# Risk Informed Margins Management as part of Risk Informed Safety Margin Characterization

**Curtis Smith**[a]
[a] Idaho National Laboratory, Idaho Falls, USA

---

**Abstract:** The ability to better characterize and quantify safety margin is important to improved decision making about Light Water Reactor (LWR) design, operation, and plant life extension. A systematic approach to characterization of safety margins 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 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 needs and opportunities to better optimize plant safety and performance will become known. To support decision making related to economics, readability, and safety, the Risk Informed Safety Margin Characterization (RISMC) Pathway provides methods and tools that enable mitigation options known as risk informed margins management (RIMM) strategies.

The purpose of the RISMC Pathway is to support plant decisions for RIMM with the aim to improve economics, reliability, and sustain safety of current NPPs over periods of extended plant operations. The goals of the RISMC Pathway are twofold:

1. Develop and demonstrate a risk-assessment method that is coupled to safety margin quantification that can be used by NPP decision makers as part of risk-informed margin management strategies.
2. Create an advanced RISMC Toolkit that enables more accurate representation of NPP safety margins.

The methods and tools provided by RISMC are essential to a comprehensive and integrated RIMM approach that supports effective preservation of margin for both active and passive SSCs. We discuss the methods and technologies behind RIMM in this paper.

**Keywords:** Safety Margin, Margin Management, RISMC, simulation.

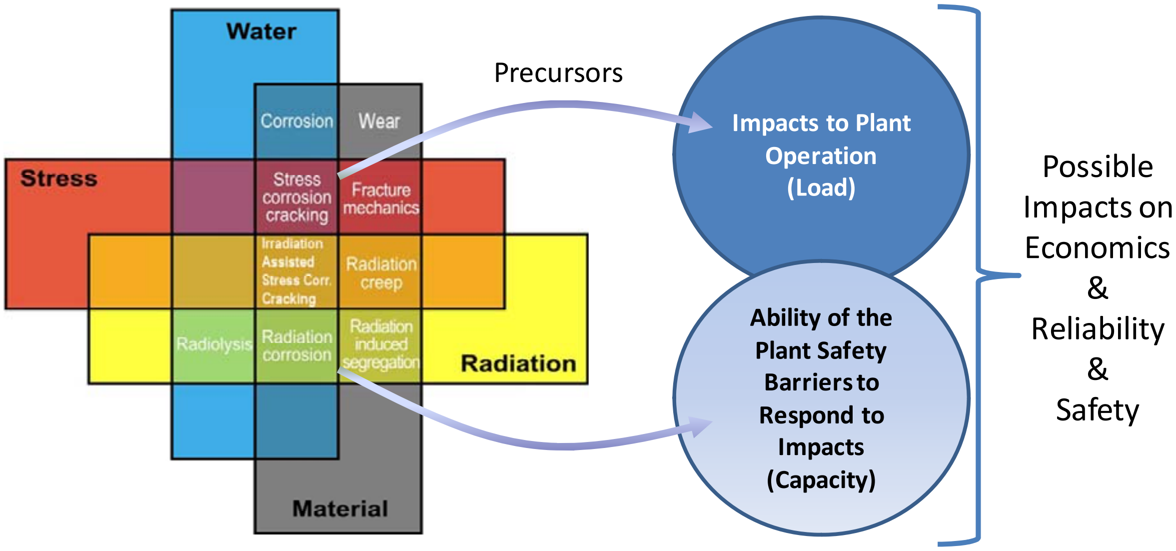
---

## 1. INTRODUCTION

The purpose of the Risk-Informed Safety Margin Characterization (RISMC) Pathway is to support plant decisions for risk-informed margins management, with the aim to improve economics and reliability and sustain safety of current nuclear power plants. The 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 nuclear power plant decision makers as part of their margin recovery strategies; and (2) create an advanced RISMC toolkit that enables a more accurate representation of a nuclear power plant safety margin. In order to carry out the research and development needed for the RISMC Pathway, the Idaho National Laboratory (INL) is performing a series of case studies that will explore methods and tools-development issues. A completed initial case study focused on demonstrating the RISMC approach using the Advanced Test Reactor (ATR). As part of the demonstration discussed in this article, we describe how thermal-hydraulics and probabilistic safety calculations are integrated and used to quantify margin recovery strategies as a part of Risk Informed Margins Management (RIMM).

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 the characterization of safety margin and the subsequent margin management represents a vital input to the licensee and regulatory analysis and decision making that will be involved. In addition, as research and development in the LWRS Program and other collaborative efforts yield new scientific understanding of aging and degradation, opportunities to better optimize plant safety and performance will become known. This interaction of degradation understanding and potential impacts to plant margins are shown in Figure 1.

**Figure 1: Representation of the Interaction of Degradation Mechanisms That May Impact Plant Operations and Safety Barriers If Left Unmitigated**



## 2. CASE STUDY USING THE ADVANCED TEST REACTOR

Constructed in 1967, ATR is a pressurized water test reactor that operates at low pressure and low temperature. It is located at the Advanced Test Reactor Complex on the INL site. The reactor is pressurized and is cooled with water. The reactor vessel is a 12-ft diameter cylinder, 36-ft high, and is made of stainless steel. The reactor core is 4 ft 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.

As part of the RISMC demonstration, we successfully coupled the risk assessment simulation to the thermal-hydraulics analysis (using RELAP5) in order to integrate probabilistic elements with mechanistic calculations. With the knowledge of plant response, we needed to determine whether or not a particular outcome is "success" (meaning no fuel damage) or "failure" (meaning fuel damage). For our analysis, we assumed that any event that saw a peak cladding temperature of 725°F (658 K) was a fuel damage outcome.

In general, margin management strategies are proposed alternatives (i.e., changes to system, structures, components, or plant procedures) that work to control margin changes due to aging or plant modifications. Alternatives that off-set, or mitigate, reductions in the safety margin are known as margin *recovery* strategies.

It is intended that RIMM will support a variety of safety margin decisions, including recovery of or increasing safety margins:

- If core power levels are increased
- If a different type of fuel or clad is introduced
- If aging phenomena becomes more active over long periods of plant operation

- If advanced control systems provide additional or new information during normal and off-normal plant operation
- If plant modifications are taken to increase resiliency for hazards such as flooding and seismic events
- If systems, structures, or components are degraded or failed
- If under accident conditions, supporting severe accident guidelines

As can be seen by the possible applications above, the RISMC Pathway has a role in integrating other domains (e.g., aging, advanced control systems, hazards analysis) into a single coherent framework that will support RIMM.

The purpose of the RISMC ATR case study is to demonstrate the RISMC approach using realistic plant information, including both real probabilistic risk assessment (PRA) and thermal-hydraulics models. As part of this case study, we evaluated emergency diesel generator issues. Historically, ATR has had a continually running emergency diesel generator as a backup power supply, which is different than all commercial nuclear power plants in the United States (commercial plants have their emergency diesel generators in standby). Margin recovery strategies under consideration include the following:

- Keep the emergency power system as is (emergency diesel generator running, one in standby, and commercial power as backup)
- Redundant commercial power as primary backup, single new emergency diesel generator as backup
- Redundant commercial power as primary backup, two existing emergency diesel generators as backup.

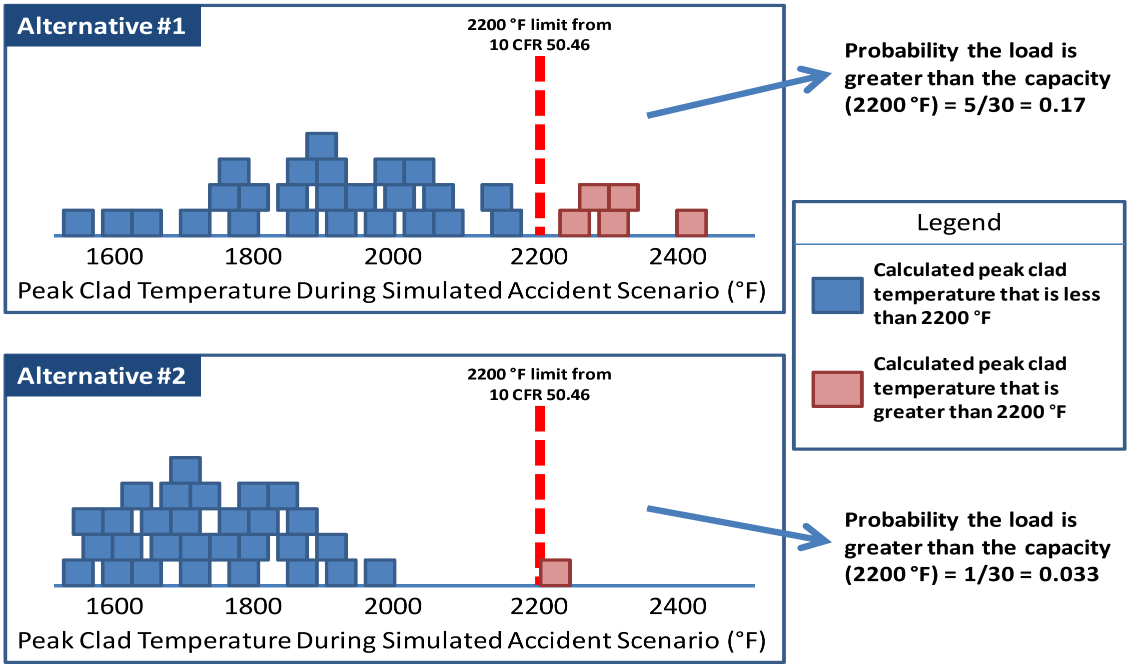
For the different strategies, we simulate the plant behavior both probabilistically and mechanistically. To perform this simulation, we used the existing PRA and thermal-hydraulics information (e.g., SAPHIRE probabilities, RELAP5 input). We then defined the simulation for different scenarios and different strategies and ran a large number of iterations to determine overall safety margins.

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) is estimated using static fault and event-tree models. However, we do not know how close (or beyond) we are to physical safety limits (say peak clad temperature) for most accident sequences described in the PRA. Further, as found in other research [1], 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 we are (or not) to this event and how might we improve our safety margin through margin recovery strategies.

In general, a probabilistic margin is defined by the probability that a “loading condition” exceeds a capacity to respond to that condition. 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 $\Pr[f(L) > f(C)]$. Thus, 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.

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. For this example, we suppose that a nuclear power plant has two alternatives to consider: (1) retain an existing, but aging, component as-is, or (2) replace the aging component with a new one. We run 30 simulations and calculate the outcome of a safety metric (e.g., peak clad temperature) and compare that against a capacity limit (assumed to be 2200°F in this example). The results of these simulations are then used to determine the probabilistic margin:

**Figure 2: Simulating Outcomes for Different Alternatives to Determine Safety Margin**



Probability the load is greater than the capacity (2200 °F) = 5/30 = 0.17

Probability the load is greater than the capacity (2200 °F) = 1/30 = 0.033

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 boxes shown in Figure 3 (representing the peak clad temperature for each scenario) and the "capacity" is the 10 CFR 50.46 limit of 2200°F. If the safety margin were the only decision factor, then Alternative #2 would be preferred (its safety characteristics are better) because we only realized one case where we exceeded our 2200°F safety limit. It should be noted that while the focus of the ATR case study was on a safety margin determination, other considerations (e.g., cost and schedule) are generally a part of decision making for complex issues.

The mechanics to conduct margins analysis, including a methodology for carrying out simulation-based studies of safety margin, are given in the following RISMC-specific process steps:

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.
3. Determine issue-specific, risk-based scenarios and accident timelines.
4. Represent plant operation probabilistically using the scenarios identified in Step 3. Because numerous scenarios will be generated, the plant and operator behavior cannot be manually created a priori like in current risk assessment using event and fault trees. In addition to the expected operator behavior, 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.
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, 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 recovery strategies.

For the ATR case study, a probabilistic simulation model used for Steps 3 and 4 was created based on the ATR PRA. As part of the research and development, we developed an approach to automatically create a dynamic simulation model using an existing static-based PRA as a starting point. From this, we used an event simulation tool, where the model consists of simulation objects that transition through various states to describe a plant response scenario to an off-normal condition. Using the simulation approach, we do not need to perform any special manipulations related to success or failure terms because the simulation directly traces outcomes of a process, including success outcomes. For example, using the ATR PRA model and evaluating the loss-of-electrical-power initiating event over a 10-year period, we simulated 11 loss-of-electrical-power events in the queue.

The first event is pulled from the queue and the simulation time advances to 0.2 years. During processing for the loss-of-electrical-power occurrence, other questions are resolved such as the plant response to the loss-of-electrical-power. For example, one step in the simulation checks the electric diesel generators for operation; therefore, 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 if fuel damage occurs for this scenario; therefore, we create a thermal-hydraulics calculation event that will perform the mechanistic analysis.

Following evaluation of the ATR probabilistic behavior, the plant physics is determined mechanistically (by systems codes such as the RELAP series). 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 probabilistic scenarios. To couple a scenario to the thermal-hydraulics calculation, we have to customize the thermal-hydraulics code model (or input deck if using a legacy code) specific to the scenario. For example, when a component fails in the simulation, a RELAP5 input also is generated that mimics the failure.

## 3. RIMM RESULTS

Once the load and capacity information is known (from the probabilistic and mechanistic analysis), it is possible to then determine the probabilistic safety margin. For ATR, 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.

After evaluating the proposed Margin recovery 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. In Figure 3, we see that Case III would be preferred over the other two strategies when using safety as the sole decision factor.

Once we have an integrated risk-informed safety margin model, 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 4, where we see that the preferred margin recovery strategy might change depending on the specifics of the plant. In this example, we see that if the ATR core power is increased to its maximum (i.e., 250 MW) then it is possible that Case III is preferred over Case II, depending on the reliability of the commercial power. Further, if it becomes known that the 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. Safety Margin Example for Three Recovery Strategies (Lower Values are Better)**

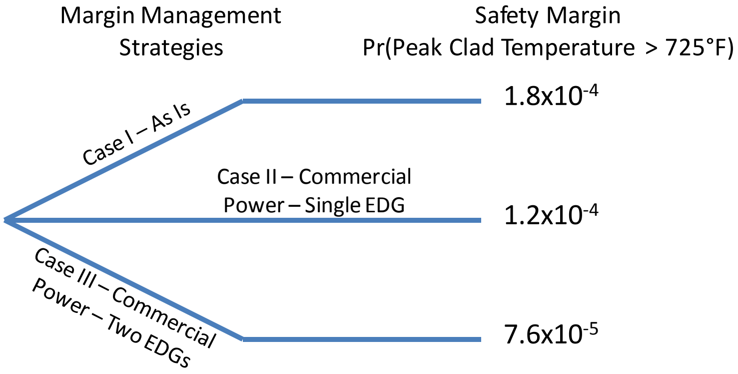
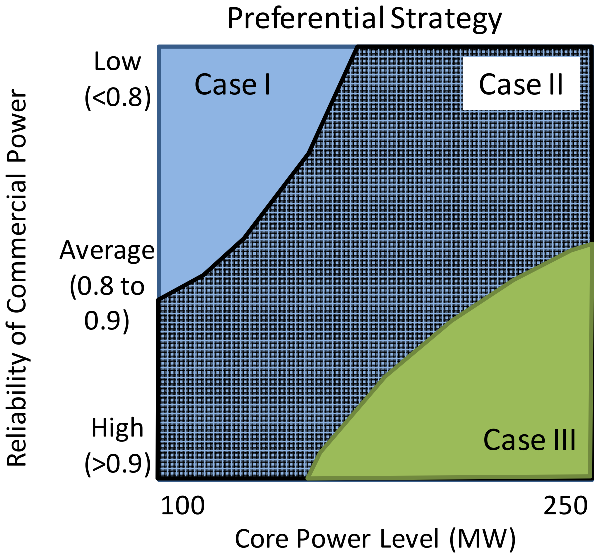


**Figure 4. Example of Decision Preferences when Key Plant Factors Change.**



For each simulation scenario, in addition to the safety margin values that are calculated, the frequency and consequences associated with that scenario are available. This allows us to determine the characteristics of the safety margin.

## 4. RISMC TOOLKIT

The approach we are using for the RISMC Pathway is to simulate plant behavior as it relates to safety margins. Specifically, we are developing the simulation components of the RISMC toolkit, which includes the following [2]:

- RELAP-7: A systems code that will simulate behavior at the plant level using advanced computational tools and techniques to allow faster and more accurate analysis. RELAP-7 is a reactor system safety analysis code, leveraging 30 years of advancements in software design, numerical integration methods, and physics models. In 2013, the INL implemented two-phase flow capability into the RELAP-7 code.
- RAVEN: A simulation module that provides input on the plant state to RELAP-7 (e.g., operator actions and systems, structures, and components states) in order to represent realistic plant behavior during normal and off-normal scenarios.

- Peacock: A graphical user interface used to create, control, and interact with the various tools in the RISMC toolkit.
- Grizzly: An aging simulation that models the physical processes related to time-dependent materials degradation and subsequent damage evolution. Grizzly is a structure and component aging code jointly developed by the INL and Oak Ridge National Laboratory for simulating aging and damage evolution in LWRs; the initial application of Grizzly is focused on the reactor pressure vessel. In 2013, the Grizzly model was compared successfully with the FAVOR (Fracture Analysis of Vessels – Oak Ridge) model, a code with a significant pedigree. This advances Grizzly toward providing an integrated, validated three-dimensional code for engineering assessments of aged reactor pressure vessels.

The RISMC toolkit is built using the Multiphysics Object-Oriented Simulation Environment (MOOSE), a computer simulation framework that simplifies the process for modeling physics as represented by mechanistic models. The MOOSE framework was developed by INL by using existing computer code and numerical libraries from proven numerical tools developed at universities and the Department of Energy. Recently, this toolkit was released under an open-source license. [3]

## 5. CONCLUSIONS

We have carried out a demonstration of the RIMM approach using ATR as a case study. We showed how traditional PRA and thermal-hydraulics quantification can be used and extended into the realm of safety margin characterization in order to improve nuclear power plant safety, reliability, and economics.

Completing the ATR case study has pointed to several additional areas of promising research and development related to risk-informed margin management. First, the current Nuclear Regulatory Commission 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 include nuclear power plant risk monitor enhancements; a general decision support capability for operational decisions; and an integrated and holistic framework to account for aging effects during the nuclear power plant lifetime.

During the research and development for the ATR case study, a variety of issues and lessons learned were encountered. Technical issues included items such 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 nuclear power plant 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. For example, an advance set of analysis tools is needed in order to streamline and enhance the RISMC approach that has been described. A new set of tailored analysis tools created using modern software and computers will empower future decision makers.

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

- Provides the safety case to decision makers in order to select operational alternatives as part of margin management.
- Develops a significantly improved plant physics approach, wherein we can couple, in an automated fashion, to mechanistic codes such as RELAP.
- 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 transfer the investment made in existing PRA models (which exist for every nuclear power plant in the United States.) into a dynamic simulation-type of model.

The approach and lessons learned from this case study will be included in future RISMC Pathway case studies and associated reports, which 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.

The RISMC Pathway has benefited from our collaboration activities, notably with the Electric Power Research Institute. The Electric Power Research Institute will continue to play an important role in high-level technical steering and in detailed planning of RISMC case studies. The RISMC Pathway research and development is coordinated with work from the Electric Power Research Institute’s Long-Term Operation Program.

## References

[1] Sherry, R. and J. Gabor, 2011, "Risk Informed Safety Margin Characterization: Trial Application to a Loss of Feedwater Event," PSA 2011, Wilmington, NC.

[2] Idaho National Laboratory, 2012, Light Water Reactor Sustainability Program Integrated Program Plan, INL/EXT-11-23452, Idaho National Laboratory.

[3] MOOSE framework, http://mooseframework.org/