

RISK AND SAFETY WORKING GROUP: PERSPECTIVES, ACCOMPLISHMENTS AND ACTIVITIES

T.J. Leahy⁽¹⁾ and G.L. Fiorini⁽²⁾

(1) Timothy J. Leahy – Idaho National Laboratory (*Timothy.Leahy@inl.gov*)

(2) Gian Luigi Fiorini – Commissariat à l'énergie atomique (*gian-luigi.fiorini@cea.fr*)

I. INTRODUCTION

The Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG) was created to promote a homogeneous and effective approach to assuring the safety of Generation IV nuclear energy systems. The six Generation IV reactor concepts that have been selected by the GIF members potentially present a diverse set of design and safety issues. A number of these issues differ significantly from those presented by the earlier generations of light water reactors. The overall success of the Generation IV program depends on developing, demonstrating, and deploying advanced system designs that exhibit excellent safety characteristics. While the RSWG recognizes the excellent safety record of nuclear power plants currently operating in GIF member countries, it believes that advanced technologies and a coherent safety approach in which safety is “built in, not added on” to the basic designs of nuclear systems hold the promise of making Generation IV energy systems even safer than the current generation of nuclear plants.

The Generation IV Technology Roadmap identifies three specific safety goals for Generation IV systems guides the Generation IV research and development program. The intent of the safety goals is to stimulate ideas for innovative energy systems that would achieve enhanced safety compared to that of the current plants, and to motivate and guide the research

and development necessary to achieve that enhanced level of safety. These safety goals are:

1. *Generation IV nuclear energy systems will excel in safety and reliability.*
2. *Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.*
3. *Generation IV nuclear energy systems will eliminate the need for offsite emergency response.*

The early work of the RSWG focused on defining a safety philosophy for Generation IV systems that is founded on lessons learned from current and prior generations of nuclear technologies, and on identifying the characteristics that may help achieve Generation IV safety goals. The RSWG is presently in the early stages of developing and demonstrating a methodology that will be used to assess and document the safety of Generation IV systems. This paper describes an integrated safety philosophy for Generation IV nuclear systems, desirable attributes to ensure safety, and the RSWG's early thinking about the integrated safety assessment methodology.

II. AN INTEGRATED PHILOSOPHY OF SAFETY

An effective and homogeneous approach to the safety of Generation IV systems must be based on a coherent and well-founded safety

philosophy. In its work to date, the RSWG has recommended that the following postulates should underlie such a safety philosophy:

- **Opportunities exist to further improve on nuclear power’s already excellent safety record in most countries.** As a starting point, the RSWG recognizes that the level of safety that has been attained by the vast majority of operating nuclear power plants (Generation II) in most countries of the world is already very good. Relative to Generation II systems, applicable quantitative safety objectives for third generation (*e.g.* AP1000 and EPR) nuclear power plants are very ambitious and provide a further improved level of safety. The RSWG believes that, although not formally required, further enhancement in the level of safety associated with Generation IV technologies is possible. Such improvements can be realized through advanced technologies and early application of an integrated safety approach driven by an assessment methodology that helps identify improvements to the developing design. Such improvements will focus on safety provisions that will be “*built-in*” to the fundamental design rather than “*added on*” to the system architecture.
- **Safety improvements should simultaneously be based on several elements which will require specific R&D efforts.** These include the notion of “optimal risk reduction”; the adoption of ambitious safety objectives that will drive the research required to attain those objectives; the application of innovative technologies; an emphasis on accident prevention backed up by mitigation; the development of robust safety architecture; and improved means of demonstrating the system’s safety robustness.
- **The diversity of the Generation IV systems and the need for a homogeneous strategy applicable for the design and the assessment of these systems justify an updated safety approach.** The

traditional approach to safety is one that has consisted largely of prescriptive requirements based largely on “engineering judgment”. The notion of the “design basis accident” as a bounding case underlies much of the historical safety basis for nuclear plants that began operation in the sixties and seventies. Advancements and analytical methods developed since then support an updated safety approach. Such an approach must include formal consideration of risk and safety issues throughout the design process, and must provide for prevention and mitigation relative to a broad spectrum of potential accident initiators and conditions.

- **The principle of “defense in depth” has served the nuclear power industry well, and must be preserved in the design of Generation IV systems.** Defense in depth is the key to achieve safety robustness, thereby helping to ensure that Generation IV systems do not exhibit any particularly dominant risk vulnerability. Embodied within the principle of defense in depth is the notion that safety margins must exist as an effective response to uncertainty.
- **The Generation IV design process should be driven by a “risk-informed” approach.** The RSWG believes that safety and economics of Generation IV designs can be positively impacted by formally adopting, as a complement of the deterministic approach, the use of PSA techniques and complementary tools as design drivers throughout the design process.

III. DESIGN AND ASSESSMENT OF INNOVATIVE SYSTEMS

Specific details of Generation IV systems designs must, of course, be left to their respective design teams. The RSWG, therefore, does not offer prescriptive guidance with respect to design issues. Rather, the RSWG has worked to define certain general design attributes or criteria that are believed to offer benefit in terms of helping

to achieve the safety goals for Generation IV systems. Some of these attributes include:

- **The Design Basis for Generation IV energy systems should cover the full range of safety significant conditions.** The historical notion of a single bounding design basis accident must be replaced by a “spectrum” of possible accidents that, while of low probability, represents with high confidence the range of physical events and phenomenology that could conceivably challenge the plant. Specific efforts, both analytical and empirical, should be made for demonstrating the “practical elimination” of initiators, sequences or situations associated with the extremely low residual risk.
- **Objectives and practices for design improvement must be explicit and complementary.** To efficiently establish these practices, **four complementary ways** should be followed by the designer: 1) critical and systematic examination and consideration of feedback from experience; 2) full implementation of the concept of defense in depth in an effective and measurable manner; 3) rationalization of the design approach by the deliberate adoption of the ALARP principle on a cost benefit basis; 4) special attention should be devoted to the reinforced treatment of the severe plant conditions through provisions of measures that provide defense (*i.e.*, prevention and mitigation) against such conditions.
- **The demonstration of a concept’s safety robustness rests on the capacity of the designer and the developer to demonstrate and to guarantee exhaustiveness in the recognition of risks stemming from phenomena considered for the design.** Whenever possible, plant design features based on natural phenomena and physical properties of materials should be used to demonstrate in an “intuitive” way the ability of the plant to arrest the accident progression. This must be done with an adequate degree of confidence, based on an understanding of the

associated uncertainties and the provision of sufficient safety margins in response to those uncertainties.

IV. A METHODOLOGY FOR ASSESSING AND DOCUMENTING THE SAFETY OF GENERATION IV SYSTEMS

One principal focus of the RSWG’s charter is the development and demonstration of an integrated methodology that can be used to assess and document the safety of Generation IV nuclear systems. Although the RSWG is still in the very early stages of developing and presenting such a methodology, this activity is the current focus of the Group, and the elements of the methodology have been largely defined. The methodology is tentatively called the Integrated Safety Assessment Methodology (ISAM).

It is envisioned that the ISAM will be used in three principal ways:

- The ISAM is intended for use throughout the concept development and design phases with insights derived from the ISAM serving to actively drive the course of the design evolution. In this application of the methodology, the ISAM is used to develop a more detailed understanding of design vulnerabilities, and resulting contributions to risk. Based on this detailed understanding of vulnerabilities, new safety provisions or other design improvements can be identified, developed, and implemented relatively early.
- Selected elements of the methodology will be applied at various points throughout the design evolution to yield an objective understanding of risk contributors, safety margins, effectiveness of safety-related design provisions, sources and impacts of uncertainties, and other issues that are important to decision makers.
- The ISAM can be applied in the late stages of design maturity to measure the level of safety and risk associated with a given design relative to safety objectives or

licensing criteria. In this way, the ISAM will allow evaluation of a particular Generation IV concept or design relative to various potentially applicable safety metrics or “figures of merit”. This *post facto* application of the ISAM will be especially useful for regulators and other decision makers who require objective measures of safety for licensing purposes, or to support certain late-stage design selection decisions.

It is specifically NOT intended that the methodology be used to dictate design requirements, that it dictate compliance with quantitative safety goals, or that it in any other way constrains designers. The sole intent is to provide a useful methodology that contributes to the attainment of Generation IV safety objectives, that yields useful insights into the nature of safety and risk of Generation IV systems, and that permits meaningful evaluations of Generation IV concepts with respect to safety.

Attributes of an Effective Safety Assessment Methodology

In formulating a Generation IV safety assessment methodology, the RSWG has sought to incorporate the following attributes:

- The methodology should consist of, or be largely based on existing tools that are widely accepted for their validity. Thus, the methodology should minimize the need for developing new tools and the potentially lengthy period of validation that may be necessary. When necessary, however, the methodology must support incorporation of new analysis techniques to address issues or phenomena specific to advanced energy systems or demonstration of the robustness of those systems.
- The methodology must be comprehensive, understandable, user-friendly, and efficient.
- The methodology must allow for the integration of a diverse range of multi-disciplinary inputs including those that are primarily probabilistic and those that are primarily deterministic in nature, as well

as those that are principally qualitative and those that are principally quantitative.

- Based on the desirability of offering a graded approach to technical issues of varying complexity and importance, practicality and flexibility must be reflected in the methodology.
- Throughout the development process, the safety assessment methodology must help designers understand design vulnerabilities, and how alternative design solutions can reduce or eliminate those vulnerabilities. In order to successfully fulfil this role, the methodology must yield information about which aspects of design contribute most to the level of risk associated with that concept or design. Thus, the methodology must serve to do more than just measure safety after the design is complete. *The methodology must actively contribute to the development of designs that fulfil the safety objectives of Generation IV systems.*
- Importantly, the methodology must provide information that permits an understanding of the level of uncertainty associated with the measured level of safety, as well as an understanding of the sources of that uncertainty.
- Based largely, but not exclusively, on a systematic understanding of sources and magnitudes of uncertainties, the methodology must help identify areas for additional research, data collection, and improved analytical models.
- Within a given concept, the methodology must support comparisons of potential alternative design options.
- The methodology must yield information that allows comparison of a concept or design relative to established safety metrics or “figures of merit.”
- The methodology must yield a mix of both qualitative and quantitative information

that will support eventual licensing and regulatory processes.

- To the extent that is appropriate, the methodology should be consistent with other relevant guidance and documentation including the RSWG Safety Philosophy document (Ref. 1), the PRPP methodology (Ref. 7), and other work including the US NRC NUREG-1860 (Ref. 2), the IAEA TECDOC-1570 (Ref. 3), and others.

ISAM Overview

The ISAM provides an integrated set of tools that reasonably fulfils the list of desired methodological attributes outlined above. Although the ISAM is fundamentally based on PSA, the integrated methodology consists of five distinct analytical tools. It is intended that each tool be used to answer specific kinds of safety-related questions in differing degrees of detail, and at different stages of design maturity. By providing specific tools to examine relevant safety issues at different points in the design evolution, the ISAM as a whole offers the flexibility to allow a graded approach to the analysis of technical issues of varying complexity and importance. The methodology is well integrated, as evidenced by the fact that the results of each analysis tool support or relate to inputs or outputs of other tools. Although individual analytical tools can be selected for individual and exclusive use, the full value of the integrated methodology is derived from using each tool, in an iterative fashion and in combination with the others, throughout the development cycle.

Because the development of the methodology is still in its very early phases, all information concerning the methodology should be regarded as tentative, preliminary, and pre-decisional. At the current time, the RSWG believes that the ISAM will consist of the following major elements:

- Qualitative Safety Features Review (QSR)

The Qualitative Safety Features Review is a new tool that provides a systematic means of ensuring and documenting that the evolving

Generation IV system concept of design incorporates the desirable safety-related attributes and characteristics that are identified and discussed in the RSWG's first report entitled, "Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems." Although this element of the ISAM is offered as an optional step, it is believed that the QSR provides a useful means of shaping designers' approaches to their work to help ensure that safety truly is "built-in, not added-onto" since the early phases of the design of Generation IV systems. Using a structured template to guide the process, concept and design developers are prompted to consider, for their respective systems, how the attributes of "defense in depth" high safety reliability, minimization of sensitivity to human error, and other important safety characteristics might best be incorporated. The QSR is not regarded as a tool that allows an analyst to determine whether or not a developing concept is "good enough", but rather, provides a measure of discipline to help ensure that certain desirable characteristics are incorporated into the design in its earliest phases. The QSR also serves as a useful preparatory step for other elements of the ISAM by promoting a richer understanding of the developing design in terms of safety issues that will be analyzed in more depth in those other analytical steps.

- Phenomena Identification and Ranking Table (PIRT)

The Phenomena Identification and Ranking Table is a technique that has been widely applied in both nuclear and non-nuclear applications. The PIRT provides a structured means of identifying and analyzing a wide variety of off-normal scenarios that potentially challenge the viability of complex technological systems. As applied to Generation IV nuclear systems, the PIRT is used to identify a spectrum of safety-related scenarios or phenomena that could affect those systems, and to rank order those scenarios on the basis of their frequencies, their potential consequences, and state of knowledge related to associate phenomena (*i.e.*, sources and magnitudes of phenomenological uncertainties).

The PIRT is used initially in the pre-conceptual design phase of a system's development, and is applied iteratively throughout the development process. It is to be used as an early screening tool to identify, categorize, and characterize phenomena and issues that are potentially important to risk and safety of a Generation IV system. The PIRT can be focused on very general issues, or on highly specific design issues, depending on the need. The method relies heavily on expert elicitation, but provides a discipline for identifying those issues that will undergo more rigorous analysis using the other tools that comprise the ISAM. As such, the PIRT forms an input to both the Objective Provision Tree (OPT) analyses, and the Probabilistic Safety Analysis (PSA) in identifying mechanisms and initiating events which will challenge the safety functions. In the case of the PSA, the PIRT is particularly helpful in defining the course of accident sequences, and defining safety system success criteria. The PIRT is essential in helping to identify areas in which additional research may be helpful to reduce uncertainties.

- Objective Provision Tree (OPT)

The Objective Provision Tree is a relatively new analytical tool that is enjoying increasing use. The International Atomic Energy Agency (IAEA) has been a particularly influential developer and proponent of this analysis tool. The purpose of the OPT is to ensure and document the provision of essential "lines of protection" to ensure successful prevention or mitigation of phenomena that could potentially damage the nuclear system. There is a natural interface between the OPT and the PIRT in that the PIRT identifies phenomena and issues that could potentially be important to safety, and the OPT focuses on identifying design provisions intended to prevent, control, or mitigate the consequences of those phenomena.

The OPT can be applied early in the pre-conceptual design phase, and iteratively through conceptual design. Note that the OPT is an entirely qualitative analysis method. As such, its purpose is to inform the design process and to help structure inputs that will eventually make their way into the PSA. The OPT can be

extremely useful in helping to focus and structure the analyst's understanding of accident sequence phenomenology, sequence success criteria, and related issues. It will help providing the right requirements (e.g. requested performances and reliability) for the design of the implemented provisions.

- Deterministic and Phenomenological Analyses (DPA)

Classical Deterministic and Phenomenological Analyses, including thermal-hydraulic analyses, computational fluid dynamics (CFD) analyses, reactor physics analyses, accident simulation, materials behavior models, structural analysis models, and the like collectively constitute a vital part of the overall Generation IV ISAM. These traditional deterministic analyses will be used as needed to understand a wide range of safety issues that must guide concept and design development, and will form inputs into the PSA. These analyses typically involve the use of familiar deterministic safety analysis codes. It is anticipated that DPA will be used from the late portion of the pre-conceptual design phase through ultimate licensing and regulation of the Generation IV system.

- Probabilistic Safety Analysis (PSA)

PSA has been widely used in a variety of nuclear and non-nuclear applications since the early 1970s. As a widely accepted, integrative method that is rigorous, disciplined, and systematic, PSA forms the principal basis of the ISAM. PSA can only be meaningfully applied to a design that has reached a sufficient level of maturity and detail. Thus, PSA is to be performed, and iterated, beginning in the late pre-conceptual design phase, and continuing through the final design stages addressing licensing and regulation concerns. In fact, as the concept of the "living PSA" (one that is frequently updated to reflect changes in design, system configuration, and operating procedures) is becoming increasingly accepted, the RSWG is advocating the idea of applying PSA as the earliest practical point in the design process, and continuing to use it as a key decision tool throughout the life of the plant or system. Although the other elements of the

ISAM have significant value as stand-alone analysis methods, to a significant degree, their value is enhanced by the fact that they serve as useful tools in helping to prepare for, and to shape, the PSA once the design has matured to a point where the PSA can be successfully applied.

Fundamentally, the PSA provides a structured means of identifying the answers to three basic questions related to the safety of Generation IV systems. These are:

- What can go wrong?
- How likely is it?
- What are the consequences?

The centerpiece of the ISAM is a “full scope” PSA that considers both internal and external events and models potential accident phenomena from the hypothetical occurrence of an initiating event through the point at which accident progression is either arrested, or offsite consequences are realized.

One of the key strengths of the PSA is that it facilitates a systematic understanding of the uncertainties relating to the safety (or risk) of a Generation IV system. Uncertainties arise from a number of sources. The traditional response to these safety-related uncertainties has been the provision of additional “safety margin” in the design, often based largely on “engineering judgment”, to provide assurance that in the event of any accident, severe loss or damage will not occur. Adding such safety margins is, of course,

expensive, and may also lead to an inappropriate focus on some aspects of design and operation to the detriment of other issues that may, in fact, be more important to safety. By facilitating a disciplined, systematic understanding of the sources and magnitudes of safety-related uncertainties, the PSA will play a key role in helping to ensure that cost and safety issues are more optimally balanced.

V. CONCLUSION

Advanced technologies and a safety approach driven by insights derived from an integrated safety assessment methodology hold the promise of making Generation IV energy systems even safer than the current generation of nuclear plants.

The ISAM is best thought of as a toolkit of useful analysis tools. Although the ISAM is essentially a PSA-based safety assessment methodology for Generation IV systems, the strength of the ISAM is that it offers tools that are tailored to answering specific types of questions at various stages of design development, and that the elements of the methodology complement and support one another in a way that contributes to a much more complete understanding of the range of safety issues. It is anticipated that using the elements of the ISAM in an integrated way will result in optimizing safety, reducing technology development cycle time, reducing development costs, and facilitating licensing of Generation IV systems.

Acknowledgements

The authors wish to thank all members of the Generation IV International Forum Risk and Safety Working Group, past and present, for their expertise and dedication in helping advance the safety objectives of the Generation IV program.

In addition, the authors wish to thank Messrs. Jean Gouvain and Javier Reig of the OECD Nuclear Energy Agency for their steady guidance and very capable support in serving as Secretariat for the RSWG.

References

1. “*Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems*,” Rev. 1, Generation IV International Forum, GIF/RSWG/2007/002, November 24, 2008.
2. “*Feasibility Study for a Risk-informed and Performance-Based Regulatory Structure for Future Plant Licensing* (NUREG 1860).” US Nuclear Regulatory Commission, December 2007.
3. “*Proposal for a Technology-Neutral Safety Approach for New Reactor Designs* (TECDOC-1570).” International Atomic Energy Agency, September 2007.
4. “*Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants* (TECDOC-1511).” International Atomic Energy Agency, July 2006.
5. “*A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors* (NEI-02-02).” Nuclear Energy Institute, May 2002.
6. “*Policy Statement on the Regulation of Advanced Reactor*.” NRC-2008-0237, US Nuclear Regulatory Commission, Federal Register. October 14, 2008.
7. “*Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems*,” Rev. 5, Generation IV International Forum, GIF/PRPPWG/2006/005, November 30, 2006.