PRA-based risk management: History and perspectives

By B. John Garrick

A key player in the development of probabilistic risk assessment methodology for the nuclear industry highlights some of the milestones along the way.

Many excellent papers have been written on the evolution and history of probabilistic risk assessment (PRA).[1] The purpose of this article is to put a somewhat different spin on the usual history of PRA by making more visible the contributions of nuclear plant owners and operators, as well as their consultants and suppliers. It is not my intent to provide a detailed chronological history of the development of PRA, but rather to highlight selected milestones in the evolution of PRA, with an emphasis on risk management practices.

The events that led to the development of PRA were primarily related to the inadequacies of the early methods that were used to assess the safety of nuclear power plants. Early nuclear reactor safety analysis involved the defense-in-depth concept and a design basis accident approach to ensure safety. Both concepts have their roots in the Manhattan Project, and both have their merits, although I have never been a proponent of the design basis accident approach. The primary shortcoming of these methods had to do with the absence of knowledge about the likelihood or frequency of severe accidents. In particular, quantitative methods were lacking for determining the safety margins of engineered barriers and safeguards to protect the plants. In the mid- to late 1950s, reactor safety analysts (myself included) recognized the need to embrace the uncertainty sciences to better represent the risks involved in the operation of nuclear power plants.[2] While there was growing concern about the lack of quantitative methods, there wasn't much action until some time later.

An effort that made clear the need for more quantitative methods of nuclear safety analysis was a 1957 U.S. Atomic Energy Commission (AEC) report, *Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants* (WASH-740), known as the Brookhaven Report. Concern about the risk of accidents and the need for a better technical basis to support enacting legislation (the Price-Anderson Act) to provide insurance against nuclear plant accidents were the motivating factors for the Brookhaven Report. The purpose of the Price-Anderson Act, which became law on September 2, 1957, is to provide adequate funds for liability claims of members of the public in the event of a nuclear power plant accident. The Price-Anderson Act was also a major factor of the eventual project known as the Reactor Safety Study (RSS). The Brookhaven Report added clarity to the possible consequences of a major accident at a large nuclear power plant, but it did not present convincing evidence on its likelihood of occurrence. The Brookhaven Report exposed the potential damage of a major accident but did not attempt to quantify the likelihood of such an accident. It did, however, elevate consciousness regarding the need to better quantify the consequences of severe accidents.

For several years after the publication of the Brookhaven Report, the emphasis was on the type of accident that was the focus of the study, the large loss-of-coolant accident (LOCA). The large LOCA surfaced as the *de facto* design basis accident. It emphasized the dependence of the integrity of the containment systems on the successful operation of emergency core-cooling systems (ECCS). Years of study, debate, congressional hearings, and field tests followed in an effort to better understand the reliability of ECCSs and the consequences of such accidents. The result was a growing interest in improving the analytical models by including probabilistic principles in accident analyses. While many of us had known for a long time that more quantitative risk methods needed to be developed for analyzing nuclear reactor safety, the Brookhaven Report, its impact, and the congressional deliberations added urgency to the quest for better methods.

In the period from 1959 to 1970, things began to happen on the analytical front as a flurry of papers, reports, and presentations began to appear, many of which are chronicled in my 1968 Ph.D. thesis[3] on nuclear plant risk assessment. Institutions, companies, and professionals published papers and reports advocating greater use of quantitative methods of nuclear power plant safety analysis, including E. Siddall,[4] of Canada, Atomics International,[5] Planning Research Corporation,[6] F. R. Farmer,[7] of the United Kingdom, Holmes & Narver,[8] Chauncey Starr,[9] and B. J. Garrick,[10] to name just a few. A detailed search of the literature would probably find many more.

There was resistance to the use of probabilistic methods, and there still is, although much less. Much of the criticism was based

B. John Garrick (<bjgarrick@aol.com>), an ANS Fellow and member since 1956, is a founder of the consulting firm Pickard, Lowe and Garrick Inc. He retired from the firm as President, Chairman, and Chief Executive Officer in 1997. *This article is adapted from a paper he presented on November 14, 2013, at the closing plenary session of the Topical Meeting on Risk Management for Complex Socio-Technical Systems, held in conjunction with the 2013 ANS Winter Meeting.*

on the view that the necessary data for such analyses were not available and that the plants were too complex. This was, in my opinion, because of a statistical view of the world rather than a probabilistic view. My colleague the late Stan Kaplan said it best: "Statistics is the science of handling data; probability is the science of handling the lack of data." Also, there are two schools of thought when it comes to data, one that says there is never enough data, and the other that claims we never use the data we have. Both are probably correct, depending on the circumstances. I just happen to be of the latter school.

As an example of resistance against the use of probabilistic methods, consider the Task Force on Nuclear Safety, Licensing, and Risk, which was put together in 1973 by the AEC regulatory staff. The task force was led by Malcom Ernst, and its report, *Study of the Reactor Licensing Process,* is known as the Ernst Report. A conclusion of this report was that the complexities associated with the design and operation of the reactors then operating exhibited so many technical challenges that a quantified risk assessment would be impossible to produce. This is not a criticism of Ernst, as he and the task force members were all very competent choices. It is more a reflection of the thinking at the time.

The Reactor Safety Study

In spite of the resistance against the use of more quantitative methods, a series of events and the growing number of large nuclear power plants coming on line in the 1960s and 1970s resulted in increasing pressure to find a better measure of the health and safety risk of nuclear power. Again it was the Price-Anderson Act that was in the middle of things, as its extension by Congress was under consideration, and the question of the risk of nuclear power was still an open one in the minds of many, including members of Congress. The risk question was further clouded by information coming out of the AEC research program on the performance of ECCSs, which I mentioned earlier as being critical to maintaining containment integrity during a major LOCA. These factors had a lot to do with a letter sent in 1972 by Sen. John O. Pastore, chairman of the Joint Committee on Atomic Energy, to AEC Chairman James Schlesinger to initiate a project to better answer the risk question. I even had an opportunity to express my views to Schlesinger on such a project, which was to become known as the RSS. The AEC eventually chose Prof. Norman Rasmussen, of the Massachusetts Institute of Technology, to lead the study, and Saul Levine, of the AEC's regulatory research staff, to generally manage the project. A key figure in the course of events surrounding the startup of the study and its review was the noted reactor physicist Herbert Kouts, of Brookhaven National Laboratory, who was not optimistic about the ability to estimate the probabilities of nuclear reactor accidents. As noted earlier, he was not alone in his skepticism.

A factor that had a lot to do with the success of the RSS, besides the outstanding leadership of Rasmussen and Levine, was the decision to reach outside the boundaries of the AEC for experts more in tune with using contemporary systems analysis methods to analyze system performance. It was the aerospace community that developed the application of the fault tree methodology, which really derived from the fundamentals of switching algebra developed at Bell Labs. The fault tree method, together with the event tree concept, which was borrowed from the decision analysis field, were critical to the success of addressing the complexities of nuclear power plants that many believed were beyond comprehensive modeling. The RSS study team, made up of some 40 scientists and engineers, had just the right mix of expertise on how nuclear power plants work and the fundamentals of probabilistic modeling. Had the decision not been made by the project leaders to reach beyond the AEC for specialists in plant and system analysis, the project would not have been as successful as it was.

The Reactor Safety Study team, made up of some 40 scientists and engineers, had just the right mix of expertise on how nuclear power plants work and the fundamentals of probabilistic modeling.

Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants (NUREG-75/014 [WASH-1400]) was published in 1975 and was the first credible assessment of the risk of nuclear power. It resulted in a step change in the understanding of the risk of nuclear power plants and how to quantify risk. Above all, it put the large LOCA in perspective as neither a major contributor to risk nor necessarily a logical basis for design. It showed that most accidents that involved releases resulted in small consequences and provided the important perspective that the major contributors to risk were transients, small LOCAs, and human error.

The RSS also took the first important step toward quantifying the impact of external events, although much more would be done in this area later. It cast doubt on using a design basis accident as the basis for managing risk and moved the thought process to scenarios and their likelihood as the most important design considerations, but that too was better developed later. In sum, the RSS was the beacon for a completely new direction in the management of the risk of nuclear power plants.

The acceptance of the RSS as a completely new paradigm was not without some setbacks immediately following its publication. Even today it has its skeptics, but their voices are diminishing. While there was a period when the study was rejected by even the U.S. Nuclear Regulatory Commission, several events, such as changes between the draft and the final report, critical reviews by the American Physical Society, and, most notably, the review by the so-called Lewis Committee,[11] eventually led to focusing on its strengths rather than just its weaknesses. The pivotal event in the RSS being reembraced by the NRC was the recognition that the Three Mile Island-2 accident scenario was actually identified in the study, even though it involved a different reactor and resulted in a different end state.

As time would show, the strong points of the study greatly overshadowed its perceived weak points, which primarily had to do with its treatment of uncertainty and the advocacy nature of the executive summary. The greatest outcome of the study, in my view, was its focus and perspective on the real issues of nuclear power plant accidents and the road map it provided for the rest of us to pursue the resolution of unresolved issues.

Zion and Indian Point PRAs

While the TMI-2 accident was a stimulant to increasing the credibility of the PRA methodology, the NRC continued to struggle with how best to implement PRA into its regulatory framework. But at about the time of the TMI-2 accident, another activity related to the RSS was under way that had an impact on plant-specific applications of PRA, and I was fortunate enough to be directly involved. At issue was a petition by the Union of Concerned Scientists to shut down Units 2 and 3 of the Indian Point plant.[12] The concern was the close proximity of the plant to New York City. Since the Zion plant was similarly close to Chicago, and the outcome of the petition could affect it as well, the utilities involved at the time decided to collaborate on the response to

the petition. The two primary issues in the ensuing Atomic Safety and Licensing Board hearings were (1) whether the plants should be permitted to continue operation and (2) whether costly backfits should be installed to reduce the risk of severe accidents. The backfits under consideration were a filtered-vented containment, a refractory core ladle, and a hydrogen combiner.

Full-scope PRAs were specifically performed for the Zion[13] and Indian Point[14] nuclear power plants to determine the safety adequacy of the as-built design of these plants in light of the claims made by the plants' opponents and to quantify the risk-reduction benefits of the proposed backfits. The lead consulting firm for performing the PRAs was Pickard, Lowe and Garrick Inc. (PLG). Other members of the team included Westinghouse, the owner/operators of the plants, and Fauske & Associates. Due to the large stakes involved with respect to the Zion and Indian Point studies, it was necessary to extend the PRA methods that were developed in the RSS in the treatment of external events and uncertainties and the consideration of plant- and site-specific issues. The Zion/Indian Point studies closely followed the first commercial plant PRA that the PLG team performed on the Oyster Creek nuclear plant. PLG went on to perform some 40 PRAs covering U.S. plants. A paper was published discussing the results of 21 of the 40 studies.[15]

The results of the hearings that followed the completion of these PRAs (1981 for Zion and 1982 for Indian Point) were favorable to the owners and operators of the plants. There were three major outcomes of the PRAs and the hearings. First, the PRA results were accepted as a basis to justify the continued operation of the plants without the need for backfits. Second, the PRA results indicated that the backfits would have a negligible impact on the overall risk. Third, the PRAs identified several low-cost changes in the plants that would have a favorable impact on risk. The precedent was set in these hearings[16] that PRA results provided a legal basis to resolve regulatory issues.

So, where do the Zion and Indian Point studies fit in the historical development of PRA? While it is clear that the single most important advancement in PRA was the RSS, there is a strong case for the view that the second most important advancement was the plant-specific, full-scope studies performed by industry on the Zion and Indian Point nuclear power plants. My view of the importance of these studies is biased by my having been the director for both of them as part of the PLG team, as well as the director of the first commercial plant PRA—the Oyster Creek study—following the RSS.

To put in context the contribution of the Zion and Indian Point studies, it should be noted that the purpose of the RSS was primarily to address the risk of nuclear power in general, not necessarily the risk of a specific plant. Specifically, the charter of the RSS was to address the question "What is the risk associated with the operation of 100 nuclear power plants in the United States?" Of course, the RSS team used specific plants as surrogates to achieve the necessary level of detail to answer the broader question of the risk of nuclear power in the United States in general, and we can be thankful that they did. But it was clear when we began the Zion and Indian Point studies that we needed to tweak the RSS methodology to achieve our intended goals. The RSS areas requiring additional work were the collection and processing of data and the treatment of uncertainty, the containment response analysis, the analysis of external events, and the atmospheric dispersion model. At the time of the Zion/Indian Point studies, there were no regulatory policies, rules, or regulations on the use of PRA. The incentive was very real in a risk management sense, as the case had to be made for the safety of the two plants to avoid the possibility of their being shut down.

The PRA team for the Zion/Indian Point studies was also under great pressure. The good news is that everyone understood what the stakes were and the team was provided the funds necessary to do the job—a rare opportunity for a project team. We were able not only to extend the capabilities of the RSS PRA model as noted earlier, but also to add some wrinkles of our own, such as the triplet definition of risk,[17] a scenario approach to risk assessment, and a matrix formalism for assembling the plant, containment, and site models. The matrix formalism enabled a transparent and systematic way of assembling the various models and, more important, provided a rigorous means of performing diagnostics that allowed for ranking the importance of scenarios and input and output states of the models, namely the plant, containment, and site models. A signature achievement of the whole team involved in the study was the rigor of the containment response analysis and the comprehensiveness of the off-site consequence model. While PLG provided the framework for the containment response analysis, it was the combination of Westinghouse and Fauske & Associates that gave it the depth to set it apart from previous studies and make it the model for future studies. Table I summarizes the contributions of the first few full-scope PRAs developed by the PLG PRA team. The Zion and Indian Point studies were responsible for most of the developments.

TABLE I. INDUSTRY-SUPPORTED PLG PRA ADVANCEMENTS

- Performed first commercial plant-specific, full-scope risk assessments: Oyster Creek, Zion, Indian Point-2 and -3, Seabrook, Midland, Browns Ferry, and Bellefonte
- Developed the scenario approach to probabilistic risk assessment
- Integrated and propagated uncertainties and external events through the model
- Developed matrix formalism for assembling model modules and performing diagnostics
- Developed atmospheric dispersion methods accounting for directional dependence and terrain-specific features
- Developed and defined numerous concepts, terms, and algorithms now a common part of probabilistic risk assessment: triplet definition of risk, the probability of frequency concept, plant damage states, containment event tree, family of curves representation of risk, seismic risk curve, and Bayesian data processing techniques

This industry story is not often included in papers that are written on the history of PRA. Most often such histories focus almost exclusively on the accomplishments of the NRC and its contractors, and certainly, they have been the major players overall. The above is just a reminder that industry was the most active party during the critical years when the RSS was being challenged for its credibility and did not have the full support of the nuclear and regulatory communities.

The NRC and PRA

Having recognized the nuclear industry for its contribution to PRA, it is appropriate to recognize important contributions of the NRC in advancing PRA. The most obvious is the RSS itself, although there are extenuating circumstances. The RSS started not as an NRC project, but as an AEC project, and when it was finished, for a time it was actually rejected by the NRC on the basis of a set of critical reviews. It was embraced following the TMI-2 accident, but the adoption of PRA as a major element of the licensing and regulatory process has been slow. Among the events that boosted its position in the

regulatory arena were the industry studies just described, the TMI-2 accident, the Kemeny Report[18] and its recommendations on cost-benefit and less dependence on design-basis accidents, the updated version of the RSS, namely NUREG-1150,[19] and encouragement from the NRC Office of Research to increase the use of PRA in its licensing activities. An important NRC event took place in 1986 that was influenced by earlier work of the Advisory Committee on Reactor Safeguards (ACRS) under the chairmanship of the late David Okrent. That event was the NRC's issuing a policy statement establishing qualitative safety goals and associated quantitative health objectives for measuring the achievement of the goals. This policy statement was originally published in the August 4, 1986, issue of the Code of Federal Regulations. The ACRS made clear its position that the RSS methodology was the best approach for measuring the quantitative component of the safety goals.

For more than two decades, the NRC has been promoting the concept of a "risk-informed" regulatory practice. Probably no one would disagree with a cautious approach to transitioning to a licensing process where quantitative methods of risk assessment play a major role. Many do believe, however, that the transition has been unnecessarily slow and clumsy—clumsy because in many instances, the burden on the licensee has been to satisfy both traditional licensing requirements and those having to do with risk-informed practices. While all U.S. plants currently have some level of a plant-specific PRA, almost four decades after the issuance of the RSS, there is still no regulation or requirement for nuclear power plants to have or maintain a PRA. The individual plant evaluations required only a systematic search for plant vulnerabilities. That requirement did not specify performing a PRA, although many plants chose to do so. Under 10 CFR Part 52, new nuclear power plants are required to have a Level 1 and Level 2 PRA (plant and containment release model) and to maintain and upgrade the PRAs according to requirements specified by the regulations.

This is not to say that the NRC hasn't been anticipating a larger role for PRA, because it has, especially as a result of the urging of the ACRS. It is simply a matter of how long it is taking. An examination of the policy statements, memoranda, regulatory guides, and even regulations that have been generated to better risk-inform the licensing practice is evidence that risk assessment practices are wedging their way into the licensing process. Why must it take so long? Several reasons have been put forth. One is the inertia that comes from the frame of mind that if the existing system works, why fix it, especially if it involves major new skill levels. There is the simple matter that some people just don't believe in quantitative methods based on probabilistic considerations. There is also the matter of how the regulations are interpreted. One interpretation is that the Backfit Rule (10 CFR 50.109) does not allow the NRC to require plant-specific PRAs because they are not cost beneficial. In fact, as the Zion/Indian Point studies indicated, there is clear evidence that they are cost beneficial. Finally, there are outside influences against probabilistic methods in the form of environmental and antinuclear groups.

Unlike the spirited use of PRA by the industry to deal with shutdown petitions in the late 1970s and early 1980s following the completion of the RSS, the level of enthusiasm of the industry as a whole toward PRA seems to have lessened, although there are the usual exceptions. For example, one utility that is recognized as a leader has adopted PRA not only to address generation risk but also to provide input to their business model. Nevertheless, there has been a substantial switch in support for PRA since the 1980s. In the 1980s, the industry—or at least a small but important sample of the industry—was enthusiastic because of the direct benefits it received from PRA, while the NRC was having its doubts. Now it appears that the NRC is exhibiting more interest in upgrading the use of PRA than is the industry, as reflected by the NRC's interest in increasing the scope of the studies[20] and the current effort to upgrade the probabilistic treatment of external events. Part of this renewed interest is being driven by the Fukushima Daiichi accident and the recognition that had a more comprehensive PRA been available on the Fukushima Daiichi reactors, it is possible that the consequences would not have been as economically disastrous as they were (and continue to be). But the main reason for signs of more rapid engagement of risk-informed licensing practices is that the NRC now has strong advocates of the PRA thought process at all levels, including the staff, the ACRS, and the commissioners.

The main reason for signs of more rapid engagement of risk-informed licensing practices is that the NRC now has strong advocates of the PRA thought process at all levels, including the staff, the ACRS, and the commissioners.

For PRA to reach its full potential in terms of benefits, it is essential that the industry recapture the leadership role it had in the 1980s. The plant owners are the real plant experts and are who we depend on in the event of a severe accident. It is my view that one of the reasons the industry has become less enthusiastic about PRA is that some aspects of it, particularly the treatment of external events, have gotten off track and appear to plant owners and operators to be out of control. I believe they are correct in that regard. The events involved are the impact on risk of phenomena and external events such as fires (both external and internal), earthquakes, and floods. The "off track" observation comes from the view that the efforts are being guided by attempts to answer the wrong question, which is "What is the risk of such threats?" The right question is "How do these threats affect the risk of the nuclear power plant?" In other words, the first question needs to be answered only to the extent of determining its impact on nuclear plant risk, not necessarily to the extent normally required for a stand-alone risk assessment. There is a big difference in interpretation between the two, which is clearly manifested when uncertainty is taken into account. The ongoing work to answer the fire question, for example, is in a runaway mode, as could be the case for earthquakes and floods if actions are not taken to correct the situation.

PRA-based risk management

The case for PRA-based risk management is very simple. Almost all of the PRAs have exposed ways to reduce risk that very likely would not have been possible without the rigor and comprehensiveness required of a PRA. The NRC and industry are practicing risk management in a number of ways.

The NRC has developed independent models for each commercial nuclear power plant under the Standardized Plant Analysis Risk (SPAR) program.[21] The SPAR models serve as a tool for communicating with licensees by allowing comparisons with each respective licensee's PRAs. The differences in the comparisons result in either revisions of the SPAR models or the identification of candidate technical issues for resolution. The SPAR models are also used to

perform risk-informed reviews of license amendments. PRAs are also used to support the licensees' inspection and surveillance activities and to risk-inform NRC oversight, inspection, and enforcement activities.

Both the NRC and the licensees use their PRAs to evaluate the impact on risk of plant modifications and online or outage maintenance, as well as to support determinations regarding the risk significance of plant transients and the safety implications of reportable events.

What about industry? PRAs are often used as a basis for selecting equipment to be monitored under the "Maintenance Rule" (10 CFR 50.65) and for selecting equipment that meets reliability and availability goals. PRAs are used to support license amendments, to update plant technical specifications, and to keep the safety parameter displays in the control room current. One of the most important applications of a PRA is with respect to training reactor operators. The use of PRAs for training varies by plant, but at many plants, operators are trained on the plant-specific simulator using the actual plant-specific accident sequences derived from the PRA.

Excellent summaries of specific PRA-based risk management examples are available in the literature.[22] Below are four examples in which I participated. The plant names have been omitted, as these are dated examples and do not represent current conditions.

Earthquake-induced building collapse

The example involves a plant situation where the PRA revealed that earthquakes were a major contributor to plant risk. The critical event was a seismic-initiated interaction of adjoining buildings that could lead to the collapse of the main control building. Coupled with the possible failure of the ceramic insulators on the off-site power transformers due to the same earthquake, the result would be loss of control and loss of AC power, and, therefore, a small LOCA and turbine trip with complete loss of cooling and loss of containment safeguards and eventual core damage. This major contributor to risk was virtually eliminated by a simple structural modification to damp the interaction between the two buildings resulting from a strong-motion earthquake. The implications of this failure mode were never manifested until the PRA seismic analysis was performed.

Separate and independent safety trains

The transition from the first-generation to the second-generation nuclear plants involved a major design change for safety systems. That change had to do with providing separate and independent safety trains to satisfy requirements such as the single failure criteria. The result was that each train of safety equipment is dependent on the operation of a single emergency power supply and a single cooling-water source, without access to alternative support equipment during some failure scenarios. While the separate and independent safety trains did provide improved protection from rare events such as pipe ruptures, large fires, severe flooding, and electrical bus faults, it became clear that—depending on the details of the design criteria adopted—the separate and independent safety trains could actually increase the vulnerability of these plants to the more frequent types of transients by eliminating the possibility of cross-connecting equipment trains of the same or adjacent units to bypass failed components. Such design practices affect a large family of very important mitigating safety systems, including service water, component cooling water, chilled water, ventilation, electric power, and automatic actuation signals.

For older plants, extensive crosstie capability was provided among support systems. These support system crossties give the plant the freedom to use all of the available equipment to provide mitigation functions in the event of an accident. The specific support systems important to risk include component cooling water, ventilation, electric power, and actuation signals. The safety equipment in the older plants was located in space requiring less dependence on support systems such as safeguards chilled water for cooling the more separated and isolated equipment rooms. One of the primary advantages of PRAs is their ability to expose the details of the role of nuclear plant support systems and how they are linked to the mainline systems to facilitate the optimization of crossties between the safety trains.

Asymmetric power dependencies

Another example of a PRA's ability to expose undesirable system dependencies has to do with asymmetric power dependencies involving the operating logic among three diesel generators and three fuel oil transfer pumps at a nuclear plant. The net effect of the asymmetric power loading was to make one diesel generator dependent on the status of the other two and to make the entire system very sensitive to the status of one particular diesel generator. The root cause of the problem was an anomaly in the start-up and operating logic between the diesels and their fuel supply. This was identified as the major contributor to the failure of electric power and an important contributor to core damage frequency. A modification was proposed to eliminate the dependency. The impact of this proposed design change was a major reduction in the calculated core damage frequency.

PRA as a design tool

At one two-unit plant, the decision was made to use PRA as a fundamental design tool. Table II illustrates the results of the process. On the left are the most important systems and operator actions that contribute to the risk of this particular plant. The numbers in the columns are the percent reduction in core damage frequency if the frequency of the contributing event or action is reduced to zero. The result of each iteration of the risk assessment was a basis for taking corrective actions to reduce the contribution of individual systems or operator actions. The end result of the process is a much better balanced system of safeguards and a lower core damage frequency than most likely would have been the case had PRA not been a part of the design process. The reason for the increase in the contribu-

TABLE II. CONTRIBUTORS TO CORE DAMAGE FOR FOUR PHASES OF RISK MANAGEMENT

System(s) or Operator Action	Percent Reduction in Core Damage Frequency if the Individual System (or Operator Action) Failure Frequency Could Be Reduced to Zero			
	First Iteration	Second Iteration	Third Iteration	Fourth Iteration
1. Electric Power	11	65	43	52
2. Auxiliary Feedwater	9	11	11	31
3. Two Trains of Electric Power Recovered				21
4. Low Pressure Injection / Decay Heat Removal	4	3	8	19
5. Failure to Reclose PORV / PSVs		5	20	17
6. ESFAS / ECCAS			14	15
7. High Pressure Injection Systems	3	9	15	14
8. Operator Recovery of Electric Power During Station Blackout		50	14	14
9. Sump Recirculation Water Source				11
10. Component Cooling Water			3	8
11. Throttle HPI Flow (Operator Action)			1	4
12. Failure of Main Steam Safety Valve to Reclose			1	4
13. Service Water	32	<1	10	4
14. Safeguards Chilled Water	20	8	13	1
15. BWST Suction Valve				1
16. Containment Isolation			1	
Relative Core Melt Frequency	1.00	0.30	0.10	0.06

tion of some systems with each iteration is that as dominant contributors are removed through design actions, the importance of the other contributors increases as the core damage frequency decreases, unless they, too, were affected by design changes. It is analogous to removing big rocks from a pool of water. As the big ones are removed or partially removed, the pool level drops (the core damage frequency level drops) and other rocks (contributors) become more important unless they too were removed or partially removed.

These examples and many more that could be discussed illustrate that PRA is like a microscope for determining what can go wrong in a complex system. PRAs provide new perspectives on safety and expand the understanding of risk beyond licensing and design basis considerations. The ability to quantify the rank order of contributors to risk while making clear the dependency of risk on plant-specific features is a major achievement for meaningful risk management.

PRA is not perfect, because it depends on many imperfect factors such as theories, hypotheses, assumptions, scope, the handling of information, and people. But it is the best method available to us at the present time, and until such time that a better one comes along, we are well advised to use it to make the best possible decisions in managing the risk of complex and hazardous systems and operations. On the other hand, if we do use PRA as input to our risk management decisions we need to pay very close attention to such factors as theories, hypotheses, assumptions, scope, and the capability of the modelers.

References

1. Keller, W., M. Modarres, "A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen," *Reliability Engineering and System Safety,* 89, pp. 271–285, 2005; Hayns, M. R., "The Evolution of Probabilistic Risk Assessment in the Nuclear Industry," *Trans IChemE,* Vol. 77, Part B, May 1999; Loewen, E. P., "To Understand Fukushima We Must Remember Our Past: The History of Probabilistic Risk Assessment of Severe Accidents," address to the 22nd Annual Congress of the Sociedad Nuclear Mexicana Conference, Aug. 8, 2011; Cooke, R. M., "A Brief History of Quantitative Risk Assessment," *Resources,* Summer 2009; and Garrick, B. J., "Nuclear Power: Risk Analysis," *Reference Module in Earth Systems and Environmental Sciences,* Science Direct, Elsevier, 2013.
2. U.S. Atomic Energy Commission, B. J. Garrick memo to the director, Division of Civilian Application, on considering the use of probabilistic methods in nuclear reactor safety analysis, 1957.
3. Garrick, B. J., "Unified Systems Safety Analysis for Nuclear Power Plants," Ph.D. thesis, University of California at Los Angeles, 1968.
4. Siddall, E., "Statistical Analysis of Reactor Safety Standards," *Nucleonics,* 17(2), pp. 64–69, Feb. 1959.
5. Willis, C. A., *Statistical Safety Evaluation of Power Reactors,* Atomics International, AI-65-Memo-212, 1965; and Hart, R. S., and W. T. Harper, editors, *Final SNAPSHOT Safeguards Report,* North American Aviation Inc., NAA-SR-10022 (Rev.), (Confidential RD), Mar. 20, 1965.
6. Mulvihill, R. J., et al., *A Probabilistic Methodology for the Safety Analysis of Nuclear Power Reactors,* Planning Research Corporation, SAN-570-2, vols. 1 and 2, Feb. 1966.
7. Farmer, F., "Reactor Safety and Siting: A Proposed Risk Criterion," *Nuclear Safety,* pp. 539–548, 1967.
8. Holmes & Narver Inc., *Reliability Analysis of Nuclear Power Plant Protective Systems,* prepared for the U.S. Atomic Energy Commission, Washington, D.C., HN-190, 1967.
9. Starr, C., "Social Benefit versus Technological Risk," *Science,* Vol. 19, pp. 1232–1238, 1969.
10. Garrick, B. J., "Principles of Unified Systems Safety Analysis," *Nuclear Engineering and Design,* 13, pp. 245–321, 1970.
11. Lewis, H., et al., *Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission,* NUREG/CR-0400, 1978.
12. Union of Concerned Scientists, "Petition for Decommissioning of Indian Point Unit 1 and Suspension of Operation of Units 2 and 3," Petition 2.206, 1979.
13. PLG (Pickard, Lowe and Garrick Inc.), Westinghouse Electric Corporation, and Fauske & Associates LLC, *Zion Probabilistic Safety Study,* prepared for Commonwealth Edison Company, Chicago, Ill., 1981.
14. PLG (Pickard, Lowe and Garrick Inc.), Westinghouse Electric Corporation, and Fauske & Associates LLC, *Indian Point Probabilistic Safety Study,* prepared for Consolidated Edison Company of New York and the New York Power Authority, New York, N.Y., 1982.
15. Garrick, B. J., "Lessons Learned from 21 Nuclear Plant Probabilistic Risk Assessments," *Nuclear Safety,* 1988.
16. Garrick, B. J., D. C. Bley, S. Kaplan, and T. E. Potter, "Transcripts of Indian Point Testimony Before the U.S. Nuclear Regulatory Commission's Atomic Safety and Licensing Board," 1982–1983.
17. Kaplan, S., B. J. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis,* 1981, 1(1), pp. 11–27.
18. Kemeny, J. G., et al., *Report of the President's Commission on the Accident at Three Mile Island,* 1979.
19. U.S. Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants,* NUREG-1150, 1990.
20. U.S. Nuclear Regulatory Commission, *Update on Staff Plans to Apply Full-Scope Site Level 3 PRA Project Results to the NRC's Regulatory Framework,* SECY-12-0123, 2012.
21. U.S. Nuclear Regulatory Commission, *Status of the Accident Sequence Precursor Program and the Development of Standardized Plant Analysis Risk Models,* SECY-07-0176, Oct. 3, 2007.
22. Garrick, B. J., and J. C. Lin, "Future Developments in Probabilistic Safety Assessment," presented at CSNI Workshop on Applications and Limitations of Probabilistic Safety Assessment, Santa Fe, N.M., Sept. 4–6, 1990.