Station Blackout: A case study in the interaction of mechanistic and probabilistic safety analysis

Curtis Smith*, Diego Mandelli, Cristian Rabiti

Idaho National Laboratory, PO Box 1625, MS 3850, Idaho Falls, ID 83415;

**Corresponding author: (Curtis.Smith@inl.gov)*

INTRODUCTION

The ability to better characterize and quantify safety margins is important to improved decision making about nuclear power plant design, operation, and plant life extension. As research and development (R&D) in the light-water reactor (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.

The purpose of the Risk Informed Safety Margin Characterization (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. In this paper, we describe the RISMC analysis process illustrating how mechanistic and probabilistic approaches are combined in order to estimate a safety margin. We use the scenario of a "station blackout" wherein offsite power and onsite power is lost, thereby causing a challenge to plant safety systems. We describe the RISMC approach, illustrate the station blackout modeling, and contrast this with traditional risk analysis modeling for this type of accident scenario.

THE RISMC APPROACH TO MODELING

In the RISMC approach, what we want to understand is not just the frequency of an event like core damage from station blackout, but how close are we (or not) to this event and how might we increase our safety margin. In general terms, a "margin" is usually characterized in one of two ways:

- A **deterministic margin**, typically defined by the ratio (or, alternatively, the difference) of a capacity (i.e., strength) over the load.
- A **probabilistic margin**, defined by the *probability* that the load exceeds the capacity.

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

The RISMC Pathway uses the probabilistic margin approach to quantify impacts to reliability and safety.

PROBABILISTIC MARGIN ILLUSTRATION

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 1. For this example, we suppose that a nuclear power plant 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

We run 30 simulations where this component plays a role in plant response under accident conditions (in "real" cases many simulations would be calculated, later we show a station blackout plot using 4000 runs). For each of the 30 simulations, we calculate the outcome of a safety metric –peak-clad temperature – and compare that against a capacity limit (assumed to be 2200°F). However, we have to run these simulations for both alternative cases (resulting in a total of 60 simulations). This illustration provides an example of how probabilistic and mechanistic calculations are combined – the scenario is described probabilistically (e.g., we will not know a priori which components might fail during a scenario) and for the resulting scenario, the details (e.g., what *has* failed at what time) determines the boundary conditions for mechanistic calculations such as the thermal-hydraulic response of the plant during the scenario.

The results of these simulations (shown in Fig. 1) 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 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 since its safety characteristics are better. 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.

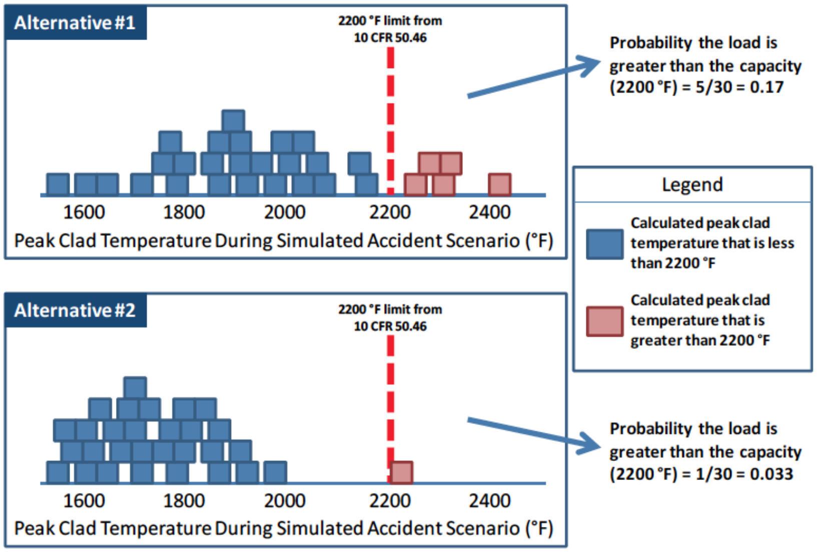

Fig. 1. Illustration of a probabilistic safety margin calculation.

The mechanics to conduct margins analysis follows the RISMC-specific steps [1]:

1. Characterize the issue to be resolved and the safety figures-of-merit to be analyzed to explicitly scope the modeling and analysis.
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. Note that a scenario is just a low-level model (e.g., a component) with active properties engaged with a larger model (e.g., the plant, including thermal-hydraulics). In this paper, we describe scenarios related to station blackout.
4. Represent plant operation *probabilistically* using the scenarios identified in Step 3. For example, plant operational rules (e.g., operator procedures) 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, the probabilistic plant representation will account for the possibility of failures.
5. Represent plant physics *mechanistically*. The plant systems-level code(s) 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. Using the simulations from Steps 3-5, construct and quantify probabilistic load and capacity distributions relating to the safety 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 the analysis.
8. Using risk management strategies, identify and characterize 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.

STATION BLACKOUT SIMULATION

In order to represent the nuclear plant behavior for station blackout scenarios, we focus the analysis within three general areas:

- Models – A representation of key systems, structures, and components (SSCs) is defined for a particular facility. We will be able to simulate with these models – by understanding how each SSC interacts with other parts of the facility (e.g., failure dependencies) – the hazard-induced susceptibilities of each SSC, and how to dial up model fidelity/resolution when needed.
- Phenomena – An approach to represent hazards and their effect on physical behavior at the plant is required. In some cases, multiple models of a specific phenomenon may be available, but this ensemble of models will need to be intelligently managed.
- Integration – Any risk-informed decision support approach will rely on a variety of probabilistic and mechanistic information. The safety-drivers will need to be integrated in order to determine the effectiveness of proposed mitigation strategies.

The scenario representation can interact or receive information from a mechanistic (e.g., physics engine) simulation. Through this capability, we can know the occurrence of various events in the simulation. This is done through "controls" placed in the model. For example, a trigger can be placed on a pipe related to an aging model so if a crack is seen (at some future time) that trigger is activated (and possibly many components can be failed due to the leaking fluid). The RISMC tool that performs the scenario representation is called RAVEN – additional detail on this tool is found in [2].

By running the simulation with these time dependent interactions, an analyst could see not only what affects a scenario has on the plant, but the relative time relationship between the events. These timing relationships may also affect other plant physics such as thermal-hydraulics in cooling systems, especially in complex situations such as those found in station blackout scenarios which range from minutes to days. Further, these timing relationships can be used to adjust performance shaping factors that are used to determine operator human error probabilities. For example, the human reliability model known as SPAR-H [3] can be integrated directly into the scenario generation in order to describe the success or failure of operator diagnosis and actions.

To simulate a station blackout scenario, we describe both the plant cooling functions (such as the primary cooling systems, as illustrated in Fig. 2) and supporting systems such as electrical power (including backup power sources such as the emergency diesel generators). Included in our station blackout model are factors such as:

- Failure probabilities and rates for key components.
- The power distribution network (e.g., lines and busses) in order to represent dependencies of support systems on the electrical system.
- Recovery actions performed by operators such as restoring offsite power or recovery of a failed diesel generator.
- Pump coast-down times (when power is lost).
- Thermal-hydraulics representing both coolant flow pressures and temperatures and clad temperatures.
- Capacity of the fuel to resist failure under high temperature conditions.
- Uncertainties on the many of the factors identified above.

Contrast with traditional station blackout modeling

While the static event-tree/fault-tree (ET/FT) approach has been used in the reliability modeling of systems for many years, numerous concerns have been raised about the capability of the ET/FT approach to handle dynamic and physical-based systems on a stand-alone basis. The ET/FT methodology does not treat the time-dependent interactions between physical processes and triggered or stochastic logical events as an accident evolves which may lead to coupling between these events through the control system. Even if these dynamic interactions are semi-quantitatively modeled through a classification of changes in process variables (e.g. "small", "moderate", "large), it may lead to the omission of some failure mechanisms due to inconsistencies in the definition of the allowed ranges for the process variables.

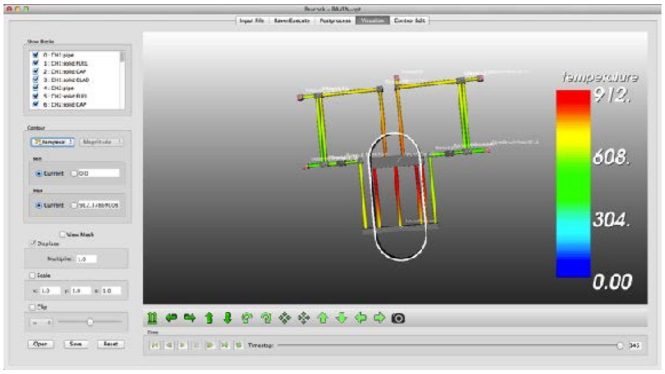

Fig. 2. Representation of cooling loops in the RAVEN tool.

In order to attempt to represent scenarios that are dynamic or involve mechanistic interactions, a variety of approximations have been used in static risk assessment models. We describe a few such approaches in this section, and for each, present why simulation using a coupled probabilistic and mechanistic approach provides a better analysis method.

One complication that occurs in cut set-based modeling is the treatment of what are called mutually-exclusive events. These are situations where two events that can be produced by the static fault tree model are, in reality, not possible are or not allowed. Current practice is to manually construct rules to post-process the results, thereby removing the suspect combinations. For example, a rule to remove an auxiliary feedwater pump (in test and maintenance) and a diesel generator (in test and maintenance) would look like:

```
if (AFW-TDP-TM * EPS-DGN-TM) then
  DeleteRoot;
Endif
```

In the simulation approach, instead of manually post-processing results, the plant rules (e.g., technical specifications) would be built into the model. Thus, the analysis would never create the combination and, consequently, would not require any additional attention.

An issue that complicates traditional cut set-based approaches is for the case where time-dependent failures or recoveries are found within a single cut set. For example, consider a typical cut set from the station blackout event tree:

IE-LOOP*DGN-FTS-A*DGN-FTR-B*OSP-NONREC

Let us focus just on the time-dependent portion of the cut set, namely: EPS-DGN-FTR-B * OSP-NONREC. Traditionally, cut set-based software would simply multiply the probabilities together for the two basic events above. However, this approach overlooks the time-dependent nature of the EDG failure, because the failure could have occurred any time between time zero and the end of the mission time (say eight hours). And the cut set describes failure as offsite power not being recovered by the time of EDG failure. Thus, not considering the time dependence can lead to erroneous answers. Consequently, some cut set models apply “fudge factors” called convolution values in order to approximate an exact answer.

The simulation approach we use to represent the station blackout models the time interactions directly, and as a consequence, no additional “fudge factors” are required in order to obtain correct estimates of probabilities.

Lastly, in order to mimic the dynamic time behavior, static risk models are frequency subdivided into artificial time segments. For example, a failure rate for a pump may be broken into a 1 hour mission time (for early failures) then a 23 hour mission time (to represent later failures). Not only does this greatly complicate the model (each part of the model is copied multiple times, thereby making it harder to understand and maintain), but is only an approximation. The simulation approach represents these types of dynamic situations directly.

CONCLUSIONS

The RISMC Pathway provides a systematic approach to the characterization of safety margins, leading to the support of margins management options (those proposed alternatives that work to control margin changes due to aging or plant modifications). As such, it provides a vital input to the owner and regulator to support decision making for NPP operations now and for extended lifetimes.

RISMC uses a probability-margin approach to quantify impacts in order to avoid conservatisms (where possible) and to treat uncertainties directly. An example of the types of results that are calculated for a station blackout analysis is shown in Fig. 3, where we calculate both a load (the blue area) and a fuel capacity (the red area). This margin approach uses a blended approach of probabilistic and mechanistic calculations.

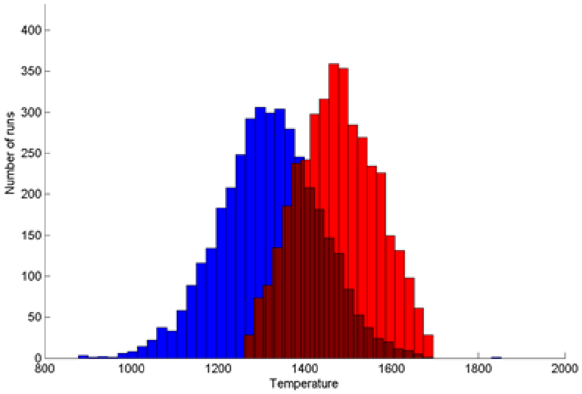

Fig. 3. Example of the load capacity margin results.

Once we complete the RISMC methods and toolkit, a link to a risk model would exist – consequently we could have an interactive risk tool and advanced training device. This interaction could be extended to allow the user to affect the risk model – for example one could “enter” the plant model and select components to modify – then they could see the safety changes and understand the safety margin magnitude. This would enable anyone familiar with the physical version of the nuclear power plant to see the ramifications of their proposed modifications.

The details that are produced from simulation approaches have been criticized due to the analysis computational burden and the resulting volume of information that can be produced. While not readily apparent, we should view these criticisms as potentials for enhancing accuracy and timeliness. For example, the scenario detail that is obtained as part of simulation analysis may be (if we ask in the right way) viewed as providing information not just on failures (the typical question) but on degradations, operability issues, maintenance issues, and human performance. Further, these simulation information streams may be mined for positive aspects of performance (what works and why) since the bulk of these simulated realities will not result in undesired outcomes – the “insights” are in the details.

REFERENCES

1. C. SMITH, C. RABITI, R. MARTINEAU, “Risk Informed Safety Margins Characterization (RISMC) Pathway Technical Program Plan,” INL/EXT-11-22977 (2012).

2. C. RABITI, A. ALFONSI, D. MANDELLI, J. COGLIATI; R. MARTINEAU; C. SMITH, “Deployment and Overview of RAVEN capabilities for a Probabilistic Risk Assessment Demo for a PWR Station Blackout,” INL/EXT-13-29510, (2013).

3. D. GERTMAN, H. BLACKMAN, J. MARBLE, J. BYERS, C. SMITH, “The SPAR-H Human Reliability Analysis Method,” NUREG/CR-6883, (2005).