Use of PRA and Safety Goals in Nuclear Power Plant Regulation

M.L. Ernst

*Division of Risk Analysis, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission,
Washington, D.C. 20555, U.S.A.*

ABSTRACT

Probabilistic risk assessments (PRAs) have been performed on more than a dozen nuclear power plants in the past few years by the NRC and the industry, and much effort has been spent in advancing the state-of-the-art. The NRC has used risk perspectives gained from PRAs, both in an absolute as well as a relative sense, as an aid in making decisions on matters of plant-specific as well as generic safety importance. However, substantial uncertainties pervade accident risk assessments, which makes the application of such analyses difficult at best in the regulation of nuclear power. Basically these uncertainties are large because the PRAs deal with events of very low likelihood (core melt accidents). However, the uncertainties are magnified by the gaps in knowledge about phenomena such as core melt progression, threats to containment integrity, in-plant fission product transport, and the recurrence frequency of large magnitude natural phenomena.

In spite of the uncertainties surrounding PRA, the Commission approved on January 10, 1983, a policy statement on safety goals for nuclear power plants for public comment and a two year evaluation period. These safety goals include quantitative design objectives, which could serve in the future as risk benchmarks for use by the NRC and the industry as part of the decision process on matters relating to nuclear safety. Clearly, if quantitative design objectives are to serve such a future role, PRA must be the tool used to provide the comparative estimates of risk. The Commission's policy statement explicitly excludes the safety goals from use both in licensing cases and in regulation for the two year evaluation period. However, PRAs will be used by the NRC during this time, both generically as well as on a plant-specific basis, to gain a risk perspective on safety issues.

The PRA methodology has been used to prioritize all potential generic safety issues so as to focus scarce NRC and industry resources on those issues of most importance, and to dismiss those issues of trivial risk significance. Also, PRAs will be used to augment NRC's decision making process in assessing the need for proposed new requirements, and the NRC will consider the results of plant-specific PRAs subsequent to the issuance of a construction permit and as part of applications for a standard plant design. Additionally, the NRC may decide to implement a program (NREP) designed to assess the likelihood of core melt and the risk of selected operating plants.

1. Introduction

Much has happened in the field of probabilistic risk assessment (PRA) since the WASH-1400 report [1] was published in 1975 on the Surry and Peach Bottom nuclear power plants. Milestones of particular interest are: the subsequent review in 1978 by the Risk Assessment Review Group (the Lewis Committee) [2] and others; the Commission's policy statement in 1979 on the use of PRA [3]; the Kemeny Commission and Rogovin inquiries into the TMI-2 accident [4] [5], which strongly supported the use of PRA and safety goals in the regulation of nuclear power; PRAs performed under the Interim Reliability Evaluation Program (IREP) and the Reactor Safety Study Methodology Applications Program (RSSMAP), sponsored by NRC's Office of Nuclear Regulatory Research; the PRAs of Big Rock Point, Limerick, Zion, and Indian Point, sponsored by utilities; other utility-sponsored PRAs now underway such as Oconee, Shoreham, and Seabrook; extensive research into the methodology, phenomenology, and data base associated with PRAs; and last, but not least, the current efforts to develop safety goals to assist consistent decision making in the area of potential reactor accidents and to enhance public understanding of the criteria that the NRC applies to the estimated risks of such accidents.

The basic strength of PRA is that it represents a comprehensive and disciplined attempt to model plant performance, including interactions between systems and humans. Through such modeling and the subsequent quantification of success/failure paths, a number of potential weaknesses in plant design and operating, test, and maintenance procedures might be identified, even though a plant may meet the NRC's deterministic requirements. Thus, PRA can be effectively used by the industry and the NRC to supplement conventional engineering evaluation techniques to enhance safety as well as to improve plant availability.

In spite of the potential advantages offered by PRA, however, the uncertainties inherent in the assessments have sharply, but appropriately, limited their usefulness in regulation. These uncertainties are pervasive, since they are a function both of the assumptions made by the individual analysts and the quality of the data base; and the PRAs are so complex that it is difficult not only to identify the uncertainties, but also to quantify and propagate them so as to measure their importance relative to estimates of absolute risk. The end result is that, after a PRA is completed, the pervasive uncertainties result in doubt as to the actual importance of the identified design and operational weaknesses and questions as to whether other weaknesses of perhaps even more risk importance have been overlooked. Therefore, it is difficult to judge whether the bottom line results of any PRA represent an underestimate or an overestimate of risk.

2. Insights Gained From PRAs

In the past few years there have been many PRAs performed, but there has been little direct application of PRA by the NRC to the regulatory process--or by the industry to improve either safety or the reliability of power generation. Since a substantial narrowing of uncertainties in the future will be difficult, the problem that needs to be addressed is how to make reasonable decisions in the face of uncertainty.

There have been some lessons learned as a result of PRAs, and some actions taken to improve safety. Examples of generic design and operational insights include the risks from the intersystem LOCA (Event V), the vulnerability of the recirculation mode in an ice

condenser containment to closed drain valves connecting the upper compartment to the sump, BWR containment overpressure sequences, the importance of reliable auxiliary feedwater systems (AFWS), and the issue of Anticipated Transients Without Scram (ATWS).

In addition to the above generic issues, a number of plant-specific issues have been evaluated. The Zion, Big Rock Point, Limerick, and Indian Point PRAs have been used by the utilities to argue against the need for numerous regulatory requirements. However, these utilities have also used the results of the PRAs to enhance training and to propose design and operational changes aimed at reducing risk.

The NRC believes one methodological lesson learned is that reasonably standardized procedures are needed to increase the scrutability and reproducibility of PRA results. While one might argue that this is not a proper way to reduce the error band, the staff believes it is, if reasonable consensus is obtained on the standardized assumptions. The basic purpose would be to provide reasonably prescriptive assumptions, models, and ways to handle the data base so that individual PRA analysts would be more likely to analyze system and human performance in the same way. This means that the differences between the results of PRAs would more likely reflect the risk and core melt importance of plant-specific design and procedural differences, rather than reflecting individual analyst differences in modeling, assumptions, and data handling.

In October 1982 a draft procedures guide [6] was issued for the performance of PRAs for the National Reliability Evaluation Program (NREP), a program that was still under development by NRR and which had not been submitted to the Commission for approval. This guide generally is more prescriptive than the IEEE/ANS procedures guide [7] that has been under development for the past year and a half; but it is somewhat less prescriptive in some areas than the IREP manual [8] used by NRC contractors.

3. Safety Goals

A PRA can result in a quantitative assessment of risk that potentially can be determined to be reasonably valid, and it will have associated with it a number of dominant accident sequences. However, unless some judgement is made as to the absolute level of risk desired, decisions as to whether to modify the plant or procedures to reduce the risk represented by the dominant sequences will be more difficult to justify. Also, if one assumes "fixes" for the dominant sequences, then these will be suppressed and other sequences will necessarily dominate--should one then "fix" those? Reasonable regulation should be structured to assure some general level of protection of public health and safety. It should not strive continually to lower risk without regard to the absolute risk actually posed by the industry being regulated. Thus, the concept of a safety goal of some sort becomes important, if one ultimately considers using PRA extensively in regulation.

On February 17, 1982, the Commission published for public comment a proposed policy statement on safety goals for nuclear power plants, and the staff published a document [9] describing the proposed goals and design objectives. After receipt of public comments, including holding public meetings in Atlanta, Boston, Chicago, and Los Angeles, the Commission revised the proposed goals and approved them on January 10, 1983 for evaluation.

In addition to two qualitative safety goals, the Commission's policy statement includes several quantitative design objectives as aiming points for risk reduction,

recognizing that there would be instances where a given nuclear power plant may not achieve all of the design objectives. These goals and design objectives will not be used in plant-specific licensing reviews during the evaluation period; nor will they be used as an aid to decision making on issues involving the regulation of nuclear power, such as decisions regarding proposed new requirements, any proposed elimination of existing requirements, and the prioritization of safety activities undertaken by the NRC. However, the Commission has instructed the staff to evaluate such decisions, once they are made, by comparing them against the safety goal.

One of the first steps taken during the two year evaluation period will be to collect available information on PRA studies and prepare a reference document that describes: the current state of knowledge of PRA, including methodological insights and the extent and nature of uncertainties; the estimated risk from nuclear power plants; the dominant accident and risk sequences; and insights gained regarding plant design and operations. This reference document should be completed by early 1984 and will be subjected to peer review.

At the end of the evaluation period the staff will provide to the Commission an assessment of experience gained and lessons learned, will recommend any needed changes to the safety goals or design objectives, and will recommend procedures for any future implementation of the safety goals and design objectives in regulation and licensing.

4. Use of PRA In Regulation and Licensing

4.1 General

In the past, the NRC's regulatory and licensing decisions have been based on the defense-in-depth concept which emphasizes good management; quality assurance; conservative design, construction, and operations; prevention of core damage accidents by requiring appropriate emergency shutdown and cooling systems; mitigation of any accidents that might lead to core damage through the use of systems that reduce the amount of fission products released to the environment; siting in areas that are not in close proximity to highly populated areas; and good emergency planning. Analyses to demonstrate compliance with NRC's requirements have generally been based on conservative engineering judgement, with little emphasis on probabilistic assessments as to the likelihood of meeting the engineering intent of the requirements. However, even the NRC's deterministic approach to licensing has been sprinkled with judgements regarding the likelihood of occurrence of certain events. These are apparent, for example, in the establishment of requirements for redundancy and diversity.

PRAs can be used to augment NRC's present, largely deterministic regulatory requirements and perspective. In most situations PRAs should be performed using realistic assumptions to develop median-valued estimates of risk, and they should include an understandable presentation of the magnitude and nature of uncertainties. The NRC's present regulatory practices are intended to provide sufficient protection to public health and safety, and PRA would be used only to find existing strengths and weak points in the regulatory fabric. Therefore, striving for high confidence or the use of conservative assumptions in the risk analyses in the search for possible strengths and weaknesses would not normally be warranted. However, in some situations the uncertainties surrounding the analyses could be so

large that special consideration would be warranted, even if median-valued calculations using realistic assumptions did not suggest any undue risk. In such situations, additional conservatism could be warranted in any regulatory decision on the issue.

4.2 Prioritization of Resources

PRA has been used by the Office of Nuclear Reactor Regulation (NRR) to prioritize potential generic safety issues by assessing their relative estimated contributions to core melt frequency and public risk. Also, the Office of Nuclear Regulatory Research (RES) is using probabilistic techniques to prioritize research programs, and the Office of Inspection and Enforcement (OIE) will test the effectiveness of these techniques in prioritizing their inspection activities.

These efforts at prioritization will not depend solely on the results of probabilistic risk evaluations. Because of the uncertainties in such analyses, one can not and should not downplay the need for the substantial consideration of other factors that would be important to prioritization decisions, such as good engineering judgement, existing regulatory requirements, preservation of the defense-in-depth concept, reduction of occupational exposures, and the influence of the public's perception of risk.

Prioritization of generic safety issues, including those TMI Action Plan items that remain to be resolved, is important, since it will provide clearer guidance for the appropriate allocation of staff and industry resources. There are insufficient resources to work (at the same time) on all of the potential safety issues that have been identified. Also, there may be some identified potential safety issues whose risk appears to be so small as to raise the question whether any resources should be expended at all to resolve the issues.

4.3 Assessment of Regulatory Requirements

The NRC staff routinely proposes new rules, standards, and guides for use in reactor regulation, such as new requirements that might originate from the resolution of generic safety issues. The assessment of the merits of these, as well as any proposals to eliminate certain requirements, previously has been based predominantly on engineering analysis and judgement. However, in early 1982 substantially increased emphasis was placed on value-impact analyses to aid decision making. The use of PRA not only is important to a credible value-impact analysis, it also attempts to quantify engineering analyses so as to assist the decision maker in considering alternatives, which will serve to strengthen the logical basis of NRC's regulatory requirements. The value-impact principle will be particularly valuable in generic decisions concerning the necessity for and timing of retrofits for older plants to reduce public risk.

The use of risk and reliability assessments in the regulatory process could serve as a basis for developing criteria governing the design reliability of some systems and components important to safety. If such reliability criteria were developed, they could then become appropriate generic requirements for consideration in licensing reviews, perhaps incorporating the simplified fault tree analysis approach used for auxiliary feedwater systems after TMI. Alternatively, deterministic design requirements could be developed which, if implemented, would achieve the desired levels of reliability.

Another area where safety might be enhanced through changes in regulatory requirements using probabilistic techniques is in systems interactions analyses. It is generally

believed that existing PRAs do not do a good job of identifying risk important spatial, functional, and human dependencies (common mode failures). The staff is developing methodologies that might identify such dependencies more efficiently, but these methodologies will need to be tested. If risk important dependencies are identified, then appropriate criteria will be considered as potential new regulatory requirements.

Clearly, however, the most important regulatory usage of PRA in the immediate future will be in the resolution of the degraded core issue -- i.e., are present plants (assuming implementation of present SRP and TMI requirements and resolution of USIs) safe enough, or should fundamental design changes be considered. To help answer this question all existing PRAs will be evaluated to update accident likelihood estimates based on the best consensus regarding methodological approaches, and consequences will be recalculated using revised source terms. After this is done, a range of possible design and operational changes will be studied to assess their impact on the identified accident and risk sequences to determine their costs and safety benefits.

4.4 Plant-Specific PRAs

PRAs have been utilized in the past and will be used in the future as one consideration to justify the need for plant design or procedure changes as well as to evaluate requests for exemptions from certain extant regulatory requirements. In some cases these studies had generic implications, but in others they have been plant-specific. In most cases, however, benchmarks (many times similar to the Commission's safety goals) have been either explicitly or implicitly used to provide additional perspective for the decision maker.

The NRC does not now routinely require that a PRA be performed as a part of reactor licensing proceedings, although a few licensees and applicants have, on occasion, been required to perform PRAs, and others are performing such studies of their own. However, NRC's regulations [10] now require that a plant-specific PRA be conducted within two years of issuance of a Construction Permit (CP) or Manufacturing License. The purpose of this PRA is to seek design improvements in the reliability of core and containment heat removal systems that are significant and practical and that do not have a significant impact on the fundamental plant design. Other initiatives are also being considered to introduce the requirement for a PRA even earlier in the licensing process. For example, a staff paper to the Commission [11] proposes that a PRA be conducted that is as complete as practical for each future standard plant design application.

One major program under development by NRR for possible implementation in 1983 is the National Reliability Evaluation Program (NREP). This program would require a PRA to be performed by selected utilities, and the dominant accident and risk sequences would be evaluated by the NRC to determine whether cost-effective remedial measures might be warranted to reduce public risk or the likelihood of core melt. As envisioned by the staff, this program would involve full integration with Phase III of the SEP program, although the merits of initiating the NREP program alone would be considered, if Phase III of the SEP were deemed not to be cost effective.

4.5 Analysis of Containment Performance and External Events

The Zion and Indian Point PRAs performed by the industry include assessments of the risk from external initiators (seismic events, in-plant fires, winds, floods). These

studies indicated that risks from these accident initiators, while arguably small in an absolute sense, tended to dominate the risks from internal initiators (events triggered by plant failures or operator error). At the present time, the staff does not believe the NRC should require plant-specific assessments of the risk from accidents initiated by external events in the initial phase of any NREP program. The rationale is the staff believes that the uncertainties involved in such assessments presently are too large, but this position will be reconsidered as better consensus is developed regarding appropriate assessment methodologies.

In a similar vein, the NRC presently does not believe that the initial phase of any NREP program should require licensees to perform detailed analyses of containment performance. While consensus has largely been achieved on the methodology for analyzing large, dry containments, reasonable consensus is likely a year or more away for other types (ice condenser and Marks I, II, and III).

The calculation of containment performance is not just the analysis of containment strength. The capability to mitigate the consequences of a core melt accident must be thought of in terms of the release characteristics of the radioactive fission products -- in particular the composition of the isotopes and the mode and timing of release. Involved in the assessments are the knowledge of phenomena (core melt progression, steam explosions, hydrogen explosions, and in-plant fission product transport), temperature and pressure loadings, the isolation capability of the containment, behavior of penetrations and seals, containment cooling, and the probability of direct releases from the primary system to the environment.

5. Conclusion

PRAs will be used more and more as one tool in the regulation of nuclear power plants. However, because of the inherent uncertainties in the analyses, it is doubtful that they will play a decisive role in decisions, at least in the foreseeable future. The results of a PRA will have to be very cautiously used by the decision maker -- the key will be the ability to make reasonable decisions in the face of uncertainty.

It is doubtful that PRAs will be required routinely in the foreseeable future as part of a license application, although the Commission could perhaps eventually require such analyses as part of standardized plant applications or new CP applications referencing such standardized designs. However, in any event it is not clear that the regulator will or should play the most important role in the use of PRA. Licensees and applicants should be able to make good use of a PRA that is at least equal in scope to that of the IREP studies. The results of such assessments could be used to: better understand the design and interactions of the plant; help develop improved test, maintenance, and operating procedures; enhance operator training; develop an improved analytical base for identifying strengths and weaknesses of design; and, if initiated early enough, serve as a useful vehicle for marrying reliability engineering with design.

It appears that PRA has the potential of being a powerful tool, and the part that the regulators play should not hamper reasonable use by the industry in the design and operation of safer nuclear plants that deliver power to the public less expensively and with greater reliability. This should be the principal goal of the users of PRA in the future.

References

- [1] Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014) (October 1975).
- [2] Risk Assessment Review Group Report To The U.S. Nuclear Regulatory Commission, NUREG/CR-0400 (September 1978).
- [3] NRC Statement on Risk Assessment and the Reactor Safety Study Report (WASH-1400) In Light of The Risk Assessment Review Group Report (January 18, 1979).
- [4] Report of The President's Commission On The Accident At Three Mile Island (October 1979).
- [5] Three Mile Island - A Report To The Commissioners and To The Public (January 1980).
- [6] National Reliability Evaluation Program (NREP) Procedures Guide, NUREG/CR-2815, BNL - NUREG-51559 (September 9, 1982).
- [7] PRA Procedures Guide, NUREG/CR-2300 (January 1983).
- [8] Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, SAND 82-1100 (April 1982).
- [9] Safety Goals for Nuclear Power Plants: A Discussion Paper, NUREG-0880 For Comment (February 1982).
- [10] Code of Federal Regulations, 10 CFR 50.34(f)(1)(i).
- [11] Proposed Commission Policy Statement on Severe Accidents and Related Views On Nuclear Reactor Regulation, SECY-82-18 (November 24, 1982).