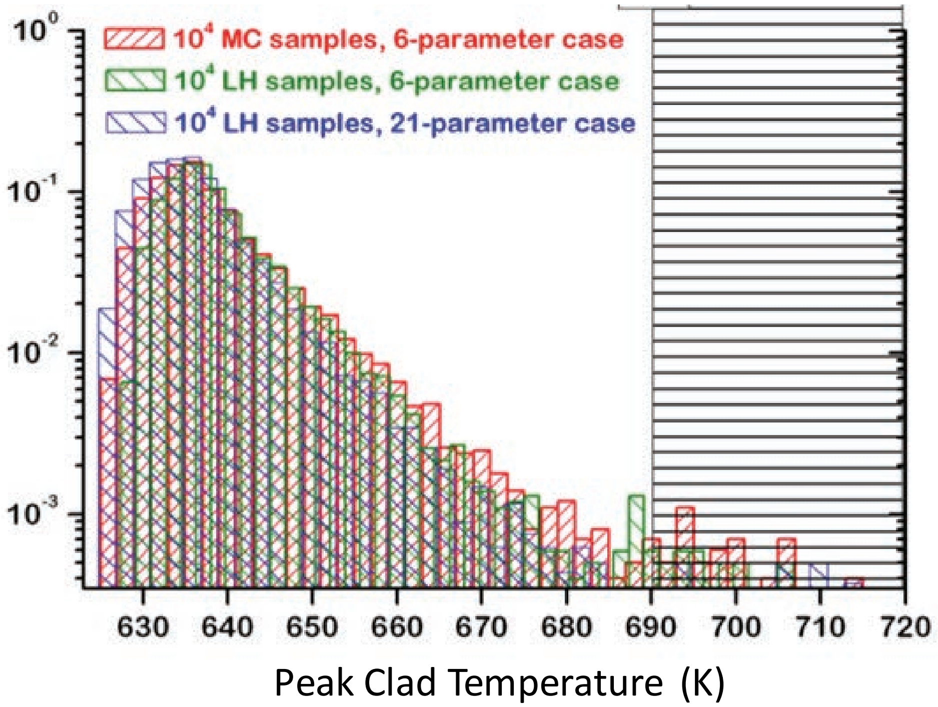


Figure 3-25. Example in the variation of peak clad temperature during uncertainty analysis.

3.8 Uncharacterized Risks

This step is used to 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 analysis protocols of "good engineering practices" to augment analysis. For example, uncertainties on the model being used (both the probabilistic and mechanistic models) should be considered. For this initial case study, we did not formally consider model uncertainty. Later applications will consider these and other uncharacterized risks.

4. CONCLUSIONS

The INL has carried out a demonstration of the RISMC approach using the ATR as a case study. We defined and described the eight steps of the approach, presenting a variety of methods, models, and results for each. We showed how traditional PRA and T-H quantification can be used and extended into the realm of safety margin characterization in order to improve NPP safety, reliability, and economics.

During the R&D for the ATR case study, a variety of issues and "lessons learned" were encountered. Technical issues included such items as how to represent dependent failures in a simulation framework; how to automate legacy codes such as RELAP5; how to integrate probabilistic and mechanistic modeling; and how to support NPP decision making with these integrated models. While several research areas were explored and improvements made, there still exists issues to be solved in future case studies. Two key issues awaiting resolution are:

1. An advance set of analysis tools is needed in order to streamline and enhance the RISMC approach that has been described. While the INL has created an approach based upon extending legacy codes, this application set has limitations and did not allow us to fully explore the case study. A new set of tailored analysis tools created using modern software and computers will empower future decision makers.

2. A method of simulating human performance as part of NPP scenarios needs to be implemented. While the ATR PRA has used the NRC sponsored SPAR-H (Gertman, Blackman, Marble, Byers, & Smith, 2005) approach to operator action quantification, these events did not play a significant role in the case study scenarios. Consequently, we did not explore how to fully extend this model into a simulation framework.

The work on the ATR case study has pointed to several additional areas of potentially fruitful R&D related to risk-informed margin management. For example, the current NRC Significance Determination Process is focused on CDF as the primary decision metric. We have showed how the concept of safety margin provided additional information, both from a quantitative aspect but more importantly from an engineering physics understanding. Further, additional applications (beyond Margins Management Strategies) are possible including NPP risk monitor enhancements; a general decision support capability for operational decisions; and an integrated and holistic framework to account for aging effects during the NPP lifetime.

Several successful outcomes have resulted from performing the ATR case study. The RISMC approach:

- Provides to decision makers the safety case (in this case, specific to the case study) in order to select operational alternatives as part of Margin Management activities.

- Develops a significantly improved plant physics approach wherein we can couple, in an automated fashion, to mechanistic codes such as RELAP. By developing this integrated strategy where probabilistic scenarios "talk" to plant physics calculations, we are able to run scenarios for numerous configurations and initiating events that could affect ATR. Previously, the number of mechanistic code calculations (as performed by RELAP5) was limited and hand-crafted for specific issues.

- Greatly improves the U.S. risk-analysis capabilities by creating a unique suite of simulation methods that builds upon traditional PRA approaches. INL has developed a method that can automatically transfer the investment made in existing PRA models (which exist for every NPP in the U.S.) into a dynamic simulation-type of model. Once these models are recast as dynamic time-dependent models, more realistic quantification approaches are possible for aspects such at T-H, component aging, dependent failures, and operator actions.

- Replaces traditional static fault- and event-tree models by merging NPP scenario simulation with improved plant physics to determine outcomes of key physical process variables. For each initiating event and scenario, we are able to track processes internal to ATR such as peak clad temperature, flow rates, and pressures. We used these processes to make a determination as to “failure” events which accounts for the possibility of damage to fuel in the reactor core.

The approach and lessons learned from this case study will be included in future Technical Basis Guides. These guides will be the mechanism for developing the specifications for RISMC tools and for defining how plant decision makers should propose and evaluate margin recovery strategies.

5. REFERENCES

Bishop, P., & Bloomfield, R. (1998). A Methodology for Safety Case Development. *Safety-Critical Systems Symposium.* Birmingham, UK.

Duckwitz, N. (2011). *10 CFR 830 Major Modification Determination for ATR Diesel Bus (E-3) and Switchgear Replacment.* INL.

Gaston, D., Hansen, G., & Newman, C. (2009). MOOSE: A Parallel Computational Framework for Couples Systems for Nonlinear Equations. *International Conference on Mathematics, Computational Methods, and Reactor Physics.* Saratoga Springs, NY: American Nuclear Society.

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.

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

Sherry, R., & Gabor, J. (2011). Risk Informed Safety Margin Characterization: Trial Application to a Loss of Feedwater Event. *PSA 2011.* Wilmington, NC.

Wikipedia. (n.d.). *Advanced Test Reactor.* Retrieved August 2012, from http://en.wikipedia.org/wiki/Advanced_Test_Reactor

Zio, E. (2009). Reliability engineering: Old problems and new challenges. *Reliability Engineering and System Safety* , 125-141.

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 novel methodology to generate a dynamic model from the static PRA models of a well established code called 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

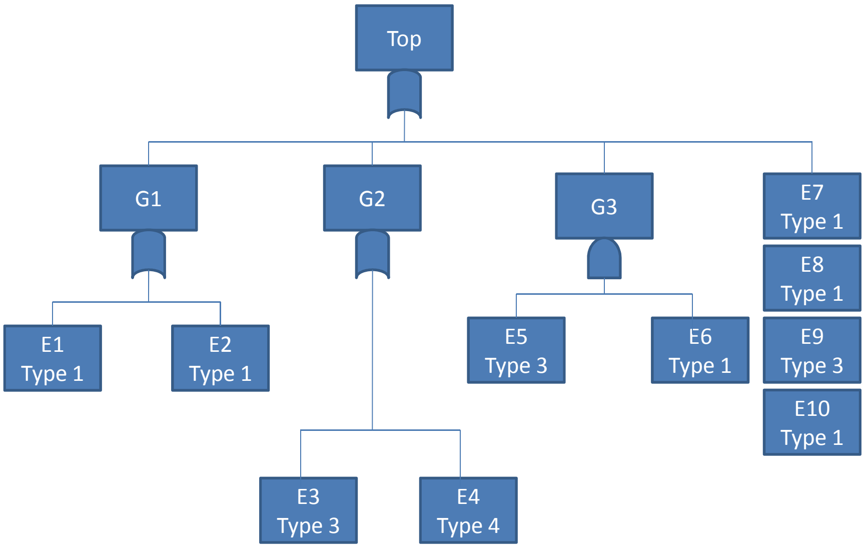
Key to the success of using the dynamic modeling approach defined above will be the automatic generation of a dynamic model from the well established and validated static models. The following concepts were discussed as a way to accomplish the model transition.

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

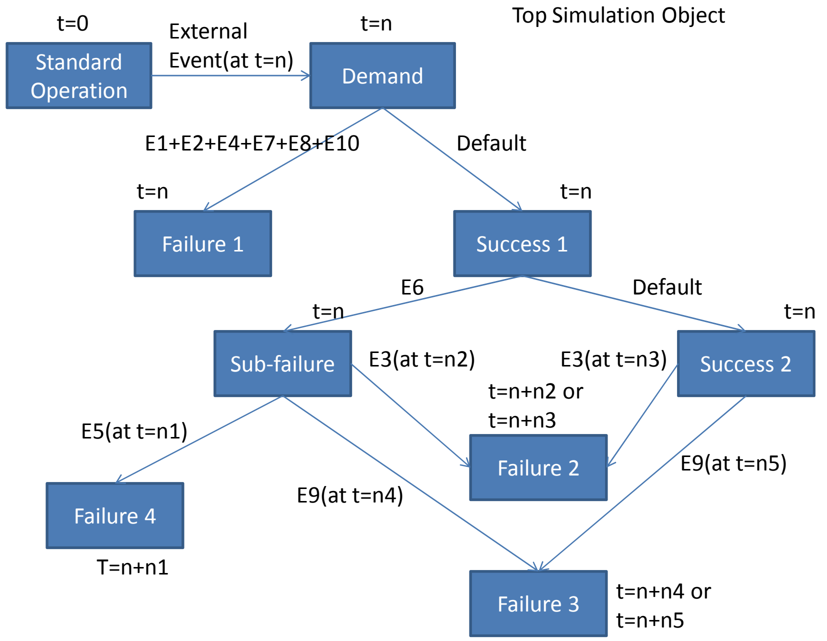
probability of occurrence, all other events will be collapsed into a single state and event for that transition.

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 following diagrams help illustrate the model transition described above.



Simplified SAPHIRE Fault Tree

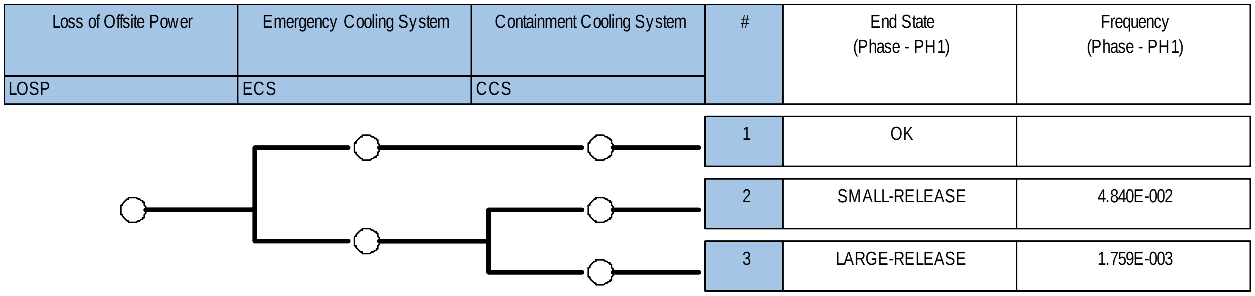


Simplified Collapsed Dynamic State Model

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-1) 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.



Loss of Offsite Power	Emergency Cooling System	Containment Cooling System	#	End State (Phase - PH1)	Frequency (Phase - PH1)
LOSP	ECS	CCS			
			1	OK	
			2	SMALL-RELEASE	4.840E-002
			3	LARGE-RELEASE	1.759E-003

Figure A-1. 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-2Figure A-2. 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-3 and Figure A-4). We use a random number generation method to simulate complex-events to determine the next simulation state.

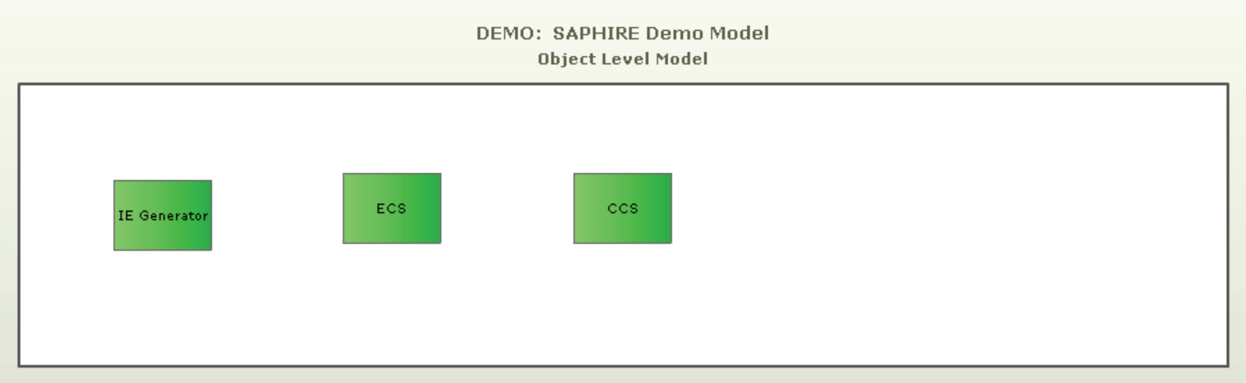
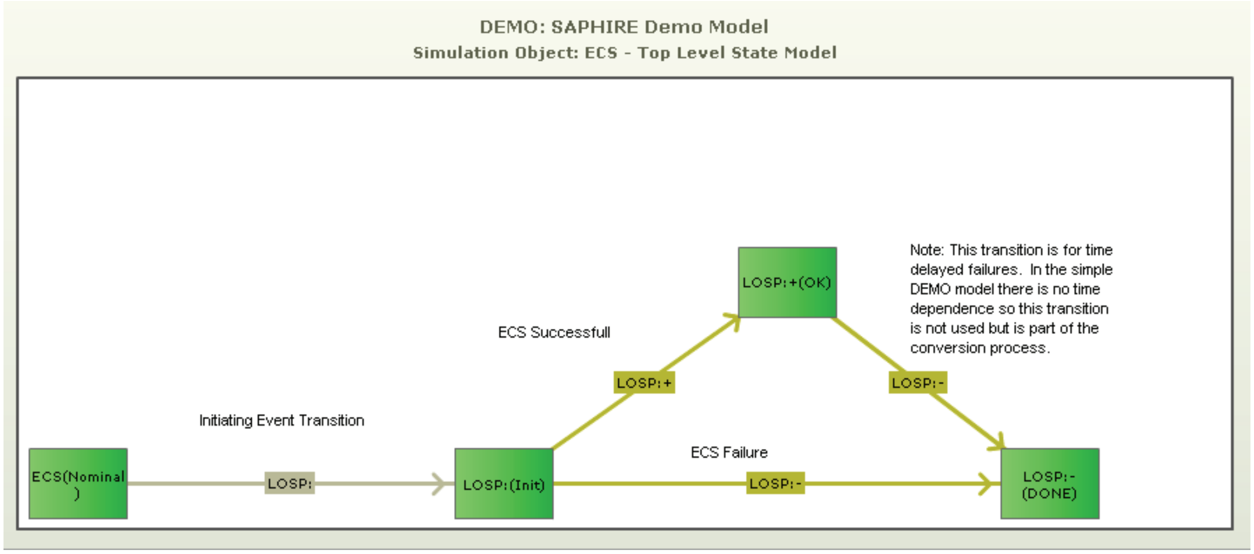


Figure A-2. Simulation model objects as seen in the browser window.



Note: This transition is for time delayed failures. In the simple DEMO model there is no time dependence so this transition is not used but is part of the conversion process.

Figure A-3. The simulation state and transition model for ECS.

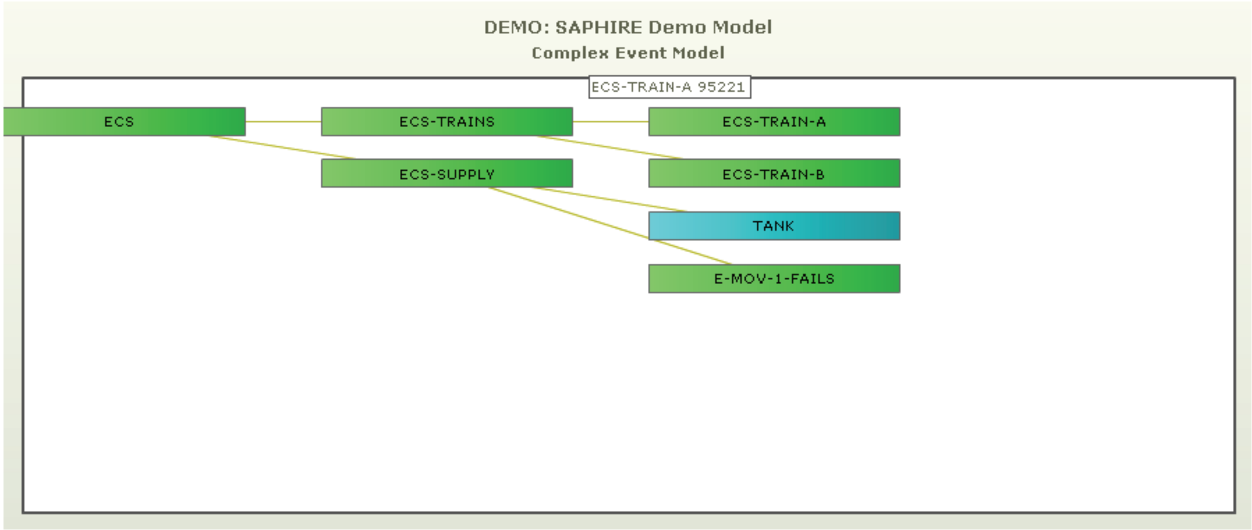


Figure A-4. The simulation complex-event model for ECS down to the basic event level (partial view).

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-1 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:

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

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

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

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.

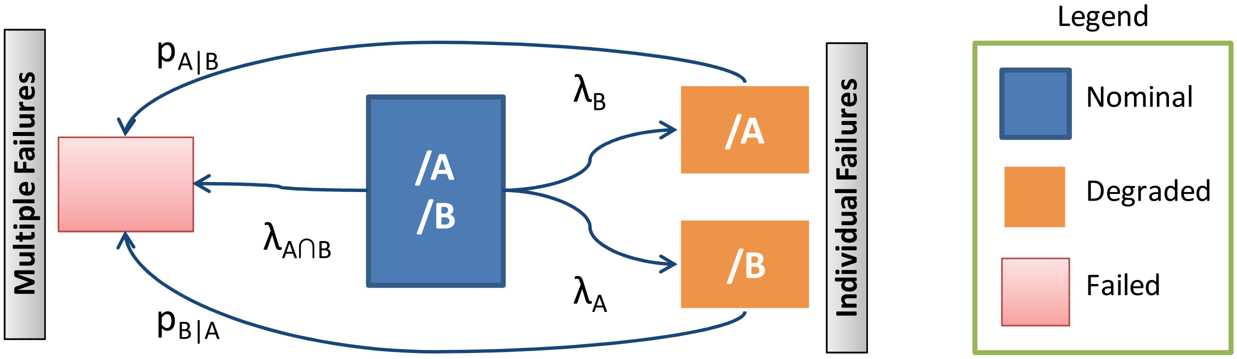


Figure B-1. Illustration of the success, degraded, and failure states of a two-train system.

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 $\lambda_A = \lambda_B = \lambda_1 = 4.9E\text{-}5/hr$. 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):

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

The conditional probability is then:

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

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

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

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-5/hr + 1.1E-5/hr = 6.0E-5/hr .

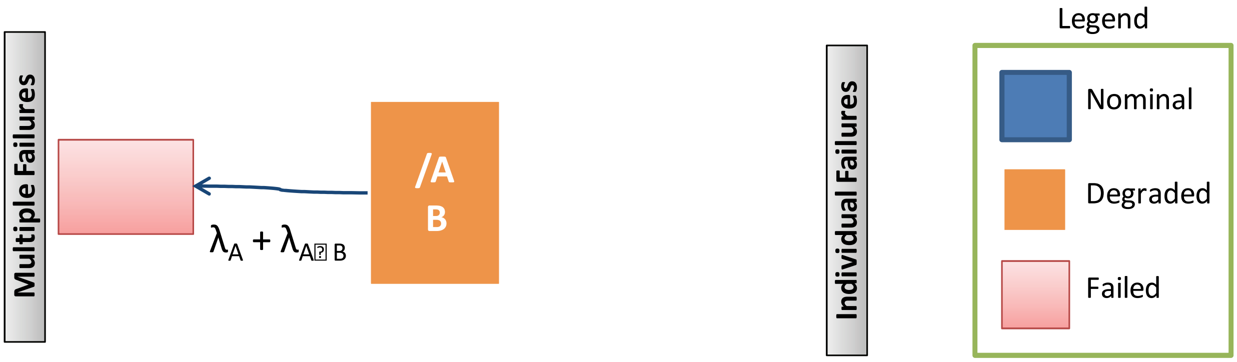


Figure B-2. Illustration of the degraded and failure states of a two-train system when EDG B is failed.