The Use of PRA, Deterministic Analysis, and Systems Experience in Decision Making

E.L. Zebroski
Electric Power Research Institute, P.O. Box 10412, Palo Alto, California 94303, U.S.A.

Abstract

Decisions on important aspects of the design, construction, operation, record-keeping, licensing, and regulation of nuclear power plants have many common elements. The decision processes commonly used often make less than the optimum use of available information and methods. The processes increasingly being used to resolve safety questions involve a combination of methods including systematic analysis of experience, sequence risk analyses, and PRAs. The practical use of such processes in other areas of decision-making is explored, including extension to construction. Possible long-term impacts of the application of such disciplines safety levels attainable is estimated.

1.0 Decision-making practices are important in many aspects of nuclear power plant design, construction, and operation. Risk-based decision-making is essential both to protect public safety and to attain rational and effective use of resources. Government safety authorities set general criteria and guidelines in the interests of public safety. However, several different technical, industrial, and governmental cultures and disciplines are evident in the interpretation and application of specific decision-making. The purpose of this paper is to set out the commonalities in the nature of the decisions involved, and to explore the practical means and benefits of broader use of the available systematic disciplines for such decisions.

1.1 Essentially all decision-making in respect to equipment and procedures in nuclear plants is overlaid by sets of safety criteria. These range from broad public safety goals, such as those being evaluated by the USNRC, to specific functional criteria, such as ASME, IEEE, and ANSI code requirements and guidelines. Conformance to criteria is often subject to varied interpretations between regulatory agencies and designers, builders or operators. This gives rise to a large body of supplemental decision-making documentation. This tends to be prescriptive in defining acceptable design

or operating approaches for meeting the applicable criteria. This process has worked adequately in terms of preserving high levels of public safety. However, in many cases this process can have undesirable by-products that can limit rather than enhance the levels of safety achieved, and that can contribute to the excessive delays and costs experienced by some projects. The deficiencies discussed in the next section are most widely evident in the United States, but some aspects of this problem are present in other countries as well.

1.2 The conventional process described in the previous section often has serious deficiencies in some important areas of decision-making, as follows:

- Prescriptive interpretations of general criteria tend to become rigid rules for design and operation, but often without adequate evaluation of their adequacy, completeness, or validity over a range of practical conditions.

- Compliance with rigid rules becomes an end in itself. The efforts involved in documenting and defending evidence of compliance may transcend or displace some of the efforts needed for proper decision-making and timely execution at practical hardware and operational levels.

- Available and desirable improvements are often inhibited or precluded by the likelihood of excessive procedural obstacles or adversarial challenges.

- Schedules of installation of mandated changes are often on critical paths, with large delays that may be disproportionate to the safety or reliability values involved. Such delays produce large, unpredictable diseconomics in construction or operation.

2.0 Optimum decision processes are now definable for most situations. These involve three main types of activities:

- o Monitoring of risk exposures
- o Assessment, evaluation, and decision
- o Implementation and tracking of risk management decisions

These activities ideally should have the common goals of providing for the best attainable levels of safety and reliability **within given levels of resources.** The assumption of indefinitely large resources is an aberration in both theoretical and practical terms.

It is reasonable that increasing the quality-related costs of nuclear steam supply system equipment, testing and documentation might have measurable benefits in terms of safety and reliability. Perhaps even to the extent of

doubling the costs of the Nuclear Steam Supply system equipment, relative to costs experienced in the 1970's. However this would account for only about 15% of the more than 100% average increase in costs experienced by projects in the U.S. completed after 1979. There are several extreme cases of 300% increases, relative to pre-1979 costs. Most of these cost increases are due to period costs (the capitalized cost of interest associated with delays in completion and operation.) These, in turn are to a large extent related to limitations in decision-making processes on presumed or known construction deficiencies, and also on backfits to cure presumed deficiencies in design.

2.1 Monitoring and Data Sources. Historically the functions of monitoring have been limited to anecdotal experience and reliability statistics on limited samples of the applicable populations of components and systems. With the development of large, high-cost engineering systems for which high levels of system reliability are essential, increasingly systematic, analytic, and comprehensive records of performance and deviations have been developed. These are increasingly available and convenient for use in decision-making.

When the Reactor Safety Study (WASH-1400) was performed in 1974-75, reliability data was sparse for both systems and components. Total operating experience of only about 150 unit-years was available for a diverse set of designs. Much of the component data was largely developed by borrowing from fossil power and chemical plant experience. Human performance was estimated from aircraft pilot performance. Nevertheless, Wash-1400 did give some bounding estimates of probabilities and consequence relationships, although with uncertainties in both directions in the range of 10 to 100 - or more - at the low probability - high consequence end of the scale.

Important capabilities developed since that time are the following: Levine and Rasmussen[1], Bernero[2], NRC Report [3].

- Comprehensive coverage of experience and analysis of on-going experience

- Systematic information storage and retrieval of systems and components experience with widely available accessibility

- A sizable body of data on plant-specific operating conditions, and statistically meaningful sub-sets of data for closely related system designs and unit designs

- Ability to do meaningful trend and time-series analyses on component or system malfunctions

- Good coverage of over 750 unit-years of experience, (in the U.S.), plus some coverage of 1200 unit years more outside of the U.S.

2.2 Assessment and Evaluations. Paralleling the growth of experience and data has been a large growth in the disciplines and body of results in assessment and evaluation, as follows:

- Nearly two dozen PRA studies

- Systems interaction studies, to find low frequency sequences that may not be found in some PRAs[2]

- Computer-assisted systems for organizing and using large PRA studies

- Sequence risk analysis has developed as a set of systematic processes for the comprehensive analysis of plant operating events, accidents, or observations from inspections and tests, Zebroski, et al [4], INPO Report [5], Fader, et al [6].

- The methods for qualitative and quantitative ranking of the levels of importance of events are well established, Vesely, et al[7].

- The identification and evaluation of remedies for significant events has been made systematic and comprehensive[4].

- The use of plant-specific PRA's to define self-consistent sets of input parameters is increasingly recognized as essential to most deterministic analysis.

2.3 Risk Management - Processes. The growth of the test data and methods for risk monitoring and assessment provide the essential tools for rational risk management. These tools are increasingly being used in the monitoring, assessment, and response to perceived operating deficiencies.

Utilities are now routinely and comprehensively reporting on operating events and abnormal conditions. These reports are increasinqly analytic, and often cover the investigation of the human factors and corrective measures. The licensee event reports (LER's) have improved in depth of coverage and reduced in numbers. (This has resulted in part from the redefinition of LER scope. Single component failures with limited system consequences are now reported in a reliability data base, Nuclear Plant Reliabiilty Data System, NPRDS). The utility reporting and analyses are backed up by the "Significant Events Program" at the Institute for Nuclear Power Operations (INPO) in Atlanta, which also evaluates the relative importance of events, and the priority for implementation of remedies[5]. INPO also estimates conditional probabilities

for events or conditions that meet defined criteria of relative importance[6]. In addition, the Nuclear Safety Analysis Center, at EPRI in Palo Alto, also analyzes events or issues that have generic application.

The NRC has integrated its events analysis capabilities in the group "Analysis and Evaluation of Operating Data" (AEOD), which provides and documents analyses of selected events or issues. This is in addition to the usual policing, review and investigative functions in three other divisions of the NRC. One of these provides immediate reporting, by on-site observers, of unusual events or conditions. These reports are called "Preliminary Notifications".

Utilities and NRC now often approach the resolution of specific issues using probabilistic analysis of plant-specific sequences to estimate the importance of a given safety-related question, relative to the overall probabilities of serious consequences or of core damage. This is sometimes called Sequence Risk Analysis (SRA). It can provide the conditional probability of serious consequence, given that an initiating event has occurred or a degraded condition exists[6]. This approach also provides a framework for several important risk-management decisions--namely:

- Is the estimated risk large enough relative to the total risk to warrant timely correction, remedy, and/or added surveillance?

- What improvement factors (reductions in conditional probability) are available from alternate remedies

- Can the implementation of costly or disruptive remedies be delayed, either by interim operational improvement measures, or because the risk contribution is small relative to the overall values?

3.0 More general application of risk-analysis-based decision making appears especially fruitful in the area of managing the responses to construction deficiencies, the evaluation of the need for backfits, or of the options for accomplishing the needed remedies, Zebroski and Starr[8]. The priority and timing determinations can be made mainly using **relative** risk assessments. This approach, generally similar to that used in France, can permit full benefit of useful safety and performance improvements while avoiding most of the costly impacts on construction and operating schedules now experienced.

4.0 The role of uncertainties and potential incompleteness of risk assessments has been a serious deterrant to the use of PRA in decision making for regulation, Jordan and Weiss[9], H. W. Lewis [10]. Many kinds of significant decisions have low sensitivity to such uncertainties through the use of relative measures and bounding values from experience, Vesely and

Rasmussen[11], Okrent and Baldewicz[12].

The growing experience base provides a decreasing upper bound to the likelihood of severe accidents, **provided that risk management decision-making is rational and makes full use of the monitoring and assessment tools now available.**

REFERENCES

[1] S. Levine and N. C. Rasmussen, "Nuclear Plant PRA; How Far Has it Come?" Risk Analysis 4, 4 (Dec. 1984) 247.

[2] R. M. Bernero, "Probabilistic Risk Analysis" NRC Programs and Perspectives", Risk Analysis 4, #4, (Dec. 1984), 287.

[3] "Probabilistic Risk Assessment (PRA) Status Report and Guidance for Regulatory Application" NUREG I050, Sept. 1984.

[4] E. L. Zebroski, C. D. Wilkinson, and S. L. Rosen "INPO Programs for Use of Operating Experience" Proc. Amer. Power Conf. 45 (1983) 723-731.

[5] "Significant Events Evaluation and Information Network Manual", INPO-83-001 Feb. 1983.

[6] G. B. Fader, E. L. Zebroski, and M. A. Jones, "Sequence Risk Analysis; A Method for Evaluation of Event Significance Based on Potential Core Damage Frequency" Anticipated and Abnormal Plant Transients in Light Water Reactors Vol. 2, Plenum Press N.Y. (1984).

[7] W. E. Vesely, T. C. Davis, R. S. Denning, N. Saltos, "Measures of Risk Importance and Their Applications" NUREG/CR 3385, (BMI-2103-RX) July 1983.

[8] E. L. Zebroski and C. Starr, "Use of PRA in the Life Cycle Management of Construction Deficiencies" ANS/ENS Meeting Feb. 1985.

[9] W. S. Jordan and E. R. Weiss, "Comments of the Union of Concerned Scientists on Proposed Revisions of the Backfitting Process for Power Reactors ANPR 48 Fed. Reg. 44127". Docketed USNRC 10/28/83.

[10] H. W. Lewis, "Comments Regarding Limitations of PRA" (Transmitted by ACRS to GAO, 11/23/83).

[11] W. E. Vesely and D. M. Rasmuson "Uncertainties in Nuclear Probabilistic Risk Analysis" Risk Analysis 4, 4 (Dec. 1984), 322.

[12] D. Okrent and W. L. Baldewicz, "On the Development of Threshold Criteria for Action for Light Water Reactors" UCLA-ENG-8124, March 1982.