STI 10-050

PRA In Design: Increasing Confidence in Pre-operational Assessments of Risks (Results of a Joint NASA/ NRC Workshop)

Robert Youngblood[a*], Homayoon Dezfuli[b], and Nathan Siu[c]
[a]Idaho National Laboratory, Idaho Falls, Idaho, USA
[b]National Aeronautics and Space Administration (NASA), Washington, DC, USA
[c]US Nuclear Regulatory Commission, Washington, DC, USA

Abstract: In late 2009, the National Aeronautics and Space Administration (NASA) and the U.S. Nuclear Regulatory Commission (NRC) jointly organized a workshop to discuss technical issues associated with application of risk assessments to early phases of system design. The workshop, which was coordinated by the Idaho National Laboratory, involved invited presentations from a number of PRA experts in the aerospace and nuclear fields and subsequent discussion to address the following questions: (a) What technical issues limit decision-makers' confidence in PRA results, especially at a preoperational phase of the system life cycle? (b) What is being done to address these issues? (c) What more can be done? The workshop resulted in participant observations and suggestions on several technical issues, including the pursuit of non-traditional approaches to risk assessment and the verification and validation of risk models. The workshop participants also identified several important non-technical issues, including risk communication with decision makers, and the integration of PRA into the overall design process.

Keywords: PRA, Pre-Operational, Decision-Making

1. INTRODUCTION

1.1 Purpose of This Paper

This paper provides an overview of a workshop on "PRA In Design: Increasing Confidence in Pre-Operational Assessments of Risk," and comments on selected points made in the course of those discussions. The workshop was held jointly by the U.S. Nuclear Regulatory Commission (NRC) and the National Aeronautics and Space Administration (NASA), pursuant to a Memorandum of Understanding between those two agencies [1]. The workshop took place November 17-19, 2009 at the Hyatt Regency in Bethesda, MD. Participation was by invitation. Collectively, the participants brought to the workshop a high level of experience in performing PRA, and in applying PRA in diverse decision contexts. Some participants are also members of the community of decision-makers that use PRA, and some participants represent both communities.

The keynote questions for the workshop were the following:

- What technical issues limit decision-makers' (DMs') confidence in PRA results, especially at a preoperational phase of the life cycle?
- What is being done to address these issues?
- What more can be done?

This paper summarizes key points raised during the discussion, and provides additional perspectives that may be helpful to follow-on activities in this topic area.

1.2 Organizational Context

Although NRC does not design/build/operate systems or facilities whereas NASA does, the application of PRA within the two agencies is sufficiently similar that comparison of issues and solutions within the two communities of practice is worthwhile. For example, NRC requires PRA as part of design certification [2], and uses PRA in the context of "risk-informed decision-making" regarding license amendments [3] and in prioritizing and resolving generic issues. NRC has recently participated in the development of consensus standards for PRA (e.g., [4]). NASA uses PRA in certain contexts [5, 6, 7], especially for human space flight. Moreover, with the future involvement of commercial launch services in the national space program, NASA is in the process of implementing a safety goal policy, implying an increased use of scenario-based modeling and application of quantitative safety goals and thresholds to guide risk acceptance decisions.

With respect to this workshop, a noteworthy difference between the two agencies is that most of NRC's current PRA applications involve the nation's fleet of nuclear power plants, which have been operating for many years, whereas NASA's PRA applications often involve new, sometimes unique vehicles and systems that are being conceptualized, designed, and built. Thus, for NRC, the notion of "PRA in design" has recently been stimulated by the submittal of applications for design certification and new plant licensing, while for NASA, many of its PRA applications are in the design context. Consequently, many of the issues raised in the workshop by participants from NASA and its supporting organizations were issues that the reactor community would likely judge are general to PRA, and not just "PRA in design."

1.3 Motivation for the Workshop

The formulation of the workshop was driven by the following considerations. Within the PRA community of practice, it is widely accepted that PRA of complex and high-stakes systems can be useful even at a fairly early stage of design. For example, given a functional description of a design, a scenario-based portrayal of contributors to risk can highlight effects of certain design choices, even at a pre-operational stage, when no system-specific operational experience is available to refine quantification. However, the workshop organizers and participants recognized that many decision makers who are intended users of the PRA results do not share this view on the usefulness of PRA in the design stage.

1.4 Approach

Prior to the workshop, the organizers circulated a white paper to the participants that listed a number of potential issues for discussion. This list included a number of issues that are quite clear to PRA analysts and users, including: the lack of design and operational details (especially early in the design process), controversy regarding the applicability of "heritage data" (i.e., data from operating systems), and the validation of phenomenological models used in the pre-operational PRA. The list also included a number of less well-discussed issues, including: conceptual difficulties in treating the contribution of design errors, the lack of guidance/aids to support decision makers (e.g., in balancing qualitative and quantitative information), the need to support rapid turnaround in some design processes, and the extent to which consensus standards could help.

The workshop itself involved a number of invited presentations covering a wide range of topics (see Table 1). After each group of presentations, the attendees participated in a facilitated discussion of key points suggested by the talks, aiming at developing answers to the keynote questions identified earlier in this paper.

2. SUMMARY OF DISCUSSIONS

In general, the workshop participants supported the use of PRA in the design stage. Due to the large fraction of PRA practitioners participating, this was largely "preaching to the choir;" nevertheless, the

Table 1: Workshop Presentation Topics

	Presentation Topic
1	Decision-Making at NASA
2	ESAS (Exploration Systems Architecture Study) Experience and Lessons Learned
3	Perspective from Using PRA in Designing Advanced Reactors
4	Validation of PRA Models
5	NRC Experience with Design Certification PRAs
6	NASA Modeling & Simulation Standard
7	Simulation in PRA at the Design Stage
8	Application of the PRA to Constellation Systems
9	Use of Heritage Data
10	Communicating PRA Results to Decision Makers

participants were able to identify benefits of PRA realized in actual design situations, as well as identify and discuss the challenges that they have faced in these situations. These benefits included the support of design trade-offs ("trades"); the identification of potentially effective non-traditional solutions (e.g., instead of simply relying upon redundancy); improved team understanding of the design; and the identification and prioritization of issues for which additional research and development is needed. These benefits derive from PRA's comprehensive treatment of scenarios, identification of key weaknesses and dominant contributors, and establishment of a "level playing field" within which to assess the relative significance of contributors.

Given the motivation of the workshop, most of the discussion centered on how to improve the usefulness and use of pre-operational PRAs. The subsections below summarize points made at the workshop in response to the keynote questions. Section 3 furnishes additional perspectives on certain key points made at the workshop.

2.1 What technical issues limit decision-makers' confidence in PRA results, especially at a preoperational phase of the life cycle?

During the workshop presentations and subsequent discussions, the participants raised a large number of technical issues that they perceived to affect decision maker confidence. Some of these issues were previously identified in the pre-workshop white paper. Many of the issues were generic to PRA, regardless of life cycle phase, although they can take on greater importance during the design phase. The issues varied in scope and level of detail, ranging from philosophical concerns (e.g., distinguishing between ignorance and uncertainty) to modeling questions (e.g., the need for dynamic simulation methods to identify and analyze scenarios).

Table 2 provides a high-level categorization of the key issues raised, as well as some of the specific issues discussed. It can be seen that although the participants identified a number of issues related to PRA methods, tools, and data, many of the issues covered by Table 2 are not technical in nature. These issues, voiced and discussed extensively despite the organizers' initial desire to limit the workshop to technical issues, appeared to reflect a general belief among the participants that the non-technical issues were at least as important, if not more important, than the technical ones. One participant was adamant in declaring that technology was not the problem with PRA.

Regarding the non-technical issues, the participants were particularly concerned with issues in communication with decision makers. There was considerable discussion regarding good communication practices (e.g., engaging with decision makers to develop a shared understanding of PRA results and implications), communication tools (e.g., simplified matrices to represent the full

Table 2: Factors Affecting Design-Stage PRA Acceptance[1]

Categories of Challenges	Specific Challenges (Examples)	Sample of Points Raised in Presentation or Discussion
PRA Technology[2]	Appropriate methods for given problem	Some recent studies are using simulation-based methods (instead of traditional event tree/fault tree tools).
	Appropriate incorporation of science/engineering (especially with respect to success criteria)	Subject matter experts need to be involved; phenomenological concerns (e.g., physics of failure) need to be integrated into the analysis .
	Ability to address additional applications	Some have proposed the use of PRAs to identify design-basis events (that will then be addressed through deterministic requirements).
	Appropriate credit for "fixes" to identified problems	The effectiveness of design changes to address identified vulnerabilities can be a significant source of uncertainty.
	Avoiding excessive detail	For systems in the early stage of design, overly detailed models may erode decision maker confidence, as well as waste analysis resources.
	Avoiding underrepresentation of uncertainty	Analysts can be tempted to ignore uncertainties, or use ad hoc methods that understate uncertainties.
	Methods, models, tools, and processes for timely support of design process (with potential rapid changes)	As the design evolves, even the fundamental question to the PRA can change (from "what could be the risk" to "what is the risk"); the methods and tools need to change accordingly.
	Capturing design flaws	Some past design-stage PRAs have not been successful in identifying design flaws (that were identified via other processes). The PRA tools used can "drive the answers."
PRA team makeup and expertise	Ensuring collective subject matter expertise in systems, phenomenology, probability and statistics	In addition to education and training appropriate to the systems and problems of interest, a program for certifying PRA proficiency should be pursued.
	Accommodating changes in analysis teams (possibly entirely different teams) as design progresses	As the design progresses, the PRA might be worked on by different analysts, or even different analysis teams.

[1] A number of these factors are common to PRAs for operating systems and facilities as well. However, their importance is accentuated by characteristics of the design process (e.g., the need for rapid turnaround, the involvement of multiple teams with different roles, detailed objectives, and perspectives).

[2] The issues of lack of design detail and the lack of operational data are well-recognized and not expanded upon in this table.

Table 2: Factors Affecting Design-Stage PRA Acceptance (continued)

Decision maker background and perspectives	Developing a common understanding of PRA results and insights	Risk characterization, a key process in risk-informed decision making, needs to involve a two-way dialog between the decision maker and the PRA team. Various tools discussed at the workshop (e.g., credibility scales, decision maker report cards) can help this process.
	Ensuring understanding of what a PRA is and isn't	"All models are wrong, but some models are useful."
	Accommodating different decision maker preferences	Some decision makers have a deterministic analysis background; the PRA community needs to do a better job in communicating. Guidance on the management of uncertainty would be useful.
	Increasing decision maker appreciation of the potential value of PRA	In addition to improving communication (including improving summaries and transparency of documentation), PRA "success stories" should be documented.
Consensus PRA standards and guidance	Identifying good practices for PRA in design	Past efforts suggest lessons regarding process-related practices (e.g., regarding team makeup, top-down vs. bottom-up analysis approaches, document control).
	Developing consensus standards and associated guidance	The American Society of Mechanical Engineers is developing a consensus PRA standard for non-light water reactor applications that will address some aspects of PRA in design. NASA's standard on modeling and simulation standard is also relevant.
Programmatic context	Ensuring PRA is integrated into the design process	PRAs need to be performed quickly and early enough to affect design development, rather than as after-the-fact confirmatory analyses. There needs to be good cross-communication between teams.
	Ensuring use of PRA results	On one side, organizational commitment is important. On the other, PRAs need to provide value at each stage in the process.

spectrum of PRA results, their bases, and their credibility), and the varying backgrounds and perspectives of decision makers (which affect the nature and success of communication).

There was also considerable discussion on the programmatic context of the PRA. For example, a number of participants emphasized the need to situate the PRA activity in the proper decision-making context, and the need to integrate the PRA into the design activity, rather than having it be an isolated add-on to the overall effort.

It should be noted that one participant took issue with the view that PRA should furnish risk metric results to the decision maker, who then uses these results (along with uncertainty information) in his/her own way to formulate expectations regarding the performance of decision alternatives. That participant felt that this purely prognostic view of PRA at the design stage is too narrow: that the PRA should be understood not just as an unconditional (albeit uncertain) prediction of performance, but more importantly for mapping from presumed (or perhaps "committed") performance levels of components and subsystems to top-level risk metrics. In short, the design-stage PRA should be seen as a tool for allocation. Its output is not prognostic, but only conditionally prognostic: its results can

apply only if the input levels of performance are attained. Recent developments in risk management stress this proactive use of risk analysis [8, 9].

2.2 What more can be done?

At the workshop, there was broad agreement on the desirability of integrating PRA at earlier stages of design evolution. This is true not only so that the benefits of PRA can be realized earlier, but also because integration of PRA elements at that stage changes the very process: the PRA sensibility changes the formulation of alternatives and the preliminary screening of them.
Both agencies invest substantially in training PRA practitioners. Some discussants suggested some kind of certification for analysts, as a way of promoting decision maker confidence in the analyses. Some suggested that training courses need to stress capabilities and limitations of the PRA techniques presented.

There were also suggestions for training material to support communications with decision makers. Potential topics include:

- What the probabilistic results (e.g., the results of Bayesian analysis) mean.
- How much the decision maker can trust the PRA results.
- What the decision maker should be asking: key assumptions, value of uncertainty reduction, verification and validation of PRA models.

There was some consensus regarding the value of PRA standards. Given that NRC in particular has invested substantially in standards intended to help streamline its decision processes, this was not surprising. However, some participants noted that the existence of standards can inhibit technical innovation (e.g., regarding alternative PRA methods and models). However, participants felt that value would be added by standards for PRA communicators / practitioners that:

- Address how and how much we should provide regarding uncertainty, assumptions, limitations, applicability;
- Promote integration of PRA effort within a program (e.g., within a design activity);
- Address development and application of PRA at different stages of project life cycle;
- Place a premium on individual analyst capability;
- Address broader issues in uncertainty analysis, such as the important issue of knowledge gaps, including model uncertainty and "unknown unknowns."
- Present improvements in techniques for communicating full uncertainty to the decision maker, going beyond the uncertainties only arising due to model parameter uncertainties.

Many participants indicated that investment should be made in the validation of models: not just "review," but calibration of PRA models with experience. It is not practical to compare rare event frequencies with experience, but much more could be done with intermediate model results (e.g., model predictions at subsystem levels) than is normally attempted. Some effort typically goes into what can be called validation of unconditional basic event probabilities; but validation of the predicted frequencies of *combinations* of events is much less typical.

A number of participants stated that increased stress should be placed on simulations integrating phenomenology considerations and reliability considerations. In some quarters, this has been underway for decades, but improvements in computers and software currently enable much more progress to be made in this area.

2.3 Other Comments

Surprisingly for some participants, there was significant discussion regarding the application of the term "PRA" itself. A number of participants indicated that, in their practical experience, there is a lack of general agreement on the definition of the term, and that "PRA" is often interpreted to mean a large-scale, highly-detailed event-tree / fault-tree analysis, rather than a probabilistic assessment of risk (as defined by the classical risk triplet of Kaplan and Garrick [10]) performed using whatever methods, models, and tools are the best match for the current decision problem, and at whatever scope and level of detail are required. For those participants concerned with the more narrow interpretation, their particular concerns involved "PRA's" implication of: (a) a certain style of modeling that may not be consistent with other engineering disciplines' views of a problem (which can affect understanding and confidence); (b) may not be suitable for dynamic systems (e.g., flight systems); and (c) a complex and expensive enterprise.

3. CONCLUDING REMARKS

While many of the suggestions discussed above would materially improve PRA, and make its results more easily usable by decision-makers, these effects will not by themselves guarantee increased acceptance of PRA by the broader community. In fact, in contrast to the distrust of PRA noted above, Hubbard [11] suggests that the use of "soft" risk assessments supporting risk management programs is increasing at a great rate, despite clearly suffering more technical shortcomings than PRA does.

In addition to this, Hubbard identifies several key characteristics of different risk management practices, some of which distinguish certain soft risk assessment practices from potentially-better practices. One of those key characteristics is verifiability. As discussed earlier in this paper, the point was made strongly at the workshop that PRA could do a lot more in this area than it has in the past. Many PRA inputs are validated up to a point, but it is impractical to "validate" the predictions of very low event frequencies. However, it may be practical to validate predictions regarding intermediate state frequencies (e.g., frequencies of combinations of failure events). In an engineering community, the practitioners need to be told and given the resources to do this, but currently this tends not to be the general practice.

Certain trends already underway point to a gradual reduction of the barrier between the PRA community and the more established portions of the design community.

One trend helping to erode barriers between PRA and traditional design is the involvement of PRA perspective in the design process from the beginning. Currently, this may imply involving a PRA practitioner in the preliminary discussion of design concepts, but eventually, it could be hoped that more members of the design community will themselves have some PRA expertise, helping to erode the gap between "them" and "us." A related trend is the increasing discussion of top-level safety goals. In principle, these can be addressed after the fact without involving PRA people in early discussions, but having the goals up front at an early stage of design can only help.

Another trend is the increasing unification of risk/reliability modeling and phenomenological modeling. These functions are still separated in many organizations, but in some organizations, some efforts address both modeling aspects in a unified way. This cannot but erode barriers between PRA and design. The potential benefits of unified modeling have been obvious to the technical communities for generations, and this kind of modeling has been tried sporadically, but for many real-world applications, unified modeling has not been computationally feasible in many areas until recently. As modeling of this kind becomes more widespread, the organizational and cultural barriers will tend to erode further, as members of currently-isolated communities collaborate actively in the formulation, validation, and application of these models.

Overall, the workshop was a very useful activity for NRC and NASA. However, recognizing that the topic of "PRA in design" is one of many of interest to both agencies, follow-on joint activities will be considered under the Memorandum of Understanding. We note that international interest in the topic is increasing. For example, the Organization for Economic Cooperation and Development/Nuclear Energy Agency/Committee for the Safety of Nuclear Installations' Working Group on Risk Assessment has initiated a task on PRA for advanced reactors. Such activities may provide a useful means to address key issues raised in the NASA/NRC workshop.

Acknowledgements

This workshop was jointly sponsored by NASA and the USNRC. This paper has drawn on significant contributions by the workshop participants. The authors gratefully acknowledge the substantial assistance of Daniel Henry, Tony Koonce, and Kurt Vedros (Idaho National Laboratory) in the compilation of workshop discussions, and the assistance and review comments provided by S. Lai (NRC).

References

[1] Memorandum of Understanding between the National Aeronautics and Space Administration and the U.S. Nuclear Regulatory Commission Concerning Collaborative Research in Risk and Reliability Analysis Methods and Applications, January 7, 2009.

[2] U. S. Code of Federal Regulations, Title 10, Section 52 (10 CFR 52).

[3] U. S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174 Rev. 1, 2002.

[4] American Society of Mechanical Engineers, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME/ANS RA-S-2008, 2008, and Addendum A, ASME/ANS RA-Sa-2009, 2009.

[5] NPR 8715.3C, "NASA General Safety Program Requirements (w/ Change 4 dated 7/20/09)" (National Aeronautics and Space Administration, March 12, 2008).

[6] NPR 8705.2B, "Human-Rating Requirements for Space Systems (w/change 1 dated 12/7/2009)" (National Aeronautics and Space Administration, May 6, 2008).

[7] "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," Version 1.1 (National Aeronautics and Space Administration, August 2002).

[8] NPR 8000.4A, "Agency Risk Management Procedural Requirements" (National Aeronautics and Space Administration, December 16, 2008).

[9] NASA/SP-2010-576, "NASA Risk-Informed Decision Making Handbook" (National Aeronautics and Space Administration, April, 2010).

[10] S. Kaplan and B.J. Garrick, "On the Quantitative Definition of Risk," **Risk Analysis 1**, 11-27(1981).

[11] Douglas W. Hubbard, *The Failure of Risk Management*, John Wiley & Sons, Inc. (Hoboken, New Jersey, 2009).