INL/EXT-13-28565

Integrating Safety Assessment Methods Using the Risk Informed Safety Margins Characterization (RISMC) Approach

Curtis Smith
Diego Mandelli

March 2013

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

INL/EXT-13-28565

Integrating Safety Assessment Methods Using the Risk Informed Safety Margins Characterization (RISMC) Approach

Curtis Smith
Diego Mandelli

March 2013

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

Integrating Safety Assessment Methods using the Risk Informed Safety Margins Characterization (RISMC) Approach

Curtis Smith[†] and Diego Mandelli[‡]

Idaho National Laboratory (INL), 2525 Freemont ave., Idaho Falls (ID) 83415

[†]curtis.smith@inl.gov, [‡]diego.mandelli@inl.gov

INTRODUCTION

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 system structure and component (SSC) 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".

The ability to better characterize and quantify safety margin [1] 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 "extended design basis" operation. A systematic approach to characterization of safety margins represents a vital input to the licensee and regulatory analysis and decision making that will be involved. In addition, as R&D in the LWR Sustainability Program [2] and other collaborative efforts yield new data 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 Fig. 1.

To successfully understand safety margins, the Risk Informed Safety Margins Characterization (RISMC) Pathway [2] will clearly define and demonstrate the safety margin approach. The determination of the degree of a safety margin requires an understanding of risk-based scenarios. Within a scenario, an integration 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. Then, to characterize safety margin for a specific performance metric of consideration (e.g., peak clad temperature), the integrated 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.

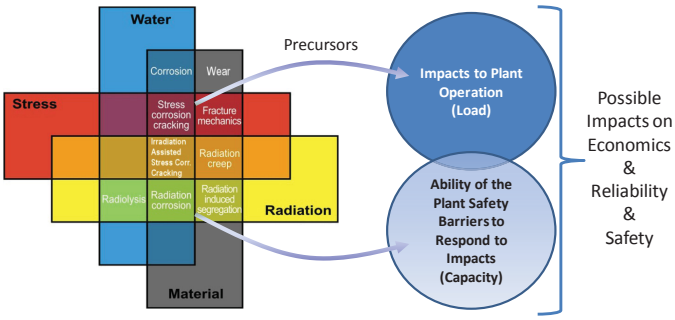

Fig. 1. Representation of the interaction of degradation mechanisms that may impact plant operations and safety barriers if left unmitigated.

BACKGROUND

"Margin" is a term that gets redefined in almost every report in which it is used. This seems to occur partly because its meaning is context-dependent, and partly because not everyone chooses to stress the probabilistic aspects of it. In order to avoid a lengthy etymological digression, rather than developing a thesis about the concept of "margin," the present discussion will simply stress what we are trying to accomplish. We are trying to develop actionable engineering insights into certain kinds of failure scenarios, in order to understand better how to prevent them, or at least develop a more realistic appreciation of the risk associated with them, in order that plant investment decisions may be better informed. This development is applicable to failure scenarios about which there is very significant uncertainty, due to variability in how the scenarios evolve, and/or state-of-knowledge uncertainty about how to model them.

In order to develop these actionable engineering insights, we simulate some number of time histories of plant performance bearing on a particular issue. Each time history evolves mechanistically, but is conditional on the

current values of uncertain inputs that are derived from a sampling process. The inputs to the simulations are chosen in such a way that the aggregate of time histories can be analyzed to show how likely certain kinds of failures are, or how unsure we are of the failure potential, or what potentially-controllable factors themselves control the failure potential.

In the above, the phrase "some number of time histories" usually means, in practice, "as many as practical, the more the better." In a complex problem, it may be desirable to simulate hundreds or even thousands of time histories in order to sample an issue space adequately. This may take a lot of computation. Accordingly, while this kind of analysis has been contemplated for over 30 years, it has mostly been academic up to now, owing to previously existing limitations in computer hardware and software. Computer hardware has improved very significantly in the last 30 years, and it is expected that new software for phenomenology simulation will represent a step change in software capability.

MARGIN ANLYSIS TECHNIQUES

RISMC will address the mechanics of techniques to conduct margins analysis [3, 4], including methodology for carrying out simulation-based studies of safety margin, using the following process steps (see Fig. 2):

1. Characterize the issue to be resolved in a way that explicitly scopes the modeling and analysis to be performed. Formulate an "issue space" that describes the safety figures of merit to be analyzed.
2. Quantify the decision-maker and analyst's state-of-knowledge (uncertainty) of the key variables and models relevant to the issue. For example, if long-term operation is a facet of the analysis, then potential aging mechanisms that may degrade components should be included in the quantification.
3. Determine issue-specific, risk-based scenarios and accident timelines.
4. Represent plant operation probabilistically using the scenarios identified in Step 3. For example, plant operational rules (e.g., operator procedures, technical specifications, maintenance schedules) are used to provide realism for scenario generation. Because numerous scenarios will be generated, the plant and operator behavior cannot be manually created like in current risk assessment using event- and fault-trees. In addition to the expected operator behavior (plant procedures), the probabilistic plant representation will account for the possibility of failures.
5. Represent plant physics mechanistically. The plant systems level code 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. 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 within this issue to in order to proposed Margin Management Strategies. Determine whether additional work to reduce uncertainty would be worthwhile or if additional (or relaxed) safety control is justified.

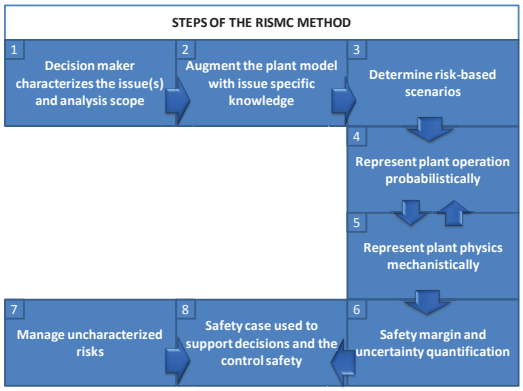

Fig. 2. Steps required in the RISMC method.

MODES OF CODE APPLICATION

Conservative Mode

This mode of application contemplates code applications that resemble the classical safety analysis [5] ("Safety Analysis Report" Chapter 15) applications of RELAP-5. The limiting case of a design-basis accident is analyzed with the traditional conservatisms, and satisfaction of regulatory acceptance criteria is demonstrated based on the point value results. The limiting single failure is assumed; with and without concurrent loss of offsite power (the more limiting case is applied).

Best-Estimate-Plus-Parameter-Uncertainty (BEPU) Mode

This mode of application somewhat resembles more recent licensing applications that are more "realistic" (i.e.,

they still analyze stylized limiting scenarios, but have fewer embedded conservatisms), and also address parameter uncertainty by characterizing the uncertainty in the output variables. Within the BEPU approach, in order to characterize output uncertainty for RELAP, one builds up the distribution on the output variables by appropriately sampling the joint distribution of the uncertain input parameters, and then carrying out one RELAP run for each sample.

The number of samples needed for this is determined by a tradeoff between the statistics needed and the computer time available. Assessment of output uncertainty can be done much more efficiently if it is allowed for in the code development from the beginning.

RISMC Mode

In this mode, the endeavor is to characterize safety margin by developing probabilistic load spectra and corresponding probabilistic capacity spectra for key functions and systems, structures, and components (SSCs), conditional on a user-specified "issue space" (e.g., Large loss of coolant accidents (LOCA), loss-of-all-feed water transients,…). This assessment provides more risk-informed insight into accident likelihood than is to be had by analysis of stylized limiting cases.

This mode is a generalization of the above modes: instead of deriving a conservative point estimate of a key variable in a licensing scenario, and comparing that with a precise regulatory acceptance threshold (Conservative), or building up a parameter uncertainty distribution around the same scenario with less embedded conservatism (BEPU), one derives uncertainty distributions on load and capacity conditional on a specific set of scenarios, recognizing that the initiating event may vary in severity and/or break location, diverse equipment failures may occur within the mitigating systems' mission time, and so on.

Basically, "scenario" degrees of freedom that were frozen in the "conservative" and "BEPU" modes are unfrozen in the probabilistic margin assessment mode. It is still necessary either to generate one time history per "scenario," with scenarios sampled probabilistically, or make use of a restart capability in order to be able to re-use portions of scenarios leading up to branch points (as in "dynamic probabilistic risk analysis"); but in the end, the distributions on load and capacity reflect aleatory variability as well as parameter uncertainty, and are much better suited to support risk-informed decision-making than the "deterministic" results.

Vulnerability-Search / Limit-Surface Mode

In this mode, the point to understand qualitatively the conditions under which failure occurs. This could take the form of characterizing the limit surface. The use of probability information is different in the vulnerability-search / limit-surface mode from its use in RISMC.

In both of these modes, the simulation will be inside an automated driver, and needs to be able to be run essentially unattended, and the faster the better.

CONCLUSIONS

The purpose of the 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. 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.

The methods and tools provided by RISMC are key to a Risk-Informed Margin Management approach where we are able to use methods maintain margins for active and passive SSCs. The deliverables provided by the Pathway include: (1) Technical Basis Guides for Risk-Informed Margins Management and (2) the RISMC Toolkit. These deliverables will serve to provide a comprehensive approach and software to support safety, reliability and economic decisions needed for long term NPP operation.

REFERENCES

1. E. ZIO, "Reliability engineering: Old problems and new challenges," *Reliability Engineering and System Safety*, 125-141 (2009).
2. IDAHO NATIONAL LABORATORY, "Light Water Reactor Sustainability Research and Development Program Plan (Fiscal Years 2009-2013)", INL/MIS-08-14918, Rev. 1 (2009).
3. V.N. DANG, T-W. KIM, M.A. ZIMMERMANN, A. MANERA, "Assessing Safety Margins: The Impact of a Power Uprate on Risk from Small and Medium LOCA Scenarios," *Proc. of the 10th International Probabilistic Safety Assessment & Management Conference*, Seattle (2010).
4. M.A. ZIMMERMANN et al., "Towards quantification of plant safety margins: a status report," *Proc. 13th Int. Topical Meeting on Nuclear Reactor Thermal Hydraulics* (NURETH-13), Kanazawa City, Ishikawa Prefecture, Japan (2009).
5. P. BISHOP, R.A. BLOOMFIELD, "Methodology for Safety Case Development," *Safety-Critical Systems Symposium*, Birmingham, UK (1998).