INL/CON-09-15549
PREPRINT

Risk-Informed Safety Margin Characterization

ICONE 17

Stephen M. Hess
Nam Dinh
John P. Gaertner
Ronaldo Szilard

July 2009

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

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Proceedings of the 17th International Conference on Nuclear Engineering
ICONE17
July 12-16, 2008, Brussels, Belgium

ICONE17-75064

RISK-INFORMED SAFETY MARGIN CHARACTERIZATION

Stephen M. Hess
Electric Power Research Institute
West Chester, PA, USA

Nam Dinh
Idaho National Laboratory
Idaho Falls, ID, USA

John P. Gaertner
Electric Power Research Institute
Charlotte, NC, USA

Ronaldo Szilard
Idaho National Laboratory
Idaho Falls, ID, USA

ABSTRACT

The concept of safety margins has served as a fundamental principle in the design and operation of commercial nuclear power plants (NPPs). Defined as the minimum distance between a system's "loading" and its "capacity", plant design and operation is predicated on ensuring an adequate safety margin for safety-significant parameters (e.g., fuel cladding temperature, containment pressure, etc.) is provided over the spectrum of anticipated plant operating, transient and accident conditions. To meet the anticipated challenges associated with extending the operational lifetimes of the current fleet of operating NPPs, the United States Department of Energy (USDOE), the Idaho National Laboratory (INL) and the Electric Power Research Institute (EPRI) have developed a collaboration to conduct coordinated research to identify and address the technological challenges and opportunities that likely would affect the safe and economic operation of the existing NPP fleet over the postulated long-term time horizons. In this paper we describe a framework for developing and implementing a Risk-Informed Safety Margin Characterization (RISMC) approach to evaluate and manage changes in plant safety margins over long time horizons.

INTRODUCTION

The concept of safety margins as a cornerstone of nuclear reactor design emerged during the early days of commercial nuclear power as a part of the defense-in-depth approach to ensuring nuclear safety. Defined as the minimum distance between the system's "loading" and "capacity", safety margin is expressed in terms of safety-significant parameters and is determined for a range of anticipated system operating conditions. In the traditional approach to NPP design and licensing, demonstration of adequate safety margins is required for a prescribed set of design-basis accidents. Due to limitations of knowledge, both with respect to phenomenology and plant response, large and conservatively specified safety margins typically are applied to compensate for these uncertainties.

As a result of both economic and environmental (e.g. climate change) imperatives, it is envisioned that operation of the current fleet of commercial NPPs in the United States will extend significantly beyond the original 40 year licensing period. Currently, the average age of U.S. nuclear plants is 29 years with the oldest operating plant in year 39 of its license. Figure 1 shows the distribution of U.S. nuclear plants by the year in which their original 40-year license would expire. At this time, nearly one half of the current fleet of US plants has been granted regulatory approval to extend their operating license to 60 years. Additionally, many NPP operators are considering the possibility of extending the operating lives of these reactors to 80 or even 100 years. This extension of operating license by a factor of two or more from the original design lifetime can result in significant challenges for both plant technology and the regulatory process. Reference [1, 2, 3] provides a discussion of many of these challenges from the perspective of NPP operators.

To meet these challenges, the USDOE, INL and EPRI are collaborating to develop coordinated research to identify and address the technological challenges that could impact the safe and economic operation of the existing NPP fleet over the postulated long-term time horizons associated with extended operation. This has led to the identification of four specific research pathways [4]:

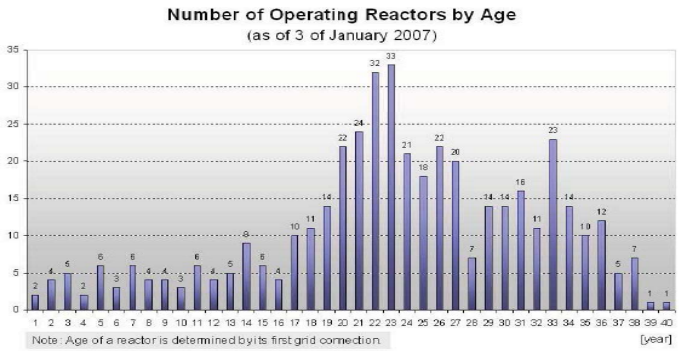

Figure 1: Number of US operating reactors by age.

- nuclear materials aging and degradation,
- advanced light water reactor fuel development,
- risk-informed safety margin characterization,
- advanced instrumentation and control technologies.

These four research and development pathways have been identified to obtain improved understanding of the challenges posed by NPP aging with a focus on improving the fundamental aging and degradation knowledge basis in reactor material sciences, creating improved inspection and monitoring technologies, fostering development of advanced fuels, and incorporating risk-informed, performance-based techniques in safety margin characterization and life extension decision-making. The research in these pathways is being performed as a collaborative effort between the Light Water Reactor Sustainability (LWRS) program sponsored by the USDOE and managed by INL and the Long Term Operation (LTO) initiative sponsored by EPRI. In this paper we describe the objectives, technical elements, research approach and anticipated outcomes for the RISMC pathway.

Each of these pathways will address specific aging degradation, plant up-rates and refurbishments, and other design and operational changes intended to enhance the plant through modernization. In addition to its own specific objectives, the RISMC pathway can characterize the individual and integrated effects of the other pathways using common measures of safety. This integrating role of the RISMC pathway is displayed schematically in Figure 2.

Risk-informed regulations and operations of NPPs have become part of regulatory policy of the U.S. Nuclear Regulatory Commission and of the operational culture at U.S. NPPs. That this would be the case is both logical and technically sound. First, elements of nuclear plant licensing, design, and operation originally were established when there was little operating experience with nuclear plants. As such, licensing requirements were conservative and prescriptive. Designs had significant safety margin. Operations, testing, work management, and maintenance programs were complex. With more than 3000 operating years of experience in the U.S. alone, operators now confidently can optimize these requirements and processes. Two decades of carefully implementing risk-informed processes have demonstrated that safety-risk is an appropriate criterion for such optimization of regulations; it also is effective for optimization of NPP operations. This optimization improves safety, plant performance, and cost to both the plant operators and to electricity consumers. With considerations for differences in safety policies and practices, it is believed that risk-informed operations and regulations would be applicable world-wide.

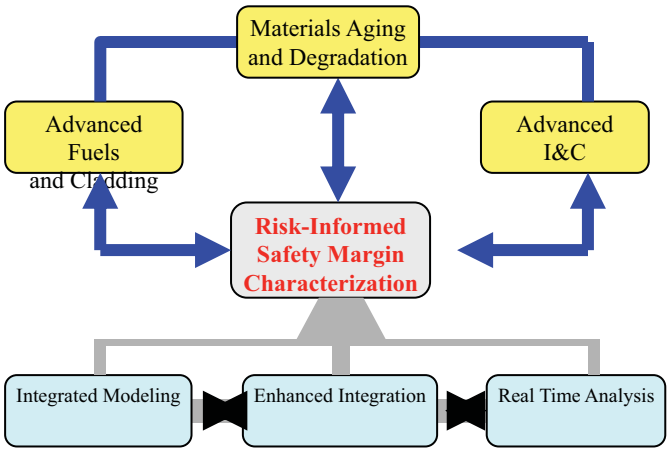

Figure 2: LWRS / LTO technical pathways and integration.

NOMENCLATURE

CFD – Computational Fluid Dynamics
CRM – Configuration Risk Management
DBA – Design Basis Accident
DSA – Deterministic Safety Assessment
EPRI – Electric Power Research Institute
I&C – Instrumentation and Controls
INL – Idaho National Laboratory
LTO – Long Term Operation
LWRS – Light Water Reactor Sustainability
NDE – Nondestructive Examination
NPP – Nuclear Power Plant
PRA – Probabilistic Risk Assessment
R&D – Research and Development
RISMC – Risk Informed Safety Margin Characterization
SCI – Sustainability Critical Information
SCT – Sustainability Critical Tools
SSC – Structures, Systems and Components
USDOE – United States Department of Energy

RISMC PATHWAY OBJECTIVES

The RISMC pathway represents one of four identified research pathways in the USDOE LWRS and EPRI LTO initiatives. The pathway is intended to support the development

and implementation of risk-informed plant safety margins for effective and efficient evaluation / management of changes in those safety margins over the long time horizons that are representative of extended NPP operation. The pathway also is envisioned to develop an integrated decision framework that would support enhanced operational flexibility and safety over these time frames. The framework includes the following technical elements:

- Identifying technical needs by investigating safety analysis applications likely to be needed to ensure safe, economical long term operation.
- Enhancing best-estimate analysis methods available for engineering, regulatory, and operational applications, including development of advanced simulation tools.
- Enhancing risk calculation methods and tools.
- Development of integrated modeling capability to support both design based and operational risk-informed decision making.
- Validating the framework via one or more significant generic pilot applications.
- Facilitating deployment of the results for widespread application.

Since both the LWRS and LTO programs represent long term research initiatives, research and development performed to support the RISMC pathway has both short and long-term objectives. For the short term, the basic pathway approach will investigate actions necessary to integrate risk-informed, performance-based methodologies with fundamental scientific understanding of critical phenomenological conditions and deterministic predictions of nuclear plant performance. The outcomes of this analytical framework are intended to provide an integrated characterization of safety margins resulting in optimization of nuclear safety, plant performance, and long-term asset management. Thus, over the next 5 years, the research effort has the following objectives:

1) Achieve significant progress toward development of a consensus approach that is accepted by NPP operators, regulatory authorities, and other stakeholders for risk-informed safety margin assessments.
2) Have completed at least two case studies of safety margin applications of interest and value to NPP stakeholders for long term operations decisions.
3) Achieve significant progress on enhanced deterministic safety assessment (DSA) capability, computational engines, uncertainty quantification, results visualization, and validation.
4) Achieve significant advances in enabling broad application of an integrated suite of probabilistic risk assessment (PRA) tool(s) with capability to apply advanced computational methods, full scope PRA aggregation capabilities, results visualization, and connectivity to plant information for configuration risk management (CRM).
5) Develop a plan and progress toward an integrated RISMC capability including interface of PRA and DSA codes, broad connectivity to plant information, and simulation capability.

Over the longer term, the RISMC pathway's objective is to develop and apply advanced analysis methods and simulation tools to predict and manage plant response and safety margins as an essential part of operational and regulatory decision-making for commercial NPPs.

ELEMENTS OF RISMC

In the context of risk-informed regulation, safety margin – while broadened as a concept – remains a fundamental tenet of both the regulatory and operational decision-making framework. Generally, safety margin can be defined as the minimum distance between a system's "loading" and its "capacity," as shown schematically in Figure 3. Traditionally in licensing of commercial NPP designs, the availability of adequate safety margins must be demonstrated for a prescribed set of design basis accidents (DBAs). Due to limited knowledge, large (i.e., conservatively specified) safety margins are applied to compensate for approximations used in (the phenomenological or deterministic) models and associated computer codes which estimate the "loads" and the "capacity" in the reactor systems that occur during the complex accident sequences that are analyzed.

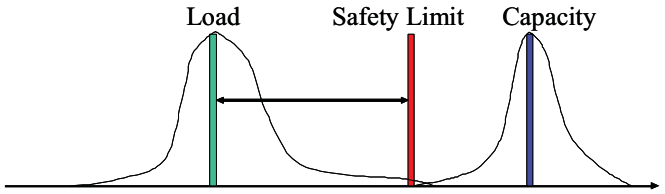

Figure 3: Schematic of safety margin.

In addition to the required deterministic safety analyses, probabilistic risk assessment methods have been developed and applied to analyze the safety of NPPs. Within the PRA framework, safety margins calculated by the DSA methods are used to support the specification of PRA "success criteria" for the various postulated accident sequences. Since its inception in the mid-1970s, PRA technology has matured to the point where it currently provides a powerful tool from which plant safety and system vulnerabilities can be analyzed. A significant barometer of this level of maturity is that PRA technology serves as the fundamental framework for all of the risk-informed regulatory initiatives that have been implemented in the United States.

So what does it mean to "risk-inform" the safety margin characterization? Figure 3 illustrates that load and capacity are not discrete values, but have distributions. In the current framework, the concept of safety margin is limited to characterizing the "load" as a known quantity with the margin given by the distance from this load to the defined safety limit. In this concept, uncertainties only are addressed implicitly, i.e., the assessment of the "load" is conducted using conservative assumptions and analysis methods. However, as described in [5], there are several problems associated with this approach. First, the current generation of physics based models are capable of only providing approximate results of the real "load" representing the actual plant condition. Second, the application of conservatisms (in assumptions and modeling) can lead to non-conservative predictions of the load. In the current approach, the use of a safety limit as a surrogate for the "capacity" serves as an additional conservatism; however, because the degree to which the safety limit is conservative is unknown, this approach prescribes significant operational limitations on the plant. The intent of a risk-informed approach to characterization of safety margins is to integrate the information from both deterministic and probabilistic safety analyses to obtain a complete picture.

However, there are significant limitations and inefficiencies in the integration of the DSA and PRA technologies as they currently exist and are applied. In particular, application of the current state of the art can be characterized as a "brute force" approach that requires a sequence of serial steps to evaluate and characterize safety margins. Furthermore, the tools and methods have legacy issues from their initial development 20 to 40 years ago; that is, they have simplified mechanistic models, inefficient computational algorithms, primitive connectivity, and non-intuitive visualization of results. Although adequate, application of the current technology is usually overly conservative, labor intensive, time consuming and expensive. Applications for simulation and monitoring often are precluded.

The likelihood that the current fleet of commercial NPPs will operate over extended periods of time will require resolution of the limitations and deficiencies previously described. Operation over these extended time frames will result in challenges to NPP safety margins, impacting both the load and capacity elements. For example, activities performed to enhance the economic competitiveness of the NPP (such as power uprates and use of high burnup fuel) may result in an increase in the load portion of the safety margin. Likewise, material degradations due to aging mechanisms could result in decreases in the capabilities of plant structures, systems and components (SSCs), i.e. the capacity portion of the safety margin. In both cases, longer operating lifetimes also have the potential to increase the uncertainties in their characterizations. The net effect is a potential for reduced safety margins over time. This concept is shown schematically in Figure 4.

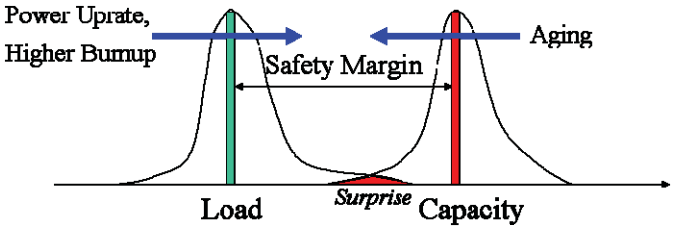

Figure 4: Impact of extended NPP lifecycle on safety margins.

The use of risk information in characterizing plant safety broadens the definition of "safety margin" relative to the one used in the traditional licensing (i.e., prescriptive) approach. For example, under a risk-informed approach, deterministic criteria specified for a number of enveloping DBAs could be modified by results that account for both the frequency and potential consequences of the postulated event.

The planned research and development can be viewed as consisting of three inter-related groups addressing the following issues: (1) advanced PRA techniques, (2) advanced DSA techniques, and (3) methods / tools for analysis integration and visualization of results to support effective and efficient decision-making. For all three groups, the research is intended to address completeness of analysis, treatment of uncertainty, and efficiency of computation so that more accurate and cost-effective techniques can be used to address safety margin characterizations.

In the PRA area, development of advanced analysis techniques continues to be an area of ongoing research and development. From the perspective of NPP owner / operators, significant effort has been expended to obtain practical risk-informed operational applications. A significant example of this in the US is the broadening applications of configuration risk management to plant operations and maintenance programs. From the perspective of both NPP operators and regulatory personnel, there continues to be significant desire to improve the computational efficiency of risk assessment and to develop methods and tools that more accurately characterize and address limitations inherent in the current state of the art. Examples include performing research on declarative modeling, direct probability calculation and binary decision diagramming approaches [6] to enhance the ability to model increasingly complex issues. For illustration, we provide a brief discussion of the declarative modeling approach which is a strategy to improve the transparency, flexibility and effectiveness of PRA models. The approach involves use of the capabilities inherent in modern programming languages to provide informational attributes for PRA model elements and using these attributes to process the models. In contrast to the traditional rule based structure inherent in current PRA models, in a declarative model based PRA, the calculations performed are governed by the status of the various attributes rather than the specific objects themselves.

While important advances are being made to improve the state of the art in PRA methodology, its effective use in the decision process is limited. A significant limitation, which is directly applicable to the management of safety margins, is the reliance on current generation DSA tools to determine PRA success criteria. This is due to the fact that the current generation of DSA methods and tools does not support a framework to account for uncertainty in the deterministically estimated values of "load" and "capacity." For example, where margins are relatively small or where large uncertainties exist, it is possible for functional success to occur in the PRA event tree's failure branch, and conversely, functional failure can occur in the tree's success branch. This uncertainty in the accuracy of the PRA results for cases where margins may be small can limit the usefulness of PRA in decision-making. A particularly important example is the application of PRA to passive SSCs [7, 8]. Another example of a limitation of the current PRA methods is the assumption of independence of failure rates on the system's state and evolution. Techniques for dynamic PRA, which are intended to address this issue, are still in a very early phase of development.

In the DSA area, while incremental advances to improve modeling of plant components and transient / accident phenomena have been made over the past two decades, the analysis tools are based on decades-old modeling framework and computational methodology. Thus, they have not taken advantage of modern developments in computer / computational science and engineering. Fundamental limitations in the current generation of system analysis codes are well known. Although the codes have served as an adequate basis to address safety margin analysis, significant enhancements will be necessary to support the challenges of extended and enhanced plant operations. These challenges include issues such as the presence of unquantifiable errors in numerical approximations and methods to combine results from separate physical models. The use of individually derived physics models (i.e., thermal hydraulics, neutron kinetics) and their explicit coupling to simulate reactor transients results in an inefficient approach to DSA. This approach also fails to capture complex multi-dimensional and tightly coupled multi-physics behavior when such complexity may be significant for the evaluation of safety margins. Efforts to advance the DSA technology include research and development to bring advanced methods of Computational Fluid Dynamics (CFD) to support plant safety analysis. For example, CFD methods have proven instrumental in the study of complex flow phenomena (e.g. mixing / stratification, asymmetric flow) that occur in reactor downcomers and lower plena during certain transient and accident conditions. Although CFD has proven to be a valuable tool to investigate the detailed physics of fluids, high-resolution (fine-grain) CFD is computationally expensive and, thus, is not a practical approach for the whole-system simulations of plant transients / accidents necessary to support operational evaluations and decisions. Furthermore, due to heterogeneity and high priority for multi-physics treatment of nuclear power plant transients and accidents, the commercial CFD codes (with their frozen and fluid-centric structures) are not conducive for use as a multi-physics simulation framework required for the next generation of system analysis tools.

Figure 5 depicts the elements of RISMC in the context of the LWRS and LTO research programs. In the spirit of defense-in-depth, margin is considered to be significant to the degree that it exceeds uncertainties and variabilities associated with a given comparison between the "load" and the "capacity." This idea applies to success of active functions as well as passive SSC integrity, which is instrumental to the characterization, mechanistic understanding, prediction, and monitoring of the plant aging and degradation behaviors and their impact on plant life extension decision making.

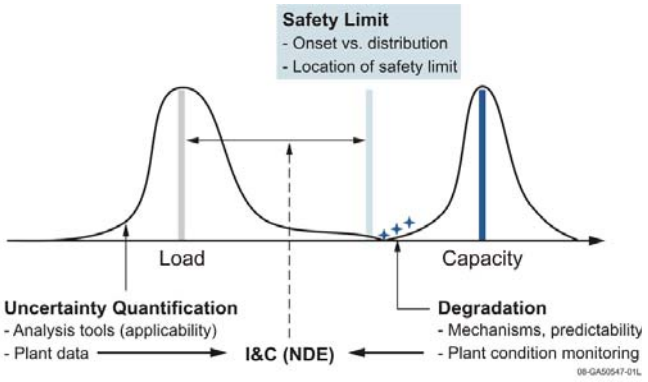

Figure 5: Elements of the RISMC model.

Given the LWR Sustainability focus, the RISMC research and development (R&D) scope is shown in Figure 6. Areas marked in light yellow (including part of the SCI and SCT boxes) depict the RISMC R&D activity domain. The success of a "Sustainability Decision" imposes requirements for "Sustainability-Critical Information (Data) - SCI" and "Sustainability-Critical Analytical Tools (SCTs)". A significant part of SCI and SCT is anticipated to be derived from advances made in the LWRS program's other technological pathways (Materials, Fuels, and instrumentation and controls (I&C)), e.g. physics-based models to predict degradation and failure modes in aging materials. Another important part of SCI / SCTs also will be created as part of longer-term RISMC R&D and includes activities such as advanced models and computer codes for high-fidelity simulation of plant transients and accidents and advanced PRA modeling and quantification techniques. An example is modeling of how testing, inspection and maintenance activities could impact SSC risk-performance over the long periods of plant operation that the LWRS effort is intended to facilitate.

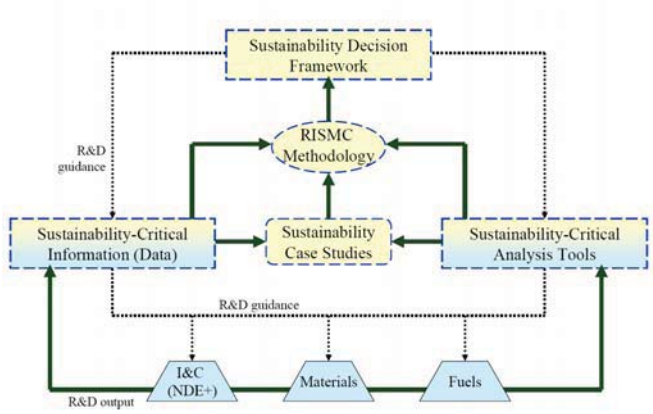

Figure 6. R&D strategy of RISMC for LWR sustainability.

The guiding principle is to focus on developing knowledge / capability to facilitate enhanced decision-making and improved regulatory / public acceptance of long-term plant operation. Furthermore, the RISMC R&D Pathway is envisioned as a mechanism to provide an integrating science-based framework to enable effective visualization and efficient implementation of advances achieved in the other LWRSP pathways (i.e. "Materials Aging and Degradation"; "Advanced Nuclear Fuels", and "Advanced I&C"). As such, the RISMC Pathway provides, on the front end, a means to risk-inform the R&D efforts performed in the other LWRS pathways; and on the back end, a mechanism for the effective and efficient implementation of advances achieved in them.

CASE STUDIES

The key element for developing an effective RISMC strategy is the development of (sustainability) case studies. These case studies will examine the potential benefits and issues associated with RISMC in situations where existing decision processes may not be sufficient to address long-term sustainability needs and objectives. Since the case studies are anticipated to be significant work activities, a series of "table top" exercises first will be performed. The intent of these exercises will be to evaluate potential applications of RISMC to address important sustainability issues. Example risk-informed applications that will be investigated in the short term are:

1) Evaluation of design basis requirements for large-break Loss of Coolant Accidents and / or High Energy Line Breaks.
2) Optimizing operations of pressurized water reactors during mid-loop conditions in the shutdown mode.
3) Evaluating the broad application of risk-managed Technical Specification Allowed Out-of-Service Times.
4) Performing a safety assessment of a phased, multi-cycle plant refurbishment and power up-rate.
5) Evaluating application of risk and safety monitoring that utilizes real-time operating parameter data, equipment configurations, success criteria, and reliability information.
6) Considering application of an efficient Significance Determination Process assessment to evaluate emergent safety issues.

Issues that are identified during the "table top" exercises might include critical limitations in the scope, resolution, or completeness of DSA / PRA tools or models; code validation including data and testing; degrees of conservatism or realism; representation of uncertainty; and use of expert elicitation, performance monitoring requirements, and generic assessment versus pilot plant applications. In addition, the results of these exercises will be used to prioritize research activities and select those applications for which detailed case studies would be performed.

SUMMARY AND CONCLUSIONS

The vision for the RISMC research pathway is to develop an integrated approach and implementation tools that permit cost-effective safety margins assessments addressing challenges and opportunities associated with extended NPP operation. In addition, the project will address enhanced RISMC capabilities to address future challenges and opportunities beyond those currently addressed. A schematic of the long-term schedule of research activities for the pathway is provided in Figure 7.

Specifically, the pathway anticipates the following accomplishments can be achieved over the next 5 years.

1) Achieve significant progress toward a consensus approach accepted by NPP operators, regulatory authorities, and other stakeholders for risk-informed safety margin assessments.
2) Have completed at least two detailed case studies of safety margin applications of interest and value to all stakeholders to support long term operations decisions.
3) Achieve significant progress on developing enhanced DSA capability, computational engines, results visualization, and validation.
4) Achieve broad application of an integrated PRA tool with advanced computational methods, full scope PRA aggregation capabilities, results visualization, and connectivity to plant information for configuration risk management.
5) Develop a comprehensive plan and obtain progress toward development of an integrated RISMC capability including interface of PRA and DSA codes, broad connectivity to plant information, and simulation capability.

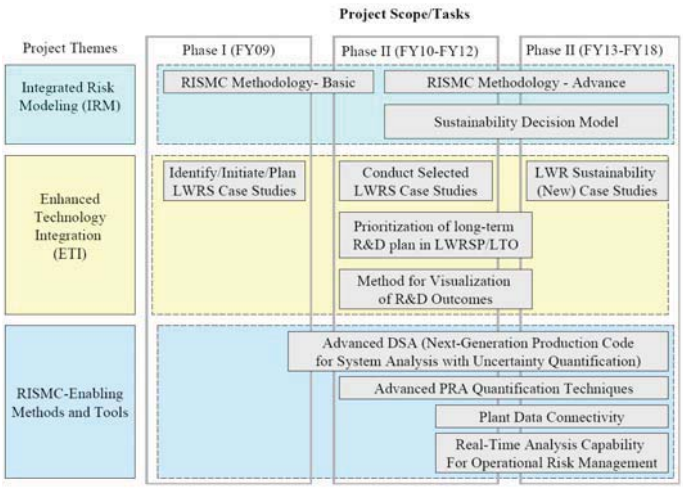

Figure 7: RISMC pathway schedule.

ACKNOWLEDGEMENTS

Two of the authors (SH and JG) wish to acknowledge that portions of this work were sponsored by the Electric Power Research Institute. Two of the authors (ND and RS) wish to acknowledge that portions of this work were supported by the U.S. Department of Energy Office of Nuclear Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

REFERENCES

[1] A. Sireli. *Program on Technology Innovation: A Preliminary Study on Decision Support for the Nuclear Power Industry*. EPRI Report 1016732, Electric Power Research Institute. Palo Alto, CA; June 2008.

[2] A. Y. Sireli and C A. Mengers; *Risk Identification for Decision Support for Long-Term Operation of U.S. Nuclear Power Plants*," in Proceedimgs of the 13th International Conference on the Foundations and Applications of Utility, Risk and Decision Theory, July 2-5, 2008, Barcelona, Spain

[3] A. Y Sireli and C. A. Mengers, *Need for Change towards Systems Thinking in the U.S. Nuclear Industry*; IEEE Systems Journal, Issue 3.2, June 2009

[4] *Light Water Reactor Sustainability Program Plan – Fiscal Year 2009*. Idaho National Laboratories, Idaho Falls, ID; September 2008. (Available electronically at https://inlportal.inl.gov/portal/server.pt/gateway/PTARGS_0_2279_13610_0_0_18/LWR_sustainabilty_program_plan_rev%200.3.pdf)

[5] Nuclear Energy Agency Task Group on Safety Margins Action Plan; *Safety Margins Action Plan - Final Report*; NEA/CSNI/R(2007)9; Organisation for Economic Co-operation and Development; Paris, France

[6] J. Riley, K. Canavan, R. Anoba and C. Cragg; *Advanced PRA Modeling and Quantification*; Proceedings of ANS PSA 2008 Topical Meeting – Challenges to PSA During the Nuclear Renaissance; 7 – 11 September 2008; Knoxville, TN; American Nuclear Society, LaGrange Park, IL, USA

[7] E. Thornsbury. *Program on Technology Innovation: Probabilistic Risk Assessment Requirements for Passive Safety Systems*. EPRI Report 1015101, Electric Power Research Institute. Palo Alto, CA; December 2007

[8] E. Thornsbury and S. Hess; *Probabilistic Risk Assessment Requirements for Passive Safety Systems*; Proceedings of ANS PSA 2008 Topical Meeting – Challenges to PSA During the Nuclear Renaissance; 7 – 11 September 2008; Knoxville, TN; American Nuclear Society, LaGrange Park, IL, US