
BY THE U.S. GENERAL ACCOUNTING OFFICE
Report To The Chairman, Subcommittee On
Energy Conservation And Power
Committee On Energy And Commerce
House Of Representatives

Probabilistic Risk Assessment: An Emerging Aid To Nuclear Power Plant Safety Regulation

Probabilistic risk assessment (PRA) is a method of quantifying the probabilities of potential accidents and their consequences at nuclear power plants. PRA analysts use complex computer models to help them predict which risks appear to be the greatest and to identify corrective actions that address factors contributing to those risks. Nuclear utilities and the Nuclear Regulatory Commission (NRC) have used PRA since 1975 to help improve plant safety and thereby reduce risks to human health and the environment.

GAO believes that NRC is making reasonable use of PRA. However, the uses and effectiveness of PRA are still evolving. Since relatively few empirical data on actual plant accidents are available, PRA analyses are and will continue to be affected by many unknowns and uncertainties about internal plant behavior, as well as external events, such as floods. GAO therefore cautions that NRC should not use PRA risk estimates as the sole or primary basis for regulatory decisions. Rather, NRC should use PRA to supplement its more traditional analytical and engineering methods.



032364

GAO/RCED-85-11
JUNE 19, 1985

Request for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Document Handling and Information
Services Facility
P.O. Box 6015
Gaithersburg, Md. 20877**

Telephone (202) 275-6241

The first five copies of individual reports are free of charge. Additional copies of bound audit reports are \$3.25 each. Additional copies of unbound report (i.e., letter reports) and most other publications are \$1.00 each. There will be a 25% discount on all orders for 100 or more copies mailed to a single address. Sales orders must be prepaid on a cash, check, or money order basis. Check should be made out to the "Superintendent of Documents".



UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

RESOURCES, COMMUNITY,
AND ECONOMIC DEVELOPMENT
DIVISION

B-211642

The Honorable Edward J. Markey
Chairman, Subcommittee on Energy
Conservation and Power
Committee on Energy and Commerce
House of Representatives

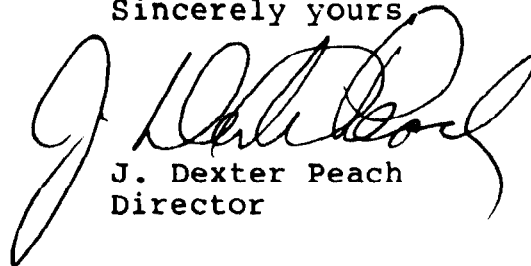
Dear Mr. Chairman:

This report represents the conclusion of a two-phase assignment we undertook in response to an August 20, 1982, request from Representative Richard Ottinger, who was then Chairman of the Subcommittee on Energy Conservation and Power. Upon your assumption of the Subcommittee Chairmanship, we were advised by your office of your continued interest in this assignment.

This report discusses probabilistic risk assessment (PRA) in general, including the state of the art of PRA, Nuclear Regulatory Commission research efforts to improve PRA techniques, and current and potential uses of PRA in regulating nuclear power. The first phase of the assignment was concluded on May 24, 1983, with a report on the Indian Point Nuclear Power Plant risk assessment study.

As arranged with your office, we are sending copies of the report to the Nuclear Regulatory Commission and other interested parties on the date it is issued.

Sincerely yours,

A handwritten signature in black ink, appearing to read "J. Dexter Peach".

J. Dexter Peach
Director

D I G E S T

The Nuclear Regulatory Commission (NRC) regulates nuclear power to ensure that public health, safety, and the environment are protected. NRC increasingly is relying on probabilistic risk assessment (PRA) to supplement its more traditional analytical methods for determining whether nuclear power plants are safe.

PRA, unlike traditional methods, systematically examines complex technical systems to identify and measure the public health, environmental, and economic risks of nuclear plants. Specifically, PRA attempts to quantify the probabilities associated with a potential accident occurring and the resulting consequences. This information is then used to determine which risks appear to be the greatest and to identify corrective actions needed to address the major contributors to those risks.

Although NRC's 1975 Reactor Safety Study was the first application of PRA to nuclear power plant risks, NRC did not significantly use PRA until after the March 1979 accident at the Three Mile Island nuclear power plant. At that time, a presidential commission and a special NRC inquiry group that investigated the accident recommended that NRC use PRA techniques in safety analyses. PRA, they said, was the best available tool for identifying how serious accidents could occur and possible corrective or preventive actions. NRC's present and future use of PRA has been the subject of concern, primarily that NRC and the nuclear industry might place excessive reliance on numerical estimates of overall plant risk--estimates that are subject to large uncertainties--in determining the safety of a nuclear power plant.

The Chairman, Subcommittee on Energy Conservation and Power, House Committee on Energy and Commerce, asked GAO to answer the following questions about PRA:

--What is the state of the art?

--How is NRC using PRA and does this appear reasonable, considering its staff's experience and training?

The Chairman also asked GAO to determine whether NRC is adequately considering the potential problems and disadvantages of PRA. Finally, the Chairman asked GAO to identify whether there were problems in the use of PRA in the safety reassessment of the Indian Point nuclear plants. GAO separately addressed that issue in a prior report.¹

PRA: STATE OF THE ART

A substantial amount of nuclear power plant operating experience has accrued and many improvements in PRA methodology have been made since the first application of PRA in 1975, but some of the uncertainties reflected in that pioneering study remain.

In researching the evolution of PRA, GAO found that PRAs, by their nature, are statements of uncertainty that identify and assign probabilities to events that rarely occur. The uncertainties are not caused by and are not unique to PRA but reflect the incomplete knowledge about plant systems, human behavior, accident processes (the physical and chemical changes that take place during an accident), the off-site consequences of accidents, and how external events such as earthquakes, fires, and floods can cause accidents.

The incomplete knowledge base contributes to uncertainty in PRAs in four general ways:

- PRA analysts may not have identified all events that could start or direct the course of an accident.
- Sufficient and reliable data may not be available to model and quantify the behavior of plant systems and accident processes.
- Analysts may not make the best assumptions where data are lacking.

¹Response to Specific Questions on the Indian Point Probabilistic Safety Study
(GAO/RCED-83-158, May 24, 1983).

--Computer models may not realistically represent plant behavior and accident processes. (See p. 15.)

In 1983, NRC began a 3-year, \$25-million research program to reduce some of those uncertainties. The program concentrates on those areas having large uncertainties and where improvements are possible in light of scientific knowledge and available resources. An important part of NRC's effort is to develop a computer model tying accident processes inside the structure containing the nuclear fuel to off-site accident consequences. (See p. 32.) NRC also plans to:

- collect experimental and actuarial data in such areas as how and why components fail (see p. 35);
- improve models for evaluating how human actions affect plant risk (see p. 37);
- improve understanding of accident processes, such as the generation and possible combustion of hydrogen (see p. 39); and
- develop models and data on external events that can cause accidents (see p. 45).

Although these research efforts may improve NRC's base knowledge of PRA, they will not resolve many of the uncertainties associated with the reliability of PRA end-result risk estimates. Some of these uncertainties are: (1) potentially significant accident sequences that could be overlooked in a plant systems analysis, (2) continued uncertainties in relatively unexplored areas such as human behavior and external causes of accidents, and (3) uncertainties resulting from the absence of actual experience or data from a severe accident. In addition, on the basis of GAO's interviews with NRC and other experts in PRA, some uncertainties may be unresolvable because they are inherent to the science of risk assessment. (See p. 47.)

NRC USES PRA TO AID DECISIONMAKING

NRC is using PRA in a variety of ways to analyze nuclear power plants, plant systems,

and related regulations and safety issues. On the basis of interviews and documents GAO reviewed, PRA has provided valuable safety insights and an orderly and disciplined means of safety analysis, and has led to safety and operational improvements at nuclear plants that otherwise would not have been made.

For example, PRA studies performed to date vary from comprehensive studies of entire plants to limited analyses of individual plant systems. Among other things, the studies perform the following functions:

- They estimate the risk of severe accidents and their potential consequences for the purpose of disclosing those risks and consequences to the public in environmental statements on new operating plants. (See p. 49.)
- They assess the overall risk of operating plants, identify potential safety improvements, and analyze the reliability of individual plant systems. Actual and potential unsafe plant conditions have been discovered as a result of PRA analyses. For example, one utility discovered that the failure of either of two electrical system relays would disable an emergency electrical power system at one plant. The utility reported the deficiency to NRC and quickly corrected it. (See p. 51.)

NRC is also using PRA to develop quantitatively-based analyses of the estimated costs and benefits of alternative regulatory actions. NRC believes that these quantitative cost/benefit analyses provide more objective information than qualitative analyses on the relative public health risks of alternative actions.

In preparing cost/benefit analyses using PRA techniques, however, NRC develops numerical risk reduction estimates for potential actions that are based on PRA results. NRC then assigns dollar values to human life and health effects. This practice is controversial; the appropriate dollar values for decisionmaking have not been determined, and NRC has not consistently applied the same dollar values to human life and health effects. In addition, the principal benefit of quantified cost/

of alternative actions--can be realized without assigning dollar values to risk calculations.

Other planned programs and activities are likely to expand NRC's use of PRA. They include proposed nuclear power plant safety goals, analysis of potentially severe accidents and nuclear power plant safety issues, and a proposed reliability assurance research program intended to maintain the level of safety at plants over their operating lifetimes. PRA's precise role in these programs and activities, however, is not yet clear. (See p. 66.)

A disadvantage of using PRAs is that they are costly and time-consuming to prepare and review. Comprehensive, plant-specific PRAs can cost utilities several million dollars and require 2 years to complete. In addition, NRC reviews of four major utility PRAs have cost from \$200,000 to \$600,000 each and required from 9 to over 18 months to complete. NRC believes that, until recently, its ability to review utilities' PRAs and to prepare and use its own PRAs has been hindered by limited staff expertise and the lack of standard PRA procedures.

These problems are now decreasing due, in part, to increased training and experience of both NRC and the contractors it uses to assist it in reviewing PRAs. In addition, NRC and the nuclear industry have begun to standardize PRA procedures, which, over time, should increase the ability of PRA users to compare different PRA studies and decrease the time needed to review subsequent studies. (See p. 74.)

In summary, and in answer to the Committee's specific question, GAO believes that in view of the evolving nature of PRA, the time and expense required to prepare and review major PRA studies, and the staff's experience and training, NRC is making timely and reasonable use of PRA in the nuclear regulatory process. GAO cautions, however, that NRC should not use end-result numerical risk estimates as the sole or primary basis for regulatory decisions. The substantial limitations and uncertainties of PRA results provide strong

arguments against such use for the foreseeable future. Rather, NRC should use PRA to supplement its more traditional analytical and engineering methods.

AGENCY COMMENTS

NRC stated that the report is "an excellent document" that provides a clear perspective on the nature of PRA and its use in dealing with complex nuclear power plant safety issues. Further, NRC agreed with the report's overall conclusions on the general use of PRA and that it should not be used as the sole or primary basis for regulatory decisions.

NRC also provided a number of detailed suggestions for actual modifications or clarification. GAO changed the final report, as it considered appropriate, to reflect these NRC comments. The complete text of NRC's comments appears as appendix IV, beginning on page 87.

C o n t e n t s

		<u>Page</u>
DIGEST		i
CHAPTER		
1	INTRODUCTION	1
	PRA use is increasing	1
	Objectives, scope, and methodology	2
	What is PRA?	3
2	PRA METHODOLOGY HAS PROGRESSED SINCE THE REACTOR SAFETY STUDY, BUT MANY LIMITATIONS STILL EXIST IN THE STATE OF THE ART	13
	PRA methodology is evolving	14
	PRA methods continue to exhibit areas of large uncertainty	15
	Some segments of PRA have large uncertainties	17
	Conclusions	30
3	NRC'S RESEARCH PROGRAM ADDRESSES LIMITATIONS IN PRA METHODOLOGY BUT CANNOT ELIMINATE THEM	32
	NRC is improving PRA techniques	32
	Uncertainties will remain large in four areas	33
	Some PRA segments will continue to have large uncertainties	34
	Conclusions	47
4	PRA SUPPLEMENTS THE REGULATORY DECISIONMAKING PROCESS IN MANY AREAS	48
	NRC uses PRA to analyze severe accident risk at new plants	49
	NRC and plant owners use PRA to examine individual operating plants	51
	PRA is used as an aid in ranking generic issues	57
	NRC has used PRA to examine generic issues	58
	NRC is using PRA as a basis for cost/benefit analyses	60
	Conclusions	63
5	NRC'S USE OF PRA IS LIKELY TO INCREASE	66
	Safety goals may encourage bottom-line PRA use	66
	Proposed integrated assessment of safety issues could require plant-specific PRAs	69
	PRA may be used qualitatively for reliability assurance	70
	PRA could supplement NRC's severe accident decisionmaking	71
	Conclusions	72

6	NRC IS ADDRESSING PROBLEMS THAT HAVE HINDERED EFFICIENT REVIEW AND USE OF PRA	74
	PRA reviews tax NRC's resources	74
	PRA expertise available to NRC has improved	74
	Standardization of some performance and review procedures may improve NRC's use of PRA	76
	Conclusions	79

APPENDIX

I	Organizations contacted by GAO in our PRA review	80
II	NRC- and utility-sponsored PRAs	82
III	Congressional request letter dated August 20, 1982	85
IV	Letter dated April 24, 1985, from William J. Dircks, Executive Director for Operations, NRC, commenting on this report	87

ILLUSTRATIONS

	Probabilistic risk assessment flow chart	6
	A simple event-tree for a single initiating event	9

ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
DOE	Department of Energy
GAO	General Accounting Office
NRC	Nuclear Regulatory Commission
PRA	Probabilistic risk assessment
SSMRP	Seismic Safety Margins Research Program

CHAPTER 1

INTRODUCTION

On August 20, 1982, the Chairman, Subcommittee on Energy Conservation and Power, House Committee on Energy and Commerce, asked that we review the reliance placed on probabilistic risk assessment (PRA) techniques by the Nuclear Regulatory Commission (NRC). PRA is a method of systematically examining complex technical systems such as nuclear power plants to identify and measure their public health, environmental, and economic risks. The Chairman was particularly interested in the safety assessments performed at the Indian Point nuclear power plants located near New York City. Specifically, he asked us to answer the following questions:

--What is the current state of the art of PRA?

--To what extent has NRC incorporated PRA into the regulatory process and does this appear reasonable, considering the staff's experience and training?

--What are the problems and potential disadvantages associated with the use of PRA and has NRC considered these?

--Are there any specific problems associated with the use of PRA in the assessment of the Indian Point plants?

We agreed to divide our review into two phases, with phase one concentrating on PRA techniques as they apply to the Indian Point safety study. We concluded phase one with our report entitled Response to Specific Questions on the Indian Point Probabilistic Safety Study (GAO/RCED-83-158, May 24, 1983). Phase two, addressed in this report, represents our assessment of the state of the art of PRA, in general, and NRC's use of risk assessment, including problems and potential disadvantages.

PRA USE IS INCREASING

PRA methodology as applied to nuclear power plants is a relatively new and evolving area. The first major application of PRA techniques specific to nuclear power was NRC's Reactor Safety Study (An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400), published in 1975. This study, which has been highly criticized for its methodology limitations and for portraying its results as being more realistic than they were, was a pioneering effort to apply formal risk assessment methodology to the issues of reactor safety. However, it is important to note that the Reactor Safety Study occurred at a time when experience with nuclear power plants was inadequate to quantify reactor safety. The study also has greatly contributed to assessing nuclear power plant risk by providing a logical framework for discussing reactor safety and by displaying the relative probabilities of various accident sequences. However, the controversy surrounding the Reactor Safety Study continued, and NRC did not

make wide use of PRA until after the Three Mile Island nuclear power plant accident in March 1979.

Two investigations of the Three Mile Island accident supported the increased use of PRA. In 1979, the report of the President's Commission on the Accident at Three Mile Island endorsed the increased use of PRA techniques in safety analyses. In 1980, NRC's Special Inquiry Group (NUREG/CR-1250) made an even stronger recommendation to increase the regulatory uses of PRA, including placing increasing reliance on quantitative risk assessment techniques. The investigative groups supported PRA as the best available guide to identifying important accidents and possible corrective or preventative actions.

In addition to the two plant-specific PRAs done as part of the Reactor Safety Study, at least 18 additional PRAs were completed between 1975 and 1983. (See app. II, p. 82.)

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of our review were to evaluate the state of the art of probabilistic risk assessment, including problems, potential disadvantages, and NRC's efforts to address them through research and other activities; examine NRC's use of PRA as an aid in licensing and regulating nuclear power plants in the United States; and evaluate whether such uses were appropriate, given NRC's level of expertise and the developing nature of PRA.

We conducted our work primarily at NRC headquarters in Washington, D.C. We interviewed NRC officials who plan, review, and set agency policy on PRA and related activities. We contacted members of NRC's Advisory Committee on Reactor Safeguards (ACRS), a statutory body of advisors to NRC, and attended ACRS meetings relevant to PRA. We also interviewed Department of Energy (DOE) officials for their comments on uses of PRA.

To become familiar with PRA and its current and potential uses, we reviewed rulemakings, legislation, and NRC and DOE guidance on nuclear power plant safety; numerous scientific articles, papers, and presentations; and our previous studies. We examined past and present NRC programs and special studies that involved the use of PRA techniques, as well as plans for programs that will use PRA in the future. We contacted many persons in a variety of organizations who made significant comments on PRA, including a former NRC commissioner and representatives from national laboratories, public interest groups, utilities with operating nuclear power plants, and utility service groups. We attended an NRC training course on systems reliability and analysis techniques as well as conferences concerning nuclear power plant issues. We also visited two operating nuclear power plants in order to familiarize ourselves with the plant systems and components discussed in PRAs.

To determine whether NRC is addressing PRA limitations, we reviewed the research programs NRC initiated to improve the state of the art of PRA. We also discussed the adequacy of NRC's research programs with the ACRS, DOE, and the Sandia National Laboratory, an NRC contractor working on PRA.

We also reviewed NRC's PRA training activities. We interviewed agency officials about NRC's current PRA capabilities and future needs. We also examined training program plans and course schedules.

Appendix I is a detailed list of organizations we contacted, the conferences we attended, and the power plants we visited.

Our review was performed during the period from July 1982 to December 1983 in accordance with generally accepted government auditing standards.

Our assessment of the state of the art of PRA and its major limitations is discussed in chapter 2. NRC's efforts to address the major limitations, the adequacy of these efforts, and their effect on the state of the art are discussed in chapter 3. NRC's use of PRA in regulatory decisionmaking and potential future uses in nuclear regulation are covered in chapters 4 and 5, respectively. We also commented in those chapters on the appropriateness of NRC's use of PRA, considering its state of the art. We did not, however, address the problem of limited NRC staff expertise and training in chapters 4 and 5. A discussion of these issues is included in chapter 6, which describes NRC's efforts to address other problems hindering the use of PRA.

WHAT IS PRA?

Probabilistic risk assessment is a method of systematically examining complex technical systems, such as nuclear power plants, to identify and measure their associated public health, environmental, and economic risks. In the nuclear power plant safety field, PRAs focus on core-damage and core-melt accidents, since they are expected to have the greatest potential risk to the public health and safety. To assess risk, it is necessary to measure both the likelihood that an accident will occur (probability) and the level of damage or loss that will result (consequences).

PRA methods provide for mathematically quantifying risk on the basis of calculated probabilities of component and human failures, whether they occur singly or in combination. PRA addresses three basic questions:

- What could go wrong?
- How likely is it that this will happen?
- If it happens, what are the consequences?

The PRA practitioner attempts to quantify probabilities and consequences as accurately as possible in order to determine realistic mathematical expressions of risk. When risks have been quantified in a consistent manner, they can be compared to determine which risks appear to be the greatest and what the major contributions to risk are. This information can be used by decisionmakers to determine whether changes to the plant are necessary to improve safety.

How PRA differs from traditional analytical methods

To understand PRA, it is important to also understand how it differs from the "deterministic" methods traditionally used in the regulatory process for limiting nuclear power plant risk.

A deterministic analysis can be described as one that produces a yes or no answer. For example, a highway engineer would use a deterministic analysis to determine whether a concrete beam supporting a bridge is safe for a rated 10-ton capacity. The analysis would use accepted civil engineering techniques to convert the rated load to allowable mechanical stresses in the supporting beam. Conservative safety factors would then be considered to account for uncertainties, such as variations in concrete properties or inaccuracy in placement of steel reinforcing bars. The product of the deterministic analysis would be a yes or no answer indicating whether or not the bridge is acceptable for a 10-ton load.

The deterministic analysis does not answer a related question--how heavy a load would cause the concrete beam supporting the bridge to fail. In contrast, PRA provides the answer to such a question. A PRA would establish the range of concrete quality that is found in bridge construction and the probability of obtaining a given level of quality. It would also consider the probability that substantial numbers of steel reinforcing bars would be omitted from the concrete. The result of a PRA would not be a yes or no answer to the question of the bridge's acceptability for its rated 10-ton load, but a description of the bridge's likely capabilities. For example, the PRA might show that:

- There is a 95-percent probability that the bridge will fail under a load of 18 tons.
- There is a 50-percent probability that the bridge will fail under a load of 15 tons.
- There is a 10-percent probability that the bridge will fail under a load of 10 tons because of the inadvertent omission of some of the necessary reinforcing bars.

Historically, deterministic analytical methods have been used to establish multiple levels of protection in nuclear plant design

to protect public health and safety. Due to the potentially severe consequences of major accidents at nuclear plants, deterministic methods have been coupled with an approach known as "defense in depth." In this approach, several classes of events are identified: (1) those that are expected to occur routinely, (2) those that are much less likely but that might occur once or twice in the life of a plant, and (3) those that are never expected to occur but that are theoretically possible. The conditions that would result from these events are calculated, and deterministic methods are then applied to each set of conditions to establish the design features of the plant.

Safety analysts have always recognized that there are theoretical events more extreme than a plant was designed to withstand. However, since such extreme accidents generally require two or more low probability events to occur in sequence, they have been considered to be so unlikely that there is no need to protect against them. One principal shortcoming of the traditional deterministic process is that it does not include a means for conducting an integrated and systematic systems analysis of nuclear power plants to uncover such rare events. PRA helps to fill this gap through 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, potential weaknesses in plant design, operation, test, and maintenance procedures might be identified, even though a plant may meet NRC's deterministic licensing requirements. An advantage of PRA is that it identifies all major contributors to risk, including those involving multiple failures. This is especially important since some of the accidents involving multiple failures that would exceed plant design are now perceived to be more likely than previously assumed, especially those with common sources, such as adverse environmental conditions like earthquakes.

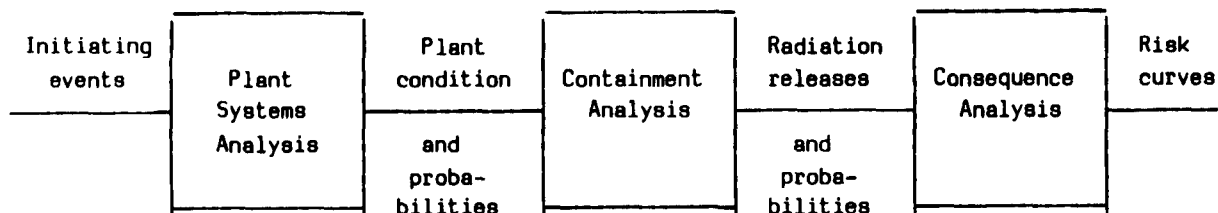
PRA scope

PRAs can be performed at many levels of scope, depending on the objectives and available resources. The three general levels of scope are:

- level one--plant systems analysis;
- level two--plant systems and containment analysis; and
- level three--plant systems, containment, and consequences analysis.

The following flow chart shows the relationship of the three segments of the analysis.

Probabilistic Risk Assessment Flow Chart



- o Systems
 - o Components
 - o Operations
 - o Tests
 - o Maintenance
 - o Human error
 - o External events
- o Core
 - o Reactor vessel
 - o Containment
 - o Containment systems
- o Meteorology
 - o Population
 - o Evacuation
 - o Health effects

A level-one PRA is an analysis of nuclear power plant design and operation at the plant system and component levels. It examines normal plant operations, test and maintenance data, and the effect of human errors and external events to identify how, when, and why accidents could occur in a plant and what the probability of such occurrences are.

A level-two PRA examines the physical processes of an accident and their effects on the reactor vessel, which is the immediate reactor container, and on the steel and concrete containment building that surrounds the reactor vessel, steam generator, and much of the reactor cooling system. A level-two analysis predicts how and when containment can fail and what radiation could be released if such failures occur. This type of analysis is done in addition to plant systems analysis but does not provide a full assessment of risk because the consequences of nuclear radiation outside the plant are not addressed.

A level-three PRA builds on the plant systems and containment analyses and analyzes the movement of radiation throughout the environment after it has been released (i.e., after containment failure) and estimates the public health and economic effects of

the release. Only a level-three study permits an overall assessment of risk, since it considers both the probability that an accident will occur and the consequences of such occurrences.

Each of the three levels of scope may include an analysis of the effects of external events, such as fires, floods, earthquakes, and storms. Analyses of external events require consideration of factors that otherwise may not have been included in the PRA, such as numerous concurrent failures and the magnitude of an event versus its frequency of occurrence. For example, an earthquake could damage many plant components simultaneously as well as disrupt plans for evacuating nearby populations.

Analyses that include external events tend to be less certain than those that do not because of greater complexity, less experience in this area of analysis, and a lack of historical data. Such analyses result in greater reliance on subjective input, such as engineering judgment and expert opinion.

General PRA methodology

Although PRA methodology as applied to nuclear power plants is a relatively new and evolving area, certain general methods of analysis are widely used and accepted. The following summary is based on the PRA Procedures Guide (NUREG/CR-2300, 1983), a joint NRC/industry effort to catalog these methods.

Collection of information

To provide reliable and precise risk assessments, the PRA process requires vast amounts of information. Depending on the scope, this information can include

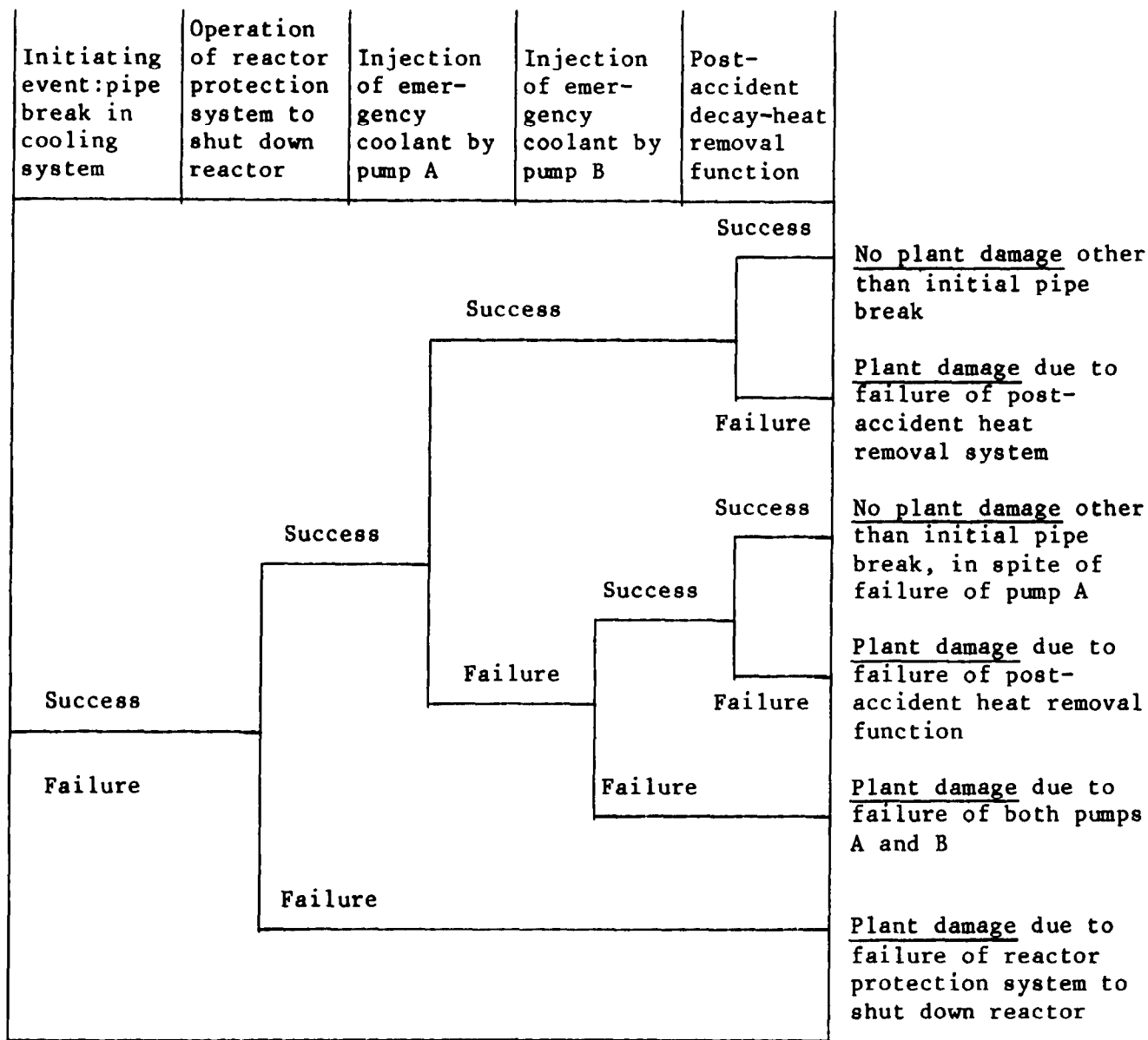
- plant design and operating information, such as drawings of piping and electrical systems and written operating procedures;
- generic and plant-specific data concerning frequency of initiating events and component reliability (e.g., NRC-compiled data summaries on pumps, valves, and other plant components); and
- site-specific meteorological, topographical, and population density information.

Plant systems analysis

A level-one PRA begins with a systematic search for contributors to risk. Two methods of analysis accomplish this and provide a graphic display of the contributors and their interrelationships. The first is event-tree analysis, which identifies the sequence of events that may result in an accident. The second is fault-tree analysis, which determines how failures in safety systems may occur.

Event-tree analysis begins with an attempt to identify all conceivable events that could precipitate an accident, such as a pipe break or loss of power to a necessary plant system. These events are referred to in PRA terminology as "initiating events." Next, all significant sequences of events that could follow each initiating event are developed. Each sequence varies, depending on the assumed success or failure of mitigating safety systems. Redundant safety features, such as multiple pumps and physical barriers, are built into nuclear power plants so that the failure of a single component, barrier, or mitigating system alone will not cause an accident. If these backup systems in a particular sequence succeed, then the sequence will be terminated before it culminates in an accident. (See p. 9 for an example of a simple event-tree adapted from the PRA Procedures Guide.)

A Simple Event-Tree for a Single Initiating Event



In the above example, it is assumed that:

--Either emergency coolant pump A or B is sufficient for successful emergency cooling.

--Failure of the reactor protection system to shut down the reactor will automatically result in plant damage. In this case, it is unnecessary to consider the other three events.

--Failure of both pumps A and B will necessarily result in plant damage.

The construction of fault-tree diagrams is a method of system modeling that displays the various ways that a safety system designed to lessen the effect of an accident can fail. Each safety system failure that was identified in the event-tree analysis as contributing to an accident is investigated to determine how faults (i.e., failure or malfunction of a component) within that system could contribute to failure of the entire safety system. This analysis considers component failure, human error, maintenance and testing activity, potential system interaction, and common-cause contributors.

To quantify the likelihood that an accident sequence (a sequence culminating in core damage or core-melt) will occur, frequencies of occurrence are assigned to (1) events that could lead to an accident and (2) component failures or human errors identified in fault-tree analyses. Frequencies are based mainly on component reliability information gathered from plant operating records, generic information, and expert opinion. Initiating events and success/failure models are combined and computers are used to quantify frequencies of occurrence of entire accident sequences.

Containment analysis

A level-two PRA includes, in addition to a plant systems analysis, an analysis of the physical processes that may occur following core damage or meltdown and the possible release of radiation from the containment building. The containment analysis considers several stages of events within the containment building that may lead to containment failure. These include

- conditions before core-melt, such as pressure within the containment building;
- events within the reactor vessel during and after core damage;
- events after the reactor vessel fails; and
- events related to the disposition and cooling of debris within the containment building that concern the behavior and effect of the radioactive materials after release within the containment building, but before release to the outside environment.

Containment event-trees are extensions of the plant system event-trees that were developed in level one of the PRA. However, while the plant systems analysis addressed questions of safety systems' success or failure, the containment event-trees ask yes or no questions concerning activity within the containment building, such as "Is water present in the reactor cavity at the time of vessel failure?" These final branches leading to

containment failure represent accidents that could release radiation to the public.

After accident sequences have been identified, analysts determine what amount and type of radiation could be released as a result of each accident and what the mode of the release would be. For example, release could occur as a steam explosion or a slow leak into the atmosphere, or the core could melt into the ground beneath the containment building.

Since the analysts may identify hundreds of accident sequences, it may not be practical to perform release analyses for every sequence individually. For this reason, the sequences may be grouped into release categories that share similar characteristics. This simplifies the analysis by assuming that the radiation release for all sequences within each category will be the same, and it allows accidents to be organized by severity of release. Establishing release categories is a subjective process. Two examples of categories that were used in a recent PRA are:

- filtered vented release, in which the release is partially decontaminated as it passes through a filtered vent system, and
- steam explosion with sprays, in which a steam explosion has occurred within the containment building and the water spray system, a safety feature designed to reduce the radiation that would be released, functions properly.

Release categories are the starting point for the next level of the PRA, the consequence analysis.

Consequence analysis

A level-three PRA includes, in addition to plant systems and containment analyses, a consequence analysis to study the movement and depositing of radiation released from the plant and the effects it could have on humans and the environment. Many variables must be considered:

- Weather conditions, wind direction, and topography of the surrounding terrain affect the dispersion of released radiation.
- The location and density of nearby populations determine the number of people that could be exposed to radiation.
- The quantity and mode of exposure to radiation determine the severity of adverse health effects that are likely to result in a given population. Dosages can be measured and used to estimate specific health effects, such as fatalities, cancer, and genetic effects.

--Mitigating circumstances, such as evacuation of the nearby population or the availability of shelter, will affect the severity of human exposure.

Presentation of results

The results of a level-three PRA integrate the findings of the plant systems analysis, the containment analysis, and the consequence analysis. Results can be presented in tables listing major scenarios and identifying their release categories, contribution to core-melt, likelihood of causing damage to public health, and other information of interest. Some information can also be displayed in graphic form. These overall results are commonly referred to as "bottom-line" risk estimates. For example, one overall result, or bottom-line risk estimate, of the 1982 Indian Point PRA was the estimate that the likelihood of an accident that would cause any adverse public health consequences is one in 1,000 years of reactor operation with about 90-percent confidence.

In addition, uncertainties and their effects on the risk results must be considered and in some way presented with the results. The most widely used quantitative measure of uncertainty has been the idea of "confidence bounds," or "confidence levels." The confidence levels express the analysts' degree of confidence that the risk estimates are realistic on the basis of the quantity and reliability of data and models used in the PRA. Often three confidence levels are displayed, representing upper and lower bounds and a "best" estimate falling between the two.

Uncertainties of plus or minus a factor of 10 times the "best" estimate are generally considered as large uncertainties. The previous example of one in 1,000 years of reactor operation would be considered to have a large uncertainty about the result if the uncertainty factor was plus or minus a factor of 10 times. That would mean that the actual result could be anywhere in a range of one in 100 years (minus 10 times the result) or one in 10,000 years (plus 10 times the result).

CHAPTER 2

PRA METHODOLOGY HAS PROGRESSED SINCE THE REACTOR SAFETY STUDY, BUT MANY LIMITATIONS STILL EXIST IN THE STATE OF THE ART

Although PRA is increasingly being used to estimate risk, PRA methodology for the nuclear power plant industry is still evolving. Many methodology improvements have been made in the last 10 years, including improved modeling of plant systems and components and events that start accidents. Techniques for identifying accident processes and analyzing human factors also are more refined. Some of the improvements that occurred in the development and application of PRA since the 1975 Reactor Safety Study are briefly described beginning on page 14.

However, the state of the art continues to exhibit many uncertainties because it is difficult, if not impossible, to ensure that

- the analysis is complete,
- sufficient and reliable data exist to model and quantify accident processes and plant behavior,
- study analysts have made the best assumptions, and
- PRA computer models represent reality.

These uncertainties result from a lack of data or understanding of plant system response, human behavior, and accident processes. They are discussed in detail beginning on page 15.

Uncertainties are present in almost all aspects of PRA, but they are particularly pronounced in the areas of

- plant systems analysis,
- human reliability,
- accident phenomenology inside the containment building,
- off-site consequences, and
- external accident initiators.

Although improvements have been made in these areas in the 10 years following the Reactor Safety Study, some of the uncertainties may be inherent in the science of risk assessment. Others can be reduced with additional research and empirically derived data. The effects of the major uncertainties on these areas are discussed beginning on page 17.

PRA METHODOLOGY IS EVOLVING

The first full-scale application of PRA to a nuclear power plant was the Reactor Safety Study. Although the methods used in this study were an advance over earlier methods applied to reactor risk, a group of experts assigned by NRC's Commissioners to review the study believed it was severely limited in several ways:

- The analysis was not complete, since fires, earthquakes, and human actions were not recognized as important accident initiators due to incomplete knowledge and unsophisticated quantification techniques.
- The uncertainty in the absolute probabilities of potential accidents was greatly understated due to an inadequate data base, the inability to quantify multiple failures due to a common cause, and the use of incorrect statistical methods.
- Many conservative and nonconservative assumptions were made in the analysis that could affect the accuracy of the bottom-line numbers by either understating or overstating the risk estimate.
- The consequence analysis used to project the spread of radioactive materials through the environment and the resulting health effects was inadequate.

A substantial amount of nuclear reactor experience has accrued in the 10 years since the completion of the Reactor Safety Study. NRC has been exploring ways of systematically applying probabilistic analysis to nuclear power plants, and the nuclear community has rapidly expanded its use of PRA techniques. Each of the PRAs subsequently performed at 18 plants has led to more thorough risk assessments and better understanding of plant design weaknesses, the importance of accident phenomena assumptions, and the significance of certain factors that contribute to plant risk.

In the course of performing and reviewing subsequent PRAs, analysts have made many methodology improvements. Systems models now examine a broader and more complete range of dependencies (i.e., ways in which systems and components interrelate to operate successfully) and events that start accidents. Techniques for identifying severe accident processes are also more refined. The accuracy of plant models, as well as the PRAs' quantitative results, have also improved to a limited extent due to more empirical data and a better understanding of plant systems and accident phenomenology.

The method used today to analyze how humans contribute to a plant's risk is a more refined and formalized version of that used in the Reactor Safety Study. Human reliability analysis now evaluates how operator recovery actions can impede the progress of accidents.

After the Three Mile Island accident, a number of research projects were undertaken to improve the ability to model accident phenomena inside the containment building. This included improvements in analyzing how severe accidents progress, containment response, and the characteristics and behavior of radioactive materials released to the environment.

PRAs performed since the Reactor Safety Study have also provided a number of significant insights into off-site consequences. One addresses emergency response actions. Until recently, analysts generally believed that emergency planning required an ordered evacuation out to 10 miles from the plant. Studies now support a response of combined evacuation and sheltering within the 10-mile zone.

Finally, advances have been made in the ability to consider external causes of accidents such as earthquakes and fires. The major improvements have been new engineering insights regarding the effect of external initiators on plant systems.

PRA METHODS CONTINUE TO EXHIBIT AREAS OF LARGE UNCERTAINTY

PRAs, by their very nature, are statements of uncertainty. They identify and assign probabilities to events that rarely occur. Uncertainties, which are not unique to PRA, reflect a lack of data or knowledge about system response, human behavior, and accident phenomenology. Therefore, those uncertainties exist regardless of whether an individual uses PRA, deterministic methods, or the best engineering judgment.

A strength of PRA, however, is that it allows uncertainties to be displayed in order to assess how the lack of experience and/or knowledge affects the insights obtained. Considering uncertainties may necessitate that the PRA analyst make conservative assumptions to compensate for the lack of knowledge or data, or to simplify very detailed models. For example, conservative success criteria for various functions are sometimes chosen, e.g., the criterion that it takes two pumps, rather than one, to perform a specific safety operation.

Some uncertainties in PRA, such as the inability to identify all accident initiators, may result in underestimating risk. Others, however, such as the failure to consider successful operator actions in arresting the progression of an accident, may result in overestimating risk. Therefore, when considering PRA results, it is difficult to judge whether the statements of risk represent an underestimate or overestimate of the risk.

The four areas of large uncertainty (i.e., plus or minus 10 times the estimated probability) are discussed in the following sections.

Completeness of the analysis

To perform a complete PRA analysis, the analyst must ensure that all events and combinations of events that could initiate or direct the course of an accident have been identified. This is a difficult, if not impossible, task, as there is always the possibility that a scenario has been overlooked. Unintentional omissions include unknown events that have never happened before or can result from the complicated nature of plant operation. Hundreds of thousands of scenarios may be considered in one study, and the chance that a significant combination of events may have been overlooked cannot be eliminated.

One type of unintentional omission is not identifying all events that can initiate accidents. Initiating events are identified by reviewing past operating experience, developing logic diagrams, and performing an initiating event/mitigating system analysis. The latter analysis examines events that start accidents and systems designed to suppress or lessen their severity. Although this method will identify many initiating events on the basis of historical data, it is less likely to accurately predict events that have never happened before. Further, the numerous ways and contexts in which these events may occur is difficult to define.

In addition, some events may be purposely omitted because they introduce substantial additional uncertainty into the PRA results. For example, sabotage may be omitted because there is no basis on which to predict the incidence of sabotage and measure the risk, or because analysts assume that its worst consequence could not exceed the worst consequences of other accidents.

Sufficiency and reliability of data

Data uncertainties arise because actual data needed to quantify the systems analysis are usually scarce. Appropriate data may be scarce because of lack of experience, as is the case with unusual events and failures, or because of lack of understanding, as is the case concerning phenomena within the containment building during and after core-melt. In such situations, little recorded historical experience exists to allow meaningful data to be obtained.

The lack of experience with unusual events and failures generally requires the analyst to make subjective judgments in deciding what data to use and what statistical methods to apply. Accordingly, subjective data carry more uncertainty with them than data based on event and failure experience. Nevertheless, subjective judgment of experts may contribute valuable information to allow better decisions to be made.

In situations in which there is a lack of understanding, analysts must rely more on generic data and small-scale experiments. Such data sources are less certain than plant-specific

data derived from operating experience. For example, in recent history some potentially disastrous events, such as severe earthquakes in regions where nuclear power plants are now located, have been rare. As a result, few historical data are available on the frequency of such occurrences and their effects on nuclear plants.

Assumptions made by study analysts

In areas that are not well understood or where few data exist, assumptions may be necessary before analysts can proceed with the study. The possibility that analysts will make invalid assumptions contributes to uncertainties. Assumptions may simplify a study or limit its scope, or they may be necessary in areas that are not well understood. Subsequently, such assumptions may be questioned by other PRA experts or disputed by new evidence. Existing PRAs have included assumptions concerning what may occur within the reactor containment building, the applicability of the internal flooding analysis of one plant to a similar plant, and plant design and construction. One of the most basic assumptions used in PRAs, for example, is that the plant was built to design specifications using concrete and steel reinforcing rods of the required strength.

Relationship of computer models to reality

How accurately PRA computer models characterize accident scenarios, plant response, and human behavior is another area of uncertainty because PRA relies on abstract models to describe plant systems, phenomena within the containment building, and accident consequences. In addition, PRAs generally deal with rare core-melt events. For this reason, analysts intentionally insert a conservative bias into PRAs where core-melt phenomenology is poorly understood. Currently, the problem of determining how representative PRA models are is compounded by an inability to validate the models or quantify the extent of these conservatisms.

SOME SEGMENTS OF PRA HAVE LARGE UNCERTAINTIES

The uncertainties in PRAs have a greater effect on some segments of PRA analysis because of a combination of factors. However, since PRA segments build on the results of each other, a flaw in one segment is incorporated and often compounded in subsequent phases. Therefore, any and all segments can contribute to imprecise results and greater uncertainty about the end results. The segments of PRA that have large uncertainties are

- plant systems analysis,
- human reliability,
- accident phenomenology inside the containment building,
- off-site consequences, and

--external accident initiators.

At the same time, significant improvements have been made in the state of the art since the Reactor Safety Study in those portions of PRA most affected by the large uncertainties. Portions of a PRA analysis most subject to uncertainties, as well as state-of-the-art advancements, are discussed in the following sections to provide a perspective on the state of the art of PRA.

Plant systems analysis

The event-tree and fault-tree techniques currently used for plant systems analysis are essentially the same as those used in the Reactor Safety Study. However, better understanding of plant system failures and accident processes has led to modifications in the original analysis. Nevertheless, few new data needed to better quantify the systems analysis have been collected, although current and planned data collection programs should improve the situation.

Refinements in systems analysis lie in the ability to model a broader range of functional as well as equipment-related dependencies. These include dependencies between events that start accidents and safety systems, between support and safety systems, and between safety systems. A more complete set of accident initiators can now be identified through improved modeling techniques, such as the construction of a detailed master diagram of how the accident progresses. External causes of accidents are now being considered as special types of initiating events.

A better understanding of accident processes has also resulted in modifications to the structure of the event-trees and the projected outcome of certain accidents. For example, the new perception that the reactor core can be cooled after some melting occurs has lessened the calculated consequences of certain accidents.

Another refinement in plant systems analysis was the development of more realistic criteria for successful system performance under accident conditions. This, in turn, led to improvements in modeling the various stages of accident progression by adding new event-tree headings and changing some of the accident consequences.

Finally, computational techniques have been streamlined to reduce the time required to construct system models. These techniques consist of using either abbreviated drawings of models or preconstructed accident sequence modules, as appropriate, for constructing fault-trees.

Despite the improvements, large uncertainties remain with respect to completeness and the accuracy with which systems models represent the plant and its behavior. It is possible to reduce

these uncertainties, but not to eliminate them altogether. The PRA community believes that uncertainties related to completeness do not significantly affect the insights gained from PRA. They acknowledge, however, that "bottom-line results"--such as core-melt frequency or off-site risk--could conceivably be affected by any discoveries of new accident processes or events.

The issue of how representative computer modeling is to actual plant behavior may also prove difficult to resolve for two reasons. First, the criteria for determining the success or failure of plant systems may be inaccurate since only two extremes--success or failure--are offered as binary coding alternatives. This affects the ability to model partial failures, which may more accurately represent the reality of a system's performance. Second, because PRA modeling involves calculating rare core-melt events, complete validation in an experimental or empirical sense is not achievable for the bottom-line risk estimates.

The lack of data also contributes to uncertainty with respect to whether PRA models represent reality. Data determine the level of resolution of our understanding of system operation and, therefore, influence the way in which "faults" are identified in the models. In addition, because most data contain some degree of uncertainty, it follows that the uncertainty will be carried over into the PRA results.

For the most part, data needed for systems analysis are still incomplete, uncertain, or unavailable. A large amount of plant-specific data has accumulated from new PRAs that might meet some data needs, but this information has yet to be combined to obtain an industry-wide data base. For the most part, PRAs performed to date still rely heavily on generic data, which may not be representative of the nuclear industry or the power plant being studied. For example, the analyst may assume that a particular valve in a nuclear plant has a similar failure rate to a valve used in oil drilling equipment. Data improvement since the Reactor Safety Study includes the addition of information on events that start accidents.

Substantive data have been collected on transients, i.e., potential events adversely affecting the normal operations of a reactor. Generic and plant-specific transient values for both pressurized-water and boiling-water reactors have been tabulated. Data on loss of coolant accidents, i.e., events resulting from a breach in the coolant boundary, have marginally improved. Many current PRAs have used the Reactor Safety Study numbers, modified by this new information, to analyze loss-of-coolant accidents.

The sources of generic data on component failure rates used in the Reactor Safety Study are still being used. They have benefited from component failures identified in licensee event reports; however, few data on causes of component failures are available, and the understanding of how components fail has not improved.

Data on test and maintenance intervals and duration is another area in which information essential to plant systems analysis is lacking. These data are instrumental in quantifying fault-trees--component tests give the frequency with which an item meets performance and reliability requirements, while maintenance logs track system failures and the system's ability to return to an operating state. These logs record routine preventative maintenance data that are obtainable but have to be collected from either plant technical specifications or actual maintenance logs. Corrective maintenance data, such as component failures reported for repair, are among the most difficult to obtain because they are not routinely collected and are occasionally subjectively estimated on the basis of discussions with plant personnel.

Finally, data on common-cause failures (i.e., multiple failures occurring due to the same cause) have improved only marginally since the Reactor Safety Study. Common-cause failure probabilities are still largely subjectively estimated and are generally not tailored to specific plant environments or maintenance and operation policies. For example, large earthquakes are rare events and there are few data on the effect a large earthquake would have on plant equipment or the plant's containment structure.

Human reliability

The role of plant personnel in the outcome of potential accidents is one of the most important and difficult elements of a PRA to evaluate. The potential for human error is present in every phase of plant operation, testing, and maintenance. In addition, the possibility is present that human recovery actions will prevent the accident, or at least lessen its severity. PRA studies have found that both beneficial and harmful human actions can play a major role in determining what accidents are most important from a risk perspective. The major uncertainty in human reliability analysis is the lack of an adequate empirical data base on human error rates.

The basic method in use today for analyzing human reliability is a more refined and formal version of that used in the Reactor Safety Study. This method is termed the Technique for Human Error Rate Prediction.

In its present form, human reliability analysis is confined to examining probabilities associated with errors of failing to perform a prescribed task or procedure. Examples of these errors include failure to open a specific valve that is required to be open, or to restore equipment to its operational state following test or maintenance. The errors that are considered in the course of a human reliability analysis are those that can occur both prior to or following an event that initiates an accident. Errors resulting from incorrectly performing a specified task are not adequately considered in the human reliability analysis. These

errors are seldom modeled and are difficult to quantify because they require anticipation of a wide range of unintended human actions that might occur under accident conditions.

Decision-based errors, as contrasted with errors of failing to perform prescribed tasks, is another area in which the state of the art is weak. A decision-based error is an error that might be made, for example, in accident diagnosis. Such errors may be critical to the course of accident sequences. In fact, an NRC publication (NUREG/CR-3010) indicates that failure to identify the correct course of action may dominate other errors because decision-based errors determine the path of an accident and, therefore, may cause dependent errors. A dependent error is one that is influenced by the occurrence of some other error. Thus, imprecision or inaccuracy by the PRA analyst, in estimating the probability of operator misdiagnosis of an accident, could have a tremendous impact on the human reliability analysis and its validity.

As human reliability analysis exists today, the analyst must rely essentially on his own judgment in determining the level of dependence among identified human errors. If the analyst's assessment of dependencies is wrong, the overall analysis may underestimate or overestimate the probability of human errors. For this reason, much uncertainty remains in the prediction of human errors.

In its present state of development, PRA conservatively treats some operator recovery actions--how plant operators recognize and rectify system failures--by assuming that the action will not be successful. Thus, the accident frequency does not reflect the probability that the recovery action will subdue the accident. Generally, successful operator recovery actions are considered in a PRA only when sufficient time and information are available to the operator and if the recovery can occur without employing innovative measures.

The human error data base supporting the current human reliability method is a modified version of the data used in the Reactor Safety Study. This data source is based almost entirely on information extrapolated from similar, but not equivalent, industries and on expert judgment. Because these are not actuarial data, they carry many uncertainties with them.

Data are particularly weak in such previously discussed areas as

- errors of incorrectly performing a given task,
- errors in decisionmaking,
- errors of failing to perform a prescribed task,
- human error dependencies, and

--operator recovery actions.

Human reliability analysis could benefit from additional data on error frequencies and performance times collected in the operation of the plants and in operations from training simulators.

Accident phenomenology inside the containment building

Experience in analyzing core-melt accidents is limited. At the time of the Reactor Safety Study, the methods available for analyzing the physical processes of core-melt accidents were primitive by today's standards. Considerable experimentation and computer model development have occurred since then, but the methods of analysis are, for the most part, not validated. PRA analysts have also had very little experience in the use of these models in risk analysis.

At present, there are no generally accepted comprehensive methods for estimating the radiation released during degraded (damaged) core accidents. The Reactor Safety Study categories for radiation releases have been used in various PRAs, but PRA experts have questioned the validity of these values.

Uncertainties are present in both the data and models used in analyzing the behavior of radioactive material. Research is ongoing in this area, but numerous questions about radiation behavior remain unanswered, such as the actual amount of radiation that might be released during an accident.

Physical processes

Many of the physical processes of core-melt accidents are analyzed by core-melt system models that were developed after the Three Mile Island accident.

Computer model development is currently in a rapid state of change. According to NRC's February 1984 PRA status report, developments are occurring so fast that, for a PRA being undertaken today, it is difficult to recommend a set of computer models. Because the models are undergoing rapid development, many versions of them are in use. This causes ambiguity regarding the underlying assumptions of the computer models and creates a validation problem. As a result, validation of these models against experimental data has been extremely limited.

Advances have been made in developing and quantifying containment event-trees used to describe the progression of an accident from the start of core-melt to containment failure. Since the Reactor Safety Study, containment event-trees have evolved that explicitly address the underlying phenomena contributing to containment failure, to the extent that both the combined and mutually exclusive effects can be considered. For example, both

hydrogen burning and a rapid release of steam can, under certain circumstances, contribute to early containment failure due to overpressurization. In other cases, the steam can cause the containment atmosphere to become inert and prevent hydrogen burning. Such advances allow the assessment of probabilities at a level where individual phenomena are addressed and where dependencies are explicitly considered.

However, much judgment is still required in quantifying the probabilities of the containment event-trees. Because of lack of knowledge about accident physical processes, it is sometimes not possible to state with complete confidence the pathways an accident will take. For example, various decisions in the containment event-tree, such as whether containment failure precedes melting and whether hydrogen combustion leads to containment failure, rely on the analyst's judgments.

Many other uncertainties exist in the understanding of the physical processes, particularly in such areas as

- the thermal history of the fuel,
- temperatures in the reactor coolant system and the containment building,
- the relative timing of core-melt and containment failure,
- the mode of containment failure,
- the extent to which the core debris can be cooled,
- the generation and combustion of hydrogen, and
- fuel-coolant interactions.

Release of radioactive material

Methods for analyzing the type and magnitude of radiation released after containment failure are still evolving. At present, there is no generally accepted comprehensive method for estimating the amount and type of radiation released during degraded-core accidents. The release categories used in the Reactor Safety Study were not comprehensive, and PRA experts question the validity of some of the release amounts. Little work has been done on constructing release categories since that study; however, some research on this topic was done as part of the 1983 Ocone PRA.

Supporting data in several areas are lacking. Data are needed to describe how radiation is dispersed by water from the fuel and disseminated within the containment building. Molten core and concrete interactions can produce radioactive aerosols, and many data need to be collected that describe this process.

Additional information also is needed describing how radiation combines with the oxygen produced from fuel disintegration.

Lack of knowledge of the chemical forms of the materials that may be released from the core, or the size of the radioactive particles, is a cause of large uncertainty in PRA. For example, the Reactor Safety Study assumed that iodine would be released in its elemental form. However, recent experiments suggest that a different, less dangerous, form of iodine (cesium iodide) may be released. This discovery could have a dramatic effect on the radiation release categories and off-site consequences.

Another uncertainty is the timing of radiation releases. This depends partly on the timing of the physical processes that occur, especially the rate at which the fuel heats up, and partly on the chemical and physical properties of the radioactive material. For a given release, it is quite possible that different materials will have different release rates owing to their different properties. Little work has been done to date to study these differences.

The Reactor Safety Study methods of estimating the release of radiation overstate the amount that is released, and release predictions represent one of the most uncertain parts of PRA methodology. Currently, however, analytical methods are still under development, their sensitivities are unexplored, the extent of validation of computer models is extremely limited, and only initial efforts have been made to quantify uncertainties in the analysis of radiation behavior. The cost of greatly narrowing some of the uncertainties in these methods also may be prohibitive.

Behavior of radioactive material

Very few improvements have been made in this area since the Reactor Safety Study. Data are imprecise or unavailable, and models used in analyzing the behavior of radioactive material may only approximate the processes they are intended to describe. The omission of important processes, because certain phenomena are not completely understood or because they cannot be modeled, represents another source of uncertainty.

Current unresolved issues in radiation behavior are numerous. For this reason, only a partial list will be mentioned here:

- Aerosols, that amass and form particles of much larger sizes, could significantly affect the amount of radiation released to the environment. Little experimental work has been done with this phenomenon in accidents that degrade or damage the reactor core.
- Limited experimental data are available on aerosol generation caused by interactions between the nuclear fuel and concrete in the containment building.

- As mentioned earlier, little information is available on the chemical forms of radiation. The chemical form can influence radiation's subsequent behavior in the reactor coolant system and in the containment structure as well.
- Little is known about how radiation is diluted when it passes through reactor water pools or ice condensers that are intended to modify or contain radiation.
- Information is needed describing how radiation deposited on containment surfaces or dissolved in water may be changed or later released as an accident progresses.

Off-site consequences

Current uncertainties in off-site consequence predictions stem from modeling limitations. These limitations are the result of an incomplete understanding of the phenomena involved in the movement of radiation released to the environment and of the health, environmental, and economic effects that result. The consequence analysis is also confined by simplifications made in the modeling process to reduce costs, complexity, and requirements for input data.

Since the Reactor Safety Study, improvements have been made in models used to predict how radioactive material moves, scatters, and settles and what the resulting economic and health effects are. These improvements lie primarily in the areas of weather sampling and emergency response.

According to NRC's February 1984 status report on the development of PRA, a comprehensive assessment of the uncertainties in off-site consequences has not been performed. What does currently exist, however, is a large body of sensitivity analyses in which consequences are calculated for a range of plausible values of a model. Factors found to contribute to uncertainties include

- the magnitude of radiation released;
- the form and effectiveness of emergency response, which can make a large difference in predicted early health effects;
- the rate at which dry radioactive material settles;
- the modeling of how wet radioactive material settles; and
- predicted radiation doses.

External accident initiators

The PRA studies that have been conducted since the Reactor Safety Study have treated external causes of accidents in varying

degrees of detail. Some studies have excluded external causes altogether. Other studies have been motivated by these events. Earthquakes, fires, floods, and high winds are the only external causes that have been studied in one or more comprehensive PRAs in the past, and therefore the state of the art encompasses only these areas. Earthquakes are the most understood and researched of these initiators. Analytical methods have not been developed and applied for other external initiators.

Greater uncertainties are associated with the risks from external initiators than are associated with internal initiators. NRC's PRA Procedures Guide states that greater uncertainties stem from less experience in analyzing external causes, lack of data, the use of relatively new analytical techniques, and greater reliance on engineering judgment and expert opinion.

The principal area of uncertainty in external initiators lies in the difficulty of estimating the frequency of occurrence of an event exceeding a given magnitude. Thus, for some external causes, the likelihood of a major initiator (e.g., a very large earthquake or extreme flood) is often neither known from the historical record nor reliably inferred from analysis of that record. Currently, methods for analyzing external causes of accidents have not progressed to the point where confidence can be placed in their quantitative assessments, particularly when comparing them with risk assessments of internal initiators.

Other uncertainties lie in the characterization of the external phenomena (width and length for a tornado) and in how the effects of the phenomena are transmitted (e.g., overpressure, ground movement) from the source of the event. In the evaluation of component sensitivity to external initiators, uncertainties arise from an insufficient understanding of the properties and failure modes of structural material, errors in the calculated equipment responses due to approximations and assumptions in modeling, and the use of generic data and engineering judgment in the absence of plant-specific data.

Seismic risk analysis

The analysis of earthquakes has received increased attention in recent years. Although the Reactor Safety Study concluded that earthquakes are not major contributors to risk, studies performed since then have indicated that a seismic disturbance may contribute significantly to overall plant risk.

Two methods are currently available for estimating seismic risk and both differ in the level of detail. The first method--called the Zion method--was applied in the 1981 PRA of the Zion plant. The second method was developed by an NRC-funded research program. This method is called the Seismic Safety Margins Research Program (SSMRP) method.

Both methods rely on engineering judgment--the Zion method to supplement sparse data and limited analyses, and the SSMRP procedure to estimate frequency of occurrence, derive component sensitivities, and perform the in-plant analysis. Each method can yield different results. However, the risk estimates derived from both procedures have large variances.

The SSMRP method emphasizes extensive component and system modeling and uses a computer model developed under the research project for calculating seismic responses of structures, systems, and components. This has greatly improved the ability to analyze how structures and equipment respond to seismic disturbances.

Seismic risk estimates are conservative, sometimes highly so. This is due, in part, to the assumption that failure of a single or a few components and/or structures brings the plant to core-melt. Conservatism is also compounded by the human factor aspects of the PRA. For example, little, if any, credit is taken in PRA studies for an operator's ability to mitigate an accident induced by an earthquake.

Large uncertainties exist in the likelihood estimates and final results of seismic analyses. These uncertainties exist because the dominant contributors to reactor risk come from earthquakes significantly larger than those used as the safety margin standard in the design of reactors. The frequency of such large earthquakes cannot easily be estimated because of the lack of historical records. In addition, because earthquakes beyond the design basis are the focus of the seismic analysis, extrapolations from historical data on large earthquakes to plant-specific and site-specific situations have to be made. This projects a source of large uncertainty into the analysis.

Many uncertainties are also present in analyzing system and structural responses to earthquakes, both in the characterization of the earthquake and in the description of the dynamic behavior of soil, structures, and subsystems. First, uncertainties in earthquake characterization arise from the limited number of parameters (velocity, energy dispersion, etc.) available to describe the earthquake motion. Unfortunately, recorded information on many important historical earthquakes is limited to structural damage reports and the geographical area over which the motion was felt.

Second, uncertainties are present in system and structure responses. Uncertainties in ground response and soil-structure interactions are due to unknowns in the soil properties themselves. Uncertainties in structure responses and piping systems result from variations in material properties, detail of construction, and assumptions made in the model of the structure.

Uncertainties in evaluating component sensitivities arise from the lack of sufficient and reliable data. Specifically,

there is insufficient knowledge of material properties, inadequate definition of failure modes, too much reliance on engineering judgment and generic data in lieu of complete plant-specific data, a lack of test data for equipment sensitivities, and a lack of data on the correlation between component capacities.

With respect to consequences of earthquakes, there is uncertainty relative to the models used. Few models are now available for predicting the effects of large earthquakes on aspects of the consequence models (e.g., evacuation time, population distribution, etc.).

Finally, there is incomplete identification of all potential seismic-related accident scenarios, a lack of data on the physical interactions between components, and incompleteness in the modeling of dependencies between component failures.

Risk analysis of fires

The early applications of risk analysis to nuclear power plants, including the application presented in the draft report of the Reactor Safety Study, did not include a quantitative assessment of accidents initiated by major fires. No assessment was made because a major fire was not judged by the study authors to be a dominant contributor to risk, and the state of the art had not yet developed an approach to assessing fires.

Fire has only recently become an accepted part of a full-scale PRA study. Those few PRAs that have applied fire methodology (i.e., Big Rock, Zion, Indian Point, and others) have demonstrated important engineering insights concerning plant vulnerability to fires. In addition, a growing body of evidence indicates that fires are important risk contributors.

The largest uncertainty in the probabilistic analysis of fires is the numerical quantification of risk. The uncertainty is due to the lack of an empirical data base for (1) determining the frequency of fire initiation and (2) quantifying the likelihood that a fire, once initiated, will disable critical equipment.

The state of the art is also weak with respect to modeling fire growth and suppression. Available models are only approximate in character and are not capable of accurately modeling fire-spread in unique configurations (i.e., in a compartment crowded full of objects).

The last area of uncertainty--completeness--stems from whether the analysis might have entirely overlooked some critical fire zone, how combustion products can induce failures, and whether all human intervention has been considered.

Risk analysis of floods

In comparison with other external accident initiators, floods have received less attention in PRA studies undertaken in the past. As a consequence, there are no well established methods for analyzing either external or internal floods. The implied perception is that floods are less likely than fires and earthquakes to induce accidents that might contribute significantly to the overall risk of a nuclear plant. In addition, NRC's PRA Procedures Guide states that it is believed that ample warning time would be available to enable safe shutdown of the reactor before significant damage to important systems and structures could occur.

However, several reasons exist for not excluding floods as potentially important risk contributors in PRA studies. First, there are large uncertainties in the estimated frequencies of external floods of extreme severity and in the associated sensitivities of plant structures and components. Second, some causes of flooding, such as the failure of an upstream dam, or a large rupture inside the turbine building's circulating water system, may not provide enough warning time to take corrective or preventative actions. Third, many of the design and operational features required to protect against external floods may not provide the same degree of protection against internally initiated floods. Finally, operating experience shows that floods have resulted in coincident loss of multiple components and multiple systems.

The major weakness dominating the uncertainty in internal flood analysis is the scarcity of data for quantifying the likelihood of flood initiators, such as pipe breaks. Other analytical problems restrict the probabilistic analysis of flood:

- Sensitivity of safety functions is difficult to assess (e.g., fragility caused by a spray-type flood from a pipe break is difficult to analyze quantitatively).
- The corrosion of equipment from the flooding can compromise the ability of a safety function to maintain its operation over the post-accident recovery period.
- The ability to quantify partial blockage of drains necessary to subdue flooding is limited.
- Flooding can bring solid matter such as sludge, silt, etc., into areas where they could cause problems difficult to analyze.
- Human intervention in terminating the flood is difficult to model.

Risk analysis of high winds

Only a few PRAs have included this segment in their overall analyses, and the methods for determining the wind hazard potential have not been applied enough times to enable one to understand all of the problems with the analysis. However, one problem is clear--the various analytical methods that exist might give answers that differ widely.

Other external initiators

The state of the art of all other external causes of accidents, such as volcanoes, sabotage, and transportation accidents, is undeveloped in practice. Most of these have never been examined in a full-scope PRA. The main insights gained to date from the analysis of "other" external initiators are that, generally, they have less risk significance. That is, seldom has any one of them turned out to need further study.

However, the threat of sabotage has been long recognized and treated outside the PRA arena. PRA techniques have, on occasion, been used to do various vital-area and penetration analyses related to sabotage, but the risk of sabotage itself has never been calculated, principally due to difficulty in quantifying the threat frequency. Further, many analysts feel that sabotage would not produce any greater risk than other accidents.

CONCLUSIONS

The Reactor Safety Study suffered from uncertainties with respect to completeness, reliability of data, assumptions made by study analysts, and the validity of models. Since that time, a substantial amount of nuclear reactor experience has accrued, leading to a better understanding of plant design weaknesses, the importance of accident phenomena assumptions, and the significance of certain factors that contribute to plant risk.

Many methodology improvements have been made as understanding has increased and additional PRAs have been performed in the last 10 years. Systems models now examine a broader and more complete range of (1) ways in which systems and components interrelate to operate successfully and (2) events that start accidents. In addition, techniques for identifying severe accident processes are more refined, and the accuracy of plant models and the PRAs' quantitative results have also improved to a limited extent. Finally:

- Human reliability analysis has been refined, formalized, and expanded to address how operator recovery actions can impede the progress of accidents.
- Research undertaken after the Three Mile Island accident has improved the ability to model accident phenomena inside the containment building.

--PRAs have provided a number of significant new insights into off-site consequences.

--Advances have been made in the ability to consider external causes of accidents in PRA.

Although significant studies and advances have been made, PRA is still an evolving methodology for nuclear reactor safety with many uncertainties. Those portions of PRA most affected by the large uncertainties are systems analysis, human reliability, accident phenomenology, off-site consequences, and external initiators. Some of these uncertainties may be inherent to the science of risk assessment or are random and inherently irreducible. Others, however, reflect current experience and knowledge and, therefore, could be reduced with additional research and empirically derived data. To put this conclusion in its proper perspective, however, it should be recognized, as discussed in chapter 1, that these uncertainties and limitations also apply to the traditional analytical methods used by the nuclear industry and NRC in addressing and resolving nuclear power plant design and safety issues.

CHAPTER 3

NRC RESEARCH PROGRAM ADDRESSES LIMITATIONS

IN PRA METHODOLOGY BUT CANNOT ELIMINATE THEM

Beginning in 1983, NRC set a course for reducing the uncertainties in PRA through a 3-year, \$25-million research program to examine the segments of PRA with large uncertainties--plant systems analysis, human reliability, accident phenomenology, off-site consequences, and external accident initiators. NRC's program is directed at those areas where improvements are possible on the basis of current scientific knowledge and available resources.

Although broad in scope, NRC's program will not be sufficiently extensive to reduce the uncertainties to a level that would make bottom-line risk estimates reliable measures of plant safety. In addition, NRC's program does not address some important limitations in PRA. For example, NRC will not collect data on the reliability of plant components, nor will it research several external events that could start severe accidents and possibly cause multiple failures. As a result, some improvements will be made, but the areas of large uncertainty--completeness, sufficiency and reliability of data, assumptions made by study analysts, and validity of models used--will remain. Further, some of the causes of uncertainty in PRA may be unresolvable, such as identifying (1) all potential causes of accidents that have not or may never occur or (2) the precise physical and chemical changes that occur in a reactor core during a core-melt accident.

NRC IS IMPROVING PRA TECHNIQUES

To reduce many of the uncertainties that plague various segments of PRA, NRC has undertaken a research program costing approximately \$25.5 million between 1983 and 1985. Research activities consist of developing and refining analysis methods, collecting experimental and actuarial data in some areas of PRA, and demonstrating state-of-the-art techniques in a full-scope PRA of the LaSalle power plant.

Plant systems analyses will be expanded to include new information on human error and external accident initiators, thereby making the analyses more complete. NRC will also develop integrated systems modeling techniques to allow risk comparisons to be made between internal and external causes of accidents. In the long run, NRC plans to develop a numerical data base to support estimates of accident probabilities. It will be derived, to a large extent, from existing data and, to a lesser extent, from new data generated by other NRC research activities. The new data will include multiple failure rates due to common-cause events and component failure rates under severe accident environments (i.e., high radiation, excessive vibration, etc.).

Second, NRC hopes to produce state-of-the-art models for evaluating the human role in plant risk. New data to support these models will be collected from controlled experiments, plant simulators, and actual occurrences reported in licensee event reports. (The latter are reports of plant component and system failures that utilities are required to make to NRC.)

Third, NRC has many developmental programs underway to research accident phenomenology inside the containment building. From this work, NRC expects to considerably enlarge knowledge of accident processes, the amount and type of radiation released, and the behavior of radioactive material.

Fourth, NRC's research activities in the area of off-site consequences should, in 2 years, provide improved estimates of the effects of severe accidents on man and the environment. The major activity in this area is the development of the MELCOR computer model that will replace the comparatively limited consequence models in use today. MELCOR will contain new data on projected health effects, evacuation schemes, radiation release exposure pathways, and economic effects. Long-duration releases of radiation will also be evaluated.

Finally, NRC plans to produce methods for assessing the risk of earthquakes, fires, and internal floods. These plans will include developing both models and data on these external accident initiators.

UNCERTAINTIES WILL REMAIN LARGE IN FOUR AREAS

Although NRC is trying to improve PRA techniques for nuclear power plants in many areas, these efforts are not extensive or concentrated enough to reduce the related uncertainties, discussed in the previous chapter, to a level at which the bottom-line estimates of risk are reliable. In addition, NRC's research program does not address many important limitations in PRA. Therefore, while NRC's program may advance the state of the art of PRA and increase its usefulness in identifying and correcting potential contributors to nuclear plant risk, it will not make PRA sufficiently reliable to serve as the sole or primary basis for determining plant safety. However, PRA can serve to supplement the more traditional analytical methods. The areas of uncertainties that will remain after NRC's research improvements are discussed below.

--NRC research activities will reduce some of the uncertainties with respect to completeness, but it will still not be possible to ensure that every potentially significant occurrence in a plant systems analysis has been considered.

--NRC's data collection activities address some, but not all, of the PRA data requirements. For example, the research

will not provide a complete set of data regarding what components fail during accidents. Therefore, the sufficiency and reliability of data will continue to be a major source of uncertainty in PRA.

--Uncertainties introduced through assumptions made by study analysts will persist in areas that are not well understood, such as in human behavior, external causes of accidents, and phenomenology within the containment building. NRC's planned research activities will improve knowledge in these areas, but may do so only to a limited extent because of the narrow scope of the program.

--NRC's research program does not completely address how accurately models characterize plant behavior. NRC is producing thermal-hydraulic computer models that better detail accident progression and provide more realistic system success criteria; however, large uncertainties will still exist for some accident scenarios. Absolute validation of plant models remains an inherent limitation that is not likely to be resolved. Validation is now possible only for particular elements of a PRA analysis by using operational or experimental data. However, validation of the frequency of rare events depicted in plant systems analysis is not subject to experimental confirmation.

SOME PRA SEGMENTS WILL CONTINUE
TO HAVE LARGE UNCERTAINTIES

NRC's research program is concentrated in those segments of PRA having large uncertainties--plant systems analysis, human reliability, accident phenomenology, off-site consequences, and external accident initiators. In 3 years, NRC expects to make improvements in these areas but recognizes that, despite these improvements, uncertainties will remain large.

While NRC's program is purposely broad to encompass the PRA segments with large uncertainties, it has some shortcomings. For example, NRC is not requiring utilities to collect component reliability data needed in plant systems analysis. However, the Institute of Nuclear Power Operations--an organization created by the nuclear industry following the Three Mile Island accident--has agreed to collect these data. NRC believes that the industry should assume some responsibility for collecting the data and that the Institute might be more successful than NRC has been in getting utilities to voluntarily report component failures. Other shortcomings include the exclusion of certain external accident initiators from the program on the basis of the perception of relatively low risk. The NRC is monitoring and evaluating this activity.

Plant systems analysis

NRC's research program addresses two areas of the problem of accurately characterizing plant behavior in a plant systems analysis. They are the integration of external causes of accidents and human behavior into plant systems analysis.

In the first area, NRC will develop integrated system modeling techniques that apply to external, as well as internal, causes of accidents. These modeling techniques, which will be developed under the NRC project entitled "PRA Methods Improvement for the Risk Methods Integration and Evaluation Program," should allow for the first time meaningful risk comparisons to be made between external and internal accident initiators. For the second area, NRC will incorporate data resulting from human reliability research into the systems analysis. These data will permit the PRA to model both positive and negative human actions that either initiate or direct the course of accidents.

Although these improvements will increase the number of events that are considered in a PRA, it will not be possible to ensure that every potential significant occurrence in the course of systems analysis has been considered.

NRC does not have any individual research activity that addresses the accuracy of plant systems models. Any improvements in this area will have to come from increased experience in operating nuclear reactors and in using the PRA models themselves. NRC is producing more advanced computer models that better detail how accidents progress and provide more realistic system success criteria; however, large uncertainties will still exist for some accidents.

In fiscal year 1984, NRC began initial planning to develop a comprehensive numerical data base for use in plant systems analysis. This data base will be derived from both existing and new data sources. Although various data sources exist, they are deficient in many respects. As a result, NRC plans to collect and analyze additional data, particularly in the areas of initiating events, component failures, test and maintenance results, and common-cause failures. None of the data requirements, however, will be completely fulfilled in the near term. NRC's activities are limited in scope and do not address all types of data needed. As a result, the planned numerical data base will not be functional until a substantial amount of data collection and analysis beyond what NRC currently plans is undertaken.

Data on internal causes of accidents are relatively mature. NRC does not plan to collect many additional data on these events since it has already developed frequencies for internal accident initiators (i.e., transient events and loss of coolant accidents). However, few data are currently available on external causes of accidents, and only one project is currently planned in

this area--a study of internal and external flood hazards. Many data are still needed for plant systems analysis on other types of external accident initiators, such as earthquakes, fires, and high winds, to advance the state of the art in this segment of PRA.

NRC has undertaken several projects to develop or supplement generic data bases on component reliability. In fiscal year 1983, NRC completed a generic component reliability data base. However, this was a cursory effort to use expert opinion to modify the component failure rates from the Reactor Safety Study. Therefore, its basis lies in subjective estimates rather than actual occurrences.

NRC's principal project in this area is the In-plant Reliability Data System. This system is derived from complete historical data from plant maintenance and operating logs. This will be a comprehensive collection of component failure information on five types of components sampled from eleven units at seven plants. When completed, the system will be a good data source for a very small number of components on the basis of hard historical data.

Collecting generic test and maintenance data (beyond the five types of components sampled from plants in the In-Plant Reliability Data System) would enable PRA analysts to determine the reliability of components (i.e., whether they are in operating order when called upon to function) and the number of times components fail during operation. NRC never intended this system to be a large data base, however, because the cost of collecting vast amounts of data is prohibitive. Further, NRC believes the impetus for such a data base should come from industry.

NRC has also sponsored a project, to be completed in fiscal year 1984, that estimates component failure rates from information contained in licensee event reports. The licensee event reports proved to be a poor source for component reliability data as they did not contain information on the number of demands made on each system in relation to the number of failures. Also, a January 1, 1984, change in NRC's licensee event-reporting requirements eliminated the collection of data for some events that are used to produce these summaries.

Few data are available regarding what components fail during accidents. NRC initiated the Harsh Environment Data Project to determine whether sufficient data exist to develop a comprehensive data base of failure rates under harsh environments, including high radiation, excessive vibration, high temperatures, and component immersion in liquid. Although such data does exist, it is proprietary; thus no NRC harsh-environment data base could be constructed.

Common-cause failure data will also be generated for NRC's Risk Methods Integration and Evaluation Program, but how substantive this information will be is not yet known. Common-cause data

describe the frequency of concurrent failures due to a single event, such as an earthquake. These data are needed to identify system dependencies in a PRA. NRC has many existing sources of common-cause data from which failure rates will be extrapolated for this program. These sources include Pickert, Lowe, and Garrick studies, Idaho National Engineering Laboratory reports, the In-plant Reliability Data System, and several nuclear plant PRAs. However, because many potential component combinations affected by common-cause failures exist, a substantial number of additional data needs to be collected. This includes data identifying common-cause failures, causes of accidents, component susceptibilities to these initiators, component locations, and time of failures.

NRC is in the process of developing statistical techniques to enhance the credibility of data used to quantify PRA models. NRC's efforts include investigating the sensitivities of uncertainties, determining how uncertainties are reproduced in large fault-trees, investigating the collection and analysis of subjective data, analyzing harsh environment and common-cause data, and identifying factors affecting component failure rates in the In-plant Reliability Data System.

Human reliability

NRC plans to refine the human reliability analysis segment of PRA through improved modeling and data collection.

Under the Human Performance Modeling Project, NRC will produce state-of-the-art models that describe human behavior and its impact on plant risk. However, the method now in use gives differing results when repeated by different analysts due to the subjectivity of the data that go into the analysis. On the other hand, it does consider decision-based errors and factors that affect operator performance, such as stress. This method is a preliminary attempt to model decision-based errors (e.g., misdiagnosis of an accident)--an area that needs further exploration.

Most of NRC's research efforts relating to human reliability analysis center around developing a more reliable human error data base. NRC's major activity is the proposed Human Reliability Data Bank. Under this project, NRC reviewed other data bases to determine whether they would be good sources of human error probabilities along with those in the Handbook of Human Reliability Analysis, prepared for NRC by Sandia National Laboratories.

Only a few existing data sources were found to be useful. As a result, NRC plans to develop a method for compiling information from the various sources into a central human reliability data bank and then to collect the remaining necessary data. Data sources will include previously established data bases, nuclear

reactor simulator research, and nuclear power plant field experience. This project includes the development and testing of procedures for comparing and combining data from diverse sources for inclusion in the data bank.

NRC also plans to develop techniques for acquiring reliable human error data from a variety of nuclear power plant-related sources. These techniques will cover

- expert judgment;
- reactor control room simulators;
- operating power plants using existing licensee event reports and the Institute of Nuclear Power Operations' Nuclear Power Reliability Data System; and
- computer modeling of power plant normal, transient, and emergency events, especially in the maintenance area.

As a result of this effort, NRC has published a book of procedures for using expert judgment to estimate human error probabilities in nuclear power plant operations. NRC is also completing a 3-year study that will determine whether a voluntary nuclear power safety reporting system can be established that can provide useful PRA data.

NRC's efforts to improve human error data are likely to improve the confidence bounds for human error probabilities. It is expected that as the data base continues to improve, statistically derived confidence bounds can be developed to replace those now based on subjective judgment.

Although it appears that substantial human error data collection either is being explored or undertaken by NRC, this segment of PRA still suffers from scarcity of actuarial data. NRC's data collection activities also suffer from other weaknesses.

First, it will take NRC a long time to collect the large body of data needed to improve the human reliability segment of PRAs. In addition to the need for controlled experiments to answer specific questions about behavior dynamics, data based on the experiences of nuclear power plant personnel are also required. The present licensee event-reporting system does not provide such data. While these reports do provide valuable information about errors that are reported, they rarely report or describe in sufficient detail the important factors affecting operator performance that would allow a complete analysis to be made. In addition, many errors are not reported at all: these include, but are not limited to, errors that did not result in reportable events. Thus, the information needed to estimate human error probabilities (i.e., number of errors and opportunities for error) is inadequate.

Simulator data are a good, but perhaps not a reliable, source for human error probabilities. To predict how nuclear power plant personnel perform under stress (i.e., abnormal events), it is essential to obtain this information as soon as possible after an abnormal event. Without such data to modify human error probabilities collected in simulations, simulator data will continue to be suspect.

Studies that simulate tasks performed outside the control room are also needed. The Reactor Safety Study risk estimates indicated that most of the human error impact on the availability of an engineered safety feature arose from maintenance and calibration tasks and errors associated with restoring safety features to their normal operating states, rather than from control room activities. NRC has developed a computer simulation model to analyze these non-control room activities.

Accident phenomenology inside the containment building

NRC has many developmental programs under way to research accident phenomenology inside the containment building. Most of these programs will culminate in the creation of a set of computer models that describe the behavior of severe accidents. Although considerable improvement in knowledge about severe accidents should result from ongoing research, major uncertainties will continue to exist in this aspect of PRA methodology. Again, however, it is important to note that uncertainties in accident phenomenology are also present in the deterministic methods now used by NRC and the nuclear industry.

NRC's research activities are centered in the areas of

- physical processes,
- release of radioactive material,
- behavior of radioactive material, and
- computer model development.

Physical processes

The analysis of physical processes, as outlined in NRC's Severe Accident Research Plan, contains many elements: Behavior of damaged fuel, hydrogen generation and control, fuel-structure interaction, containment analysis, containment failure modes, and development of computer models. NRC has research activities in each of these areas.

The accident at Three Mile Island raised many questions concerning the behavior of severely damaged reactor cores with respect to the release of accident by-products and hydrogen, and

whether the core could be cooled. To answer these questions, NRC is attempting to develop a data base for the range of conditions covered in severe accidents. The data base will help to predict

- the rate of hydrogen generation,
- the magnitude and release of accident by-products and their chemical form,
- the cooling requirements of the core, and
- the manner in which fuel is redistributed as the reactor loses the ability to cool itself.

This program will further develop two risk models. One will treat the development of fuel damage in the original core volume and the other will treat the redistribution of liquified and molten fuel through the process of core-damage and core-melt.

During an accident, or as a consequence of an accident, significant quantities of hydrogen can be generated in the reactor vessel and in the containment building. The burning of hydrogen could have two adverse effects. First, it could produce threats (such as pressure) to the containment that could exceed the ultimate strength of the building. Second, it could cause safety-related equipment to fail, which would affect the safe shutdown of the plant.

NRC's research program is currently providing information and analytical models to quantify this threat and to assess the efficiency of safety systems proposed by near-term operating license applicants and of possibly more efficient systems. This program will also develop analytical models that will permit a better understanding of how hydrogen moves in the containment building and how hydrogen burns.

The scope of NRC's research with respect to fuel-structure interactions will include small-scale experiments that examine how fuel interacts thermally, mechanically, and chemically with the containment building and structures inside the building. NRC also plans to test the accuracy of models, quantify release amounts of gaseous and radioactive materials, and evaluate the effect of coolant on the fuel-concrete interactions. The specific items to be addressed include

- the interaction of core material or severely damaged fuel with the internal containment environment,
- the rapid generation of steam and the possibility of steam explosions when the fuel interacts with water,
- the pressure on the containment structure,

--the effect on instrumentation required to follow or control the accident, and

--the amount of radiation released to assist in the design of safety systems to suppress an accident.

Next, NRC has undertaken a containment analysis project intended to improve the evaluation of nuclear power plant containment systems. As part of this effort, a computer model is being developed that will predict and characterize the chemical and mechanical pressures imposed on a reactor containment system during an extreme accident. This model will be sufficiently general to accommodate any type of containment or reactor. The Advisory Committee on Reactor Safeguards believes that considerable improvement in the state of knowledge in this area will result from NRC's research.

Containment analysis, as it exists today, reflects a major change in thinking concerning containment performance during a severe accident. One result is the expectation of fairly high containment effectiveness for some accident scenarios. However, the greatest uncertainties in containment performance in an accident lie not in the structural integrity of the containment itself, but rather in how the containment structure might fail. For example, a failure through the containment floor involves the interaction of a large mass of molten fuel and a massive slab of concrete, followed by a leak from the bottom of the containment to the outside. Currently, knowledge of how this can occur is limited. In contrast, direct containment structural failure is known to be pressure-dependent.

The main safety question in this area relates to the ability to confidently predict the amount of pressure that can be sustained by a containment structure before the rate of leakage becomes unacceptable. PRAs today cannot reliably predict how leakage will occur. The technical problems involve (1) developing an ability to predict deformities for the wide variety of containment types, (2) relating damaged areas of containment structures to leak behavior, and (3) determining the sensitivity of predictions to uncertainties about actual containment structures and the pressures associated with accident and severe environmental conditions.

NRC is developing and verifying methods to reliably predict the capacity of containment structures under accident and severe environmental pressures. This project will be a combined analytical and experimental study of steel and concrete containments. Failures resulting from both physical rupture of the containment structure and excessive leakage due to damage to the containment building will also be studied. The temperature and pressure histories necessary to cause excessive leakage will be established.

Release and behavior
of radioactive material

PRAs consistently indicate that the uncertainties associated with estimating radiation release and behavior are among the largest contributors to uncertainties in the risk to the public from severe accidents. This result is not surprising for two reasons: (1) off-site consequences are directly affected by the magnitude, timing, and makeup of radiation released from containment and (2) there are large uncertainties regarding the actual amount of radiation that might be released to the environment.

NRC is planning several projects to study both the release and behavior of radioactive material. The ultimate objective of these projects is to improve the quality of predictions of the potential radiation released from containment under accident conditions. Although a significant number of data are available on what by-products are released, and how they behave under controlled loss-of-coolant accidents, there are gaps in the data base relative to radiation release and behavior under severe core-damage and core-melt accidents. Therefore, NRC will develop an experimental data base and models to predict the release amounts and their associated behavior.

To support this project, data will be collected on (1) the release of radioactive by-products and nonradioactive aerosols from overheated and melting fuel, (2) the chemistry of the released products, (3) the reactions that generate aerosol, (4) the behavior of radioactive by-products and aerosols in the reactor coolant system and in the containment building, and (5) the effectiveness of engineered systems in suppressing the release of radioactive by-products under severe accident conditions.

Research efforts to investigate and quantify the release of radioactive by-products and aerosols from the fuel will include

- an experimental program to measure the release of radioactive by-products from light-water reactor fuel rod segments in a steam environment,
- experiments to investigate the release of radioactive materials and aerosols from larger bundles of fuel,
- a program to investigate the release of aerosols from molten core materials interacting with the concrete in the reactor cavity, and
- examination and analysis of samples of the Three Mile Island 2 core.

Computer model development

NRC is developing a computer model, called MELCOR, to analyze all segments of accident phenomenology inside the containment building--accident processes, release of radioactive materials, and behavior of radiation--and off-site consequences. MELCOR represents a major breakthrough because it will be the first model to link the processes of accident phenomenology with off-site consequences. For example, MELCOR will permit the quantitative evaluation of uncertainties, which was not possible with the older computer models.

Some of the improvements that will appear in the MELCOR model include

- ease of model replacement as new experimental data and analytical models become available;
- direct and completely compatible linkage between in-plant accident phenomenology and off-site consequences, permitting both "best-estimate" calculations and reproduction of uncertainties; and
- easy maintenance of models.

Off-site consequences

NRC programs in the area of off-site consequences should, in 2 years, provide improved estimates of off-site consequences, quantitative estimates of uncertainties, and increased confidence in the results. However, the single largest contributor to uncertainty in off-site consequence estimates relates to the magnitude of the radioactive materials released to the environment. Therefore, improvements in this area are largely dependent on developments in the radiation release and behavior research discussed earlier.

NRC research efforts in this area are directed at modeling advances in the MELCOR code for

- models that measure the dosage of radiation,
- routes that radiation can follow to exit from the containment building,
- models describing economic effects like property damage,
- data on evacuation routes,
- releases of radiation that are of long duration,
- releases that are in the form of radioactive "rain," and

--uncertainty analysis.

Models used in consequence analyses to predict radiation doses will be revised to incorporate more data on health effects. However, data on the actual health effects of radiation exposure are severely lacking for two reasons. First, the data are limited to the recorded effects of radiation occurring in historical events such as the bombing of Hiroshima and the testing of the hydrogen bomb. No recent radiation accidents have occurred that would increase knowledge of health effects. Second, many experts now believe that much less radioactivity would be released in a core-melt than was commonly believed a few years ago. Thus, in many cases, it may be that no more than a few early fatalities would occur in the event of a major accident. If this should be true, health consequences would likely be confined to large numbers of people being exposed to low levels of radiation. However, the subject is still highly controversial, and a definitive data base is lacking.

Another improvement in consequence analysis will result from NRC's examination of the relative importance of the different routes by which radiation can be released to the atmosphere. For example, NRC is now analyzing the potential consequences resulting from accidental releases of radioactive material to water routes like rivers and streams.

The economic models used in consequence analyses will also be improved. NRC is developing several detailed models depicting the off-site economic impact of different radiation release categories.

NRC plans to incorporate into MELCOR more sophisticated data on area evacuations, including more detailed evacuation routes, the effects of traffic jams, and delayed evacuation. These new data have resulted from NRC's increased experience with evacuation drills over the last few years.

The NRC-sponsored International Comparison Study will produce criteria for performing consequence analyses of long-duration radiation releases. These analyses will replace prior consequence analyses that considered only one-time short releases of radiation. A long, slow release would spread the radioactive material over a larger area and decrease the individual doses and health effects. Therefore, this new perspective could affect the predicted concentrations of radiation released and the consequences. Long-duration releases are being studied as part of NRC's research program on radioactive "rain." In this project, NRC is studying the water content of radioactive atmospheric discharges during severe accidents.

External accident initiators

NRC has initiated several programs to research seismic-, internal flood-, and fire-related causes of accidents; however several other events considered to have less risk significance are not being examined. The Advisory Committee on Reactor Safeguards believes that NRC's program is deficient in that it does not adequately address severe winds, external floods, and seismic design margins.

Earthquakes

NRC initiated a \$12-million Seismic Safety Margins Research Project in fiscal year 1979 with the purpose of developing methods for producing quantitative seismic risk estimates and producing more quantified estimates of safety limits for some plant structures, systems, and components. This includes determining seismic characteristics for a plant site, calculating how the soil and plant would interact during an earthquake, and determining major structure and subsystem responses with their associated failure probabilities.

Another project, entitled Seismic Hazard Characterization for Nuclear Power Plants in the Eastern U.S., is a probabilistic study to improve the estimation of seismic risk for all eastern U.S. plant sites. In addition, the Seismic Design Margin Research Program is being used to judge the adequacy of seismic design margins in plants using existing PRAs.

The Advisory Committee on Reactor Safeguards has commented on the adequacy of these NRC seismic projects. The Committee's assessment is that although NRC has developed seismic design criteria, the effectiveness of these criteria in controlling risk is not well quantified. In addition, the current determination of seismic contribution to risk involves large uncertainty. Data are still lacking in the areas of structural and component sensitivities and seismic risk information. In addition, the need to extrapolate seismological data from earthquakes larger than the design basis has resulted in large uncertainties in seismic risk estimates.

Fires

NRC started a PRA fire project in fiscal year 1983 to address the risk posed by fires in nuclear power plants. The main objective of this project is to improve upon current methods for modeling fire-initiated accidents to reduce the uncertainties in risk estimates. This project will produce a fire risk modeling approach for nuclear facilities using state-of-the-art techniques and will estimate the size of uncertainties in fire risk models. Therefore, the program will attempt to investigate how fires start, spread, grow, do damage, are detected, and are extinguished.

NRC will address the deficiencies identified in prior fire analyses attempted in the Indian Point, Zion, Big Rock Point, and Limerick PRAs, including

- a lack of documentation,
- an unsupported basis for fire growth and suppression assumptions,
- optimistic assumptions regarding operator response during a fire (i.e., the operator will succeed in suppressing the fire),
- unsubstantiated causes of equipment failures, and
- critical plant areas that were not addressed in prior fire analyses.

The remaining limitations involve the need for improved fire growth and suppression models and several data bases. NRC is working on improvements to the fire growth models. A data base is needed describing the maximum amount of heat the plant can sustain before systems and components are damaged, and how effective safety systems are in controlling fires. Data are also needed on the chemical makeup of the different materials that could fuel a power plant fire and on the size of fires caused by these fuels. Work to address the vulnerability of systems and components is on-going. Further, a limited survey of materials that could fuel fires is underway.

Floods

NRC is examining the risk from internal floods but is not researching the risk posed by external floods. The Advisory Committee on Reactor Safeguards has repeatedly criticized NRC for overlooking external floods in its research program. In addition, as far back as 1977, NRC's Office of Nuclear Reactor Regulation requested flood research to support its regulatory activities. NRC's Office of Research, however, does not believe external floods have high risk significance because adequate warning time would be given in the event of a flood. However, the Office of Research plans to reevaluate external flood research and will begin a research program in 1986, if they believe it is warranted.

NRC's internal flood project is a 2-year effort, which began in fiscal year 1984, to develop a method for calculating system performance as a function of the depth of water in the flooded plant. Because this project is still in the developmental stage, it is not clear how it will improve the state of the art of PRA or what the size of the uncertainties in the flood risk analysis will be.

Other external accident initiators

NRC's research program will not address several external causes of accidents. These include accidents started by high winds, other natural phenomena (such as volcanoes), transportation accidents, and sabotage.

The Advisory Committee on Reactor Safeguards has commented that NRC should explore some of the external causes of accidents listed above. In particular, high winds and sabotage are areas in which the Committee has repeatedly recommended additional work. NRC, however, believes these areas to be either low in risk significance, such as external floods, or too difficult to assess the risk, such as sabotage.

CONCLUSIONS

NRC's research program concentrates on the segments of PRA with large uncertainties and where improvements are possible in the light of current scientific knowledge and available resources. If successful, NRC will reduce many of these uncertainties. However:

- Uncertainty with respect to completeness will remain because it is not possible, for example, to ensure that every potentially significant event has been considered in a plant systems analysis.
- The sufficiency and reliability of data will continue to be a source of uncertainty because NRC's data collection activities are limited in scope.
- Uncertainties introduced by study analysts will persist in areas that are not well understood, such as in human behavior, external causes of accidents, and phenomenology within the containment building.
- It is unlikely that the accuracy of key computer models used in PRAs can be validated due to the variety of events, such as accidents leading to core-melt.

To reduce these causes of uncertainty to a level that would substantially improve the reliability of the bottom-line risk estimates would require a research program beyond what NRC is currently undertaking and a decision by NRC that PRA has enough regulatory importance to justify these expenditures. In addition, some of the causes of uncertainty in PRA may be unresolvable because they are inherent to the science of risk assessment. These include identifying all potential causes of accidents because they have not occurred or may not ever occur, or identifying the precise physical and chemical changes that occur in a reactor core during a core-melt accident.

CHAPTER 4

PRA SUPPLEMENTS THE REGULATORY

DECISIONMAKING PROCESS IN MANY AREAS

Analysis to demonstrate compliance with regulations has traditionally been based on conservative engineering judgments. Even this traditional, or deterministic, approach to licensing has been sprinkled with judgments regarding the likelihood of occurrence of certain events. These judgements are apparent, for example, in NRC's long-standing requirements for redundancy and diversity in plant systems and components, such as multiple sources of power to operate safety systems.

Now, however, NRC and plant owners are using PRA to analyze a wide variety of regulatory issues related to the risk from severe accidents and to provide supplemental qualitative and quantitative information to decisionmakers regarding these issues. These analyses vary from large-scope studies of entire plants that require a year or two to complete, to limited analyses of individual plant systems that may be performed in a matter of days. For example, PRAs have been used to

- disclose the risk of severe accidents in environmental impact statements of new plants;
- analyze and improve the safety of individual operating plants;
- supplement NRC decisionmaking, in a variety of ways, on safety issues common to all plants or large classes of plants; and
- estimate the benefits, in terms of reduction in risk, of proposed regulatory actions for comparison with alternative actions and the costs of these actions.

Given the limitations in the state of the art, NRC has appropriately used PRA to supplement its decisionmaking processes in the areas discussed above. However, in estimating the benefits of alternative regulatory actions, NRC uses "bottom-line" PRA results, which are the most uncertain aspect of PRA, and compounds those uncertainties by assigning arbitrary dollar values to human life and health effects. Although NRC officials who have developed these PRA-based estimates say that they lead to more thorough and objective analysis, the use of "bottom-line" risk estimates and their conversion to dollar amounts may add another layer of uncertainty to the cost/benefit calculations.

NRC USES PRA TO ANALYZE SEVERE
ACCIDENT RISK AT NEW PLANTS

The National Environmental Policy Act of 1969 requires federal agencies to prepare detailed environmental statements on proposed major federal actions significantly affecting the quality of the human environment. Pursuant to this requirement, NRC prepares an environmental statement on each application for a nuclear power plant construction permit or operating license.

In June 1980 the Commission published an interim policy statement on nuclear power plant accidents that requires the NRC staff to consider the probabilities and consequences of severe accidents--for example, release of radiation--in environmental statements. NRC did not require this until then because such accidents were thought to be too unlikely to ever occur. The change in policy was prompted by severe accident considerations raised in the Reactor Safety Study in 1975, in some of NRC's environmental reviews during the late 1970's, and by the March 1979 Three Mile Island accident.

The NRC staff has implemented the Commission's 1980 interim policy statement by including an analysis of severe accident probabilities and consequences in the 20 environmental statements issued since that time. At the close of our review in December 1983, environmental reviews were in progress for an additional 18 plants at 12 sites.

Severe accident assessments are based on
both generic and plant-specific information

The severe accident assessments for environmental statements published before 1984 were based on the generic releases of radioactive materials that were estimated to result from the most important accident sequences in the Reactor Safety Study. The only plant-specific aspect of the reviews was the analysis of off-site consequences based on these releases.

The severe accident risk assessments were updated to incorporate subsequent improvements in data and modeling techniques. This was done only once, not separately for each plant. For plants currently undergoing environmental review, NRC has further modified the assessments on a plant-specific basis by eliminating those accident sequences that are unlikely or impossible to occur due to differences in individual plant systems.

PRA consequence analyses that incorporate site-specific features, such as population density, weather, and land-use statistics, are performed individually for each plant. The analyses are done with the aid of a computer program originally developed for the Reactor Safety Study.

NRC plans to continue basing assessments of severe accident risks for individual plants on modified generic Reactor Safety Study accident sequences, except when a plant-specific PRA is available. The Chief of NRC's Accident Evaluation Branch, which performs severe accident consequence analyses, and NRC licensing officials told us that entirely plant-specific studies would more accurately analyze the risk of severe accidents at individual plants. They added, however, that using the Reactor Safety Study results is faster and less costly.

The Accident Evaluation Branch Chief and an NRC attorney who reviews severe accident assessments told us that the main purpose of the severe accident assessment is to disclose the risk of such accidents to the public. The assessments have not, they said, led to discovery of any unusual site or plant characteristics that might prompt NRC to order plant modifications.

Studies of two new plants may set precedent for the use of PRA

Concerns about the risks posed by plants in densely populated areas prompted the NRC staff to request the owners of the Limerick Generating Station, near Philadelphia, and Millstone 3, in Connecticut, to perform plant-specific PRAs. Both studies have been completed and submitted to NRC. This is the first time that plant-specific PRAs and the information that they provide have been available for new plants early enough to play a significant role in the operating license process. Both studies are being used as the basis for severe accident assessments in their environmental statements.

The Philadelphia Electric Company submitted a full-scope (i.e., level-three) PRA of its Limerick Generating Station in July 1981 and an additional analysis that included consideration of external events in May 1983. NRC's review of the study is complete and the staff has prepared testimony for PRA-related licensing hearings that are underway and expected to continue through 1985.

The availability of plant-specific PRAs in operating license reviews and hearings is new. Therefore, precedents in the use of PRA may be set during the course of the Limerick hearings. The NRC staff has stated that it will use information provided by the PRA to supplement the staff's traditional deterministic safety review (i.e., compliance with the regulations) and in discussions of environmental impacts. The Philadelphia Electric Company challenged the use of its PRA in the licensing hearings, stating that NRC policy calls for licensing decisions to be based principally on an applicant's compliance with applicable regulations.

Northeast Utilities submitted a full-scope PRA, including consideration of external events, of its Millstone 3 plant in August 1983. NRC is currently reviewing the study, and the staff

plans to use it as the basis for the severe accident analysis in the environmental statement for Millstone 3.

NRC policy concerning requirements
for plant-specific PRAs is inconsistent

With the exception of the Limerick and Millstone 3 plants discussed earlier, NRC does not plan to require plant-specific PRAs for any other plants now under active construction. NRC considered the possibility of requesting additional plant-specific PRAs of new plants in a 1981 staff policy statement that categorized all of the existing and planned reactor sites according to their proximity to densely populated areas. However, the decision to request additional PRAs was deferred, and the policy statement is out of date. Since that time, two plant owners have voluntarily submitted PRAs, in addition to the two studies requested by NRC, for plants located in areas with above-average population density.

On the other hand, NRC added to its reactor safety regulations the requirement that power plant applicants must perform a plant-specific PRA within 2 years of NRC's issuance of a construction permit or manufacturing license. This is a Three Mile Island-related rule intended to seek design improvements that are significant and practical and that do not have a significant impact on the basic plant design. This PRA performance requirement may increase the number of future plant-specific PRA's; however, NRC is not aware of any new construction permit applications likely to be submitted before the end of fiscal year 1985.

NRC AND PLANT OWNERS USE PRA TO
EXAMINE INDIVIDUAL OPERATING PLANTS

Both NRC and plant owners have used PRA to analyze and improve the safety of individual operating plants. Studies have been performed to assess the overall risk posed by individual plants, to analyze the workings and reliability of individual plant systems, and to rank safety issues on an individual plant basis according to their importance to risk. The scope, depth, and plant-specificity of these studies have varied according to the purpose of the analysis and the resources available.

We found that PRA was used as a supplement to NRC's traditional deterministic analysis, rather than as the sole, or even primary, basis for decisions. Plant-specific PRAs have, however, led to the discovery and correction of unsafe conditions that may not otherwise have been found and have prompted safety improvements at individual plants.

PRAs performed to advance the state of the art have provided safety insights

Nine of the existing plant-specific PRAs performed since the 1975 Reactor Safety Study were sponsored by NRC as part of research programs to advance the state of the art. (These programs are described in ch. 1.) While the main purpose of the Reactor Safety Study was to quantitatively assess the risk of nuclear power and compare this risk to other special risks, the nine subsequent NRC-sponsored studies had a number of purposes. They were to apply PRA techniques to a broader range of plant types than had previously been done, expand the cadre of PRA practitioners, and further develop PRA methods. These PRAs also had the important benefits of providing safety improvements to the individual plants examined.

For example, the limited PRA of the Sequoyah 1 plant highlighted the importance of two drains located between the upper and lower compartments of the plant's containment structure. The drains were closed during refueling but were to be left open after refueling. If these drains were inadvertently left closed, water sprayed into the upper compartment during an accident would not drain to the lower compartment. This could lead to failure of two plant systems that required water from the lower compartment. These failures, in turn, could lead to a core-melt and possibly a release of radiation. The PRA identified the importance of the drains in this chain of events, and procedures were changed to ensure that the drains were left open after refueling.

Another example occurred during the performance of the Millstone 1 Interim Reliability Evaluation Program PRA. A utility analyst discovered two violations of NRC's "single failure criteria" that apparently had been unknown to plant operators and NRC inspectors since the plant began operation more than 10 years before. NRC's single-failure criterion for electrical system design requires that the failure of a single component should not result "in a loss of the capability of the system to perform its safety function." While working on fault-trees, the utility analyst discovered that the failure of either of two relays in the electrical power system would disable the plant's emergency on-site alternating current power system--one of the redundant safety systems to ensure that core cooling is not interrupted. The discovery of the violations was reported to NRC within days and corrected by the utility.

PRAs are used to analyze a variety of individual plant safety issues

Licensees have voluntarily submitted PRAs of varying scope to NRC to support their positions concerning plant safety, exemption from selected post-Three Mile Island requirements, and requests for license amendments. NRC has also used PRAs to analyze these issues at some plants.

NRC officials involved in the performance and review of these analyses told us that PRA adds support and rationality to largely subjective judgments on the issue to be decided. They added that it forces analysts to systematically lay out their reasons for subjective judgments, use factual support when available, and explicitly identify the uncertainties in analyses that might otherwise be completely subjective.

NRC and plant owners used PRA to assess the overall risk of plants at two densely populated sites

Because of concern over the risk imposed by plants operating in densely populated areas, NRC performed limited PRAs of the Zion 1 and 2 plants, near Chicago, and Indian Point 2 and 3, near New York City. These four plants began operating between December 1973 and August 1976. The studies indicated that if one of the plants analyzed in the Reactor Safety Study were located at the Zion or Indian Point sites, it would present significantly more risk to the public than plants located at other less populated sites. The plant owners disagreed. To support their point, the plant owners independently sponsored full-scope PRAs of their plants. These studies attempted to show that, when plant-specific features were considered in addition to site features, the Zion and Indian Point plants did not present a disproportionate amount of risk.

The utility-sponsored studies were comprehensive and innovative, including an unprecedented analysis of external events that significantly advanced the state of the art. NRC took over 18 months to review each study, both of which have become focal points for discussions concerning the risk of these plants and have prompted safety improvements that may not otherwise have been made.¹

The owner of Big Rock Point plant used PRA to address post-Three Mile Island requirements

The owner of the Big Rock Point plant, located near Charlevoix, Michigan, voluntarily performed a full-scope PRA to support its position that some regulatory requirements imposed by NRC since the Three Mile Island accident were not warranted at the plant. The utility also used the PRA to address other outstanding issues related to that plant's safety.

¹As noted in chapter 1, we discussed the Indian Point PRA in our report, Response to Specific Questions on the Indian Point Probabilistic Safety Study (GAO/RCED-83-158, May 24, 1983). We found that while the Indian Point PRA may represent the state of the art in risk assessment, it suffers from the same limitations as all PRAs (uncertainties in data, models, assumptions, and methods), which are discussed in chapter 2 of this report.

Big Rock Point is a relatively small plant and is located in a sparsely populated area of northern Michigan. The plant owner contended that because it may pose a relatively low overall risk to public health and to property, some NRC requirements would not be cost-beneficial because they would result in relatively low reductions in risk.

The plant owner used the PRA to focus attention on the greatest contributors to risk and to support its proposals for alternative, less expensive plant modifications. NRC reviewed the utility's PRA, performed its own assessment of some of the issues, and presented its assessment and recommendations in a document entitled Integrated Plant Safety Assessment. The safety assessment report, however, indicated that the licensee successfully defended its position against many changes to procedures and hardware. Approximately one-half of the total issues discussed in this assessment were reviewed using PRA.

It is difficult to determine how much impact the PRA had on NRC's tentative decisions on what plant modifications would be required. For example, the accident at Three Mile Island prompted a requirement, applicable at Big Rock Point, to install special instrumentation in the control room to alert plant operators when the reactor core is not being adequately cooled. NRC's review of the major accident sequences identified in the Big Rock Point PRA indicated that this addition would have an insignificant impact on core-melt probability at that point because existing instrumentation already provides information on the adequacy of core cooling, and additional instruments would add little benefit.

The NRC staff recommended that the plant owner not be required to install the additional instrumentation but also recommended that the plant owner study ways to improve the reliability of core-cooling systems.

Limited-scope PRAs analyze proposed license amendments

In addition to full-scope plant-specific studies, NRC has considered very limited-scope PRAs as partial justification for license amendment requests. These requests involve changes to technical specifications that are sometimes decided by NRC in a matter of hours or days. PRAs are not required to support these requests and are usually not done. Further, when limited PRAs are considered, they may or may not affect NRC's decisions.

For example, Duke Power Company requested a license amendment that would allow continued operation of one of its plants for 2 weeks despite a safety valve problem. The utility planned to shut down the plant to replace the valves but preferred to wait until another plant being repaired was back in operation. To convince NRC that the risk was acceptable, the utility prepared a package addressing the safety implications of continued operation, the

need for electric power from the plant, and a limited-scope PRA of the situation.

The PRA supported the licensee's argument that the probability was low that the valves would be used during the few weeks in question and that the valves could withstand the maximum pressure to which they would likely be subjected if they were used.

Although the request was granted, NRC staff involved in the decision said that the PRA had no real effect on the decision. The deciding factor, they said, was that the valves could withstand the potential pressure. This was supported by considerable documentation on valve pressure limits that was available to NRC independent of the PRA.

In another case, NRC performed a limited PRA that added support to a decision concerning a license amendment at a plant owned by Alabama Power Company. The analysis involved the capability of the plant to safely shut down if one of its diesel generators was out of operation. Although a deterministic review of the plant design indicated that the remaining diesel generators would be sufficient for safe shutdown, the PRA added the following support:

- An analysis of the ability of the diesel generators to supply power to required equipment under various accident conditions confirmed that the generators could indeed perform as plant designs indicated.
- A review of off-site power reliability indicated that power outages were not unusually frequent in that area of the country. If such power outages were more frequent than suspected, greater demands could be put on the diesel generators, increasing the importance of redundant generators.
- A review of the history of the specific diesel generators at the plant assured analysts that the generators were as reliable as diesel generators at other plants.

NRC has used PRA to help determine
the relative importance of safety
issues at older plants

PRAs have provided "risk perspectives" on a predetermined set of issues related to the safety of 10 plants licensed prior to 1975 as part of NRC's Systematic Evaluation Program. These limited PRAs have been useful to NRC in assessing the relative importance of the safety issues at each plant and the relative benefits of proposed plant modifications.

NRC initiated the program in 1977 to examine how older plants deviated from current licensing requirements and how this deviation affected the safety of these plants. The program was a change from the NRC staff's usual practice because it integrated

NRC's review of a group of issues at each plant and looked at the proposed plant modifications as a package, rather than individually. Between 31 and 44 of the roughly 90 issues examined at each plant were found to deviate from current licensing criteria. Of these, about one-half were evaluated using PRA.

NRC staff used the limited PRAs performed in the Systematic Evaluation Program to supplement their engineering judgments of each plant in determining each issue's relative importance to risk and comparing the plant design to proposed modifications. Issues were generally ranked as having a high, medium, or low importance to risk on the basis of the effect their resolution would have on the most important accident sequences identified in the limited PRA of each plant. The significance of a proposed modification was assessed by incorporating the change into the plant models and recalculating the probability of system failure. The revised failure probability was then compared with the original failure probability to determine the effect of the proposed improvement.

Plant-specific PRAs were not available for 7 of the 10 plants reviewed in the Systematic Evaluation Program; thus, analyses of these plants were based on existing PRAs of similar plants. In some cases, a single PRA of a similar plant served as a surrogate. In other cases, it was necessary to draw on several PRAs because no existing study of a plant was sufficiently similar to the one under examination.

According to NRC staff involved in the Systematic Evaluation Program, as well as reviewers of the studies, the use of surrogate PRAs provided useful indications of each issue's relative importance to risk. The analyses did not, however, assess the overall risk of each plant in an absolute sense or relative to other power plants.

Plant-specific PRAs of varying scope were available for 3 of the 10 plants reviewed in the Systematic Evaluation Program. Analyses based on plant-specific PRAs generally provided more quantitative results than analyses based on surrogate PRAs. This occurred because plant models, probability calculations, and identification of the most important accident sequences in plant-specific PRAs provided reviewers with more detailed and reliable information on which to base their analyses of many of the issues examined. Use of plant-specific PRAs provided a more precise ranking of the importance of each issue examined and a more precise estimate of the potential risk reduction of proposed modifications. The availability of a plant-specific PRA for three plants, however, did not alter the outcome of the probabilistic analyses in the final Systematic Evaluation Program assessments of these plants.

Evaluation of a much broader range of issues at the Big Rock Point plant was assisted by the existence of a full-scope PRA of that plant, which the utility performed. At the utility's

request, NRC combined its examination of Systematic Evaluation Program issues and other outstanding issues related to the plant and evaluated modifications proposed by the utility. The PRA allowed analysts to quantitatively estimate the risk reduction that could result from the resolution of each issue.

For example, one of the Systematic Evaluation Program issues examined was the ability of the containment to prevent radioactive materials from escaping to the atmosphere in case of an accident. Preventing radioactive releases depends on the performance of a number of safety valves that would close steam and water lines and seal the containment, if necessary. Although the Big Rock Point plant has some of these safety valves, current regulations require additional redundant valves. In an analysis of the need for one particular valve, the licensee's PRA indicated that adding the valve would reduce risk by 33.8 person-rems² per year of reactor operation and cost about \$150,000. Additional analysis by the licensee indicated that instituting a testing program instead of installing the additional valve would reduce risk by 20.2 person-rems per year of reactor operation at a cost of \$4,000.

The NRC staff reviewed this analysis and concluded that the cost of adding a second valve was not warranted and that the testing program, with additional stipulations, was acceptable.

PRA IS USED AS AN AID IN RANKING GENERIC ISSUES

In the late 1960's, what was then the Atomic Energy Commission began identifying potentially significant issues, called generic issues, affecting all or a number of nuclear power plants. As of November 1983, NRC had identified a total of 482 generic issues. NRC has begun to use PRA to assist in identifying those issues with a high potential for reducing risk and in removing from consideration issues that have little safety significance.³

To rank generic issues, NRC makes a quantitative estimate of the safety importance of each issue. The estimate is measured in terms of risk and the decrease in the risk that may be attained by resolving the issue. NRC then makes a quantitative estimate of

²Person-rems are the sum of the individual exposure received by each member of a certain group or population. It is calculated by multiplying the average exposure per person by the number of persons within a geographic area. Consequently, the collective exposure is expressed in person-rems.

³Only 123 of the 482 generic issues were ranked under this PRA-based system because many issues were already resolved or near resolution, some were already known to be important, and others had been incorporated into other issues.

the cost of resolution. A numerical cost/benefit score is calculated denoting an estimated ratio of safety improvement to cost impact. The cost/benefit analyses are used only to provide generic indications of relative risk. Finally, the issues are placed into broad categories, ranging from those having high risk significance to those not directly relevant to risk, on the basis of a combination of their contribution to risk, potential to reduce risk, cost of reducing the risk, and engineering and management judgment. This is done to prioritize issues for resolution and to aid in the allocation of agency resources.

We recently completed a review of NRC's program to address and resolve generic safety issues.⁴ We found that NRC's PRA-based issue ranking system, while not entirely free of problems, represents a significant improvement over earlier ranking systems.

NRC HAS USED PRA TO EXAMINE GENERIC ISSUES

Many regulatory actions involve decisionmaking that affects all plants or large classes of plants. NRC has effectively used PRA to study various generic issues and act as the technical basis for resolving the issues in rulemaking proceedings. Generally, no specific PRA requirements will result from these proceedings. The following summarizes how NRC and the nuclear industry used PRA to review several major generic safety issues.

Anticipated transients without SCRAM

An anticipated transient without SCRAM is a failure of a safety and control system to automatically shut down the reactor (SCRAM) following an expected abnormal condition (i.e., a loss of off-site power to the reactor or the loss of water supply). These conditions are expected to happen at least once during the plant's lifetime and are a cause of concern because they could lead to severe core damage and release of radioactivity into the environment. Historically, the utility industry and NRC has used PRA to study anticipated transients without SCRAM to identify ways to reduce their occurrence.

An NRC investigation published in 1978 highlighted the relative likelihood of severe anticipated transient without SCRAM events for different reactor types and estimated the reduction of likelihoods for different proposed plant modifications. NRC subsequently used PRA to determine the predicted probability of failure of the reactor protection systems and the expected frequency of anticipated transient without SCRAM events. The review was

⁴Management Weaknesses Affect Nuclear Regulatory Commission
Efforts to Address Safety Issues Common to Nuclear Power Plants
(GAO/RCED-84-149, Sept. 19, 1984).

Based on 16 reliability studies of reactor protection systems done as part of prior PRAs. The review led to an NRC staff proposal intended to reduce the risk of such accidents. A consortium of utilities also sponsored a study that quantified the relative improvement to be gained by implementing a set of design modifications proposed by the consortium. The NRC final draft rule on this generic issue prescribes installing equipment keyed to specific reactor types and manufacturers.

Pressurized thermal shock

Pressurized thermal shock is characterized by severe overcooling of a nuclear reactor vessel and an increase in pressure. If a small crack is present on the vessel's inner surface during these events, the crack could grow to a size that might threaten vessel strength. NRC used PRA in developing the technical basis for this unresolved safety issue.

Specifically, NRC used PRA and deterministic methods to derive screening criteria used to measure the susceptibility of reactor vessel materials to break at certain temperatures. In short, the NRC staff used PRA techniques to gain insights into the frequency of pressurized thermal shock events and the sensitivity of temperature calculations that were developed deterministically. In addition, a national laboratory is performing PRA-type analyses for NRC on three prototype plants for the pressurized thermal shock rulemaking. These analyses will act as guidance for licensees as to how they may perform safety analyses on their plants if the plants do not meet the screening criteria.

The rulemaking would require licensees to determine and submit to NRC their present and projected temperature resistance values. If the licensees project these values to exceed the criteria, they must prepare PRAs of their plants to determine the significance of this problem to plant safety.

Station blackout

Current regulations require nuclear power plants to be designed to withstand the total loss of electrical power (i.e., station blackout), but they do not specify the time period that power can be off. Because many plant safety systems are dependent on electrical power, the consequence of a prolonged station blackout could be a severe core-damage accident. NRC used PRA in attempting to resolve the issue of whether plants were adequately protected against station blackout.

The NRC staff prepared a PRA to provide a preliminary evaluation of station blackout accident sequences. The study showed that no operating nuclear power plant had an unusually high susceptibility to station blackout events and subsequent core damage.

As part of the plan to resolve the issue, NRC contracted with DOE's Oak Ridge and Sandia National Laboratories to perform studies on the loss of off-site power, emergency alternating power systems, and station blackout events. The Oak Ridge National Laboratory study estimated the station blackout frequencies in 18 nuclear power plants and 10 generic plant designs. The study also identified design and operational features that are the most important to on-site power system reliability. The Sandia National Laboratory study focused on the relative importance of risk stemming from station blackout events and plant design and operational features that would reduce risk from these events. These studies are being used to formulate NRC's strategy for resolving the station blackout issue.

Although the NRC used PRA techniques in studying the station blackout issue, it will not require licensees to use PRA in complying with any new requirements on station blackout. Final resolution of the issue, currently in the rulemaking process, is expected in 1985.

Auxiliary feedwater systems

A PRA study of systems designed to cool down nuclear power plants under accident conditions (i.e., auxiliary feedwater systems) showed that these systems can comply with NRC regulations but be inadequate from a risk perspective.

Following the accident at Three Mile Island, NRC sponsored a quantitative study of the reliability of auxiliary feedwater systems of 25 nuclear reactors. One study finding was that the reliability of auxiliary feedwater systems that meet NRC regulations can vary by a factor of about 100. NRC decided that some systems had inadequate reliability. As a result, NRC (1) required changes to improve reliability, (2) placed a quantitative requirement for an additional water supply system in its review plans of operating nuclear power plants, and (3) made auxiliary feedwater studies a routine requirement for licensing. NRC's study demonstrated the value of PRA techniques applied at the systems level and led to changes in the safety review process.

NRC IS USING PRA AS A BASIS FOR COST/BENEFIT ANALYSES

PRA allows analysts to quantify the potential risk reduction (averted risk) that may result from a regulatory action and compare this benefit with the benefits of alternative actions and the costs of these actions. Quantified estimates of the averted risk are based on "bottom-line" PRA results and contain all of the uncertainties inherent in those results. In addition, NRC sometimes assigns arbitrary dollar values to these risk aversion estimates that increase their uncertainty. Despite the uncertainties, however, NRC officials say that risk aversion analyses provide useful additional information to decisionmakers.

NRC is placing more emphasis on quantified cost/benefit analysis as the centerpiece of regulatory analysis and has issued guidelines to

"ensure that the NRC regulatory decisions are based on adequate information concerning the need for and consequences of a proposed regulatory action and to ensure that cost effective regulatory actions, consistent with providing the necessary protection of the public health and safety and common defense and security, are identified."

NRC policy has always called for consideration of the costs and benefits of regulatory actions. However, in the past, these considerations have been largely qualitative and often inconsistent. PRA has provided analysts with a tool for quantifying averted risk in a more objective manner.

NRC has considered cost/benefit analyses mainly in decisions related to the ranking and resolution of generic issues as previously discussed on page 57. However, absolute risk aversion savings have also been considered in decisions related to individual plant modifications. In addition, NRC submits cost/benefit analyses to the Office of Management and Budget when certain regulatory actions are proposed.

How PRA quantifies averted risks

Although averted risk can be quantified in a variety of ways, sometimes resulting in very different estimates, it is usually expressed in units of exposure to radiation that would be avoided by a particular action. Such estimates of risk reduction are sometimes also expressed as a dollar amount.

Risk to public health is determined by estimating the probability of important accident scenarios and multiplying this by the total public radiation dose that could result from these accidents. Public dose is expressed in person-rem and, as specified in NRC guidance, calculated for a 50-mile radius around the plant.

Averted risk is determined by calculating the estimated reduction in risk per year that would result from a given action and multiplying this by the remaining life of the plant or plants involved. For example, the risk from an accident estimated to occur once every 10,000 years that was estimated to result in public exposure of 1 million person-rem could be converted to a per-year basis as 100 person-rem per year ($1/10,000$ years \times 1,000,000 person-rem). Actions that would prevent this accident would avert risk of 100 person-rem per year for every year that the plant was in operation. If the plant had a remaining life of 15 years, then the total risk averted would be 1,500 person-rem of exposure (15 years \times 100 person-rem).

Cost/benefit analyses are sensitive to many elements

Cost/benefit analyses are subject to other uncertainties besides the inherent uncertainty of the PRA results on which they are based. For this reason, NRC guidance advises that it is often appropriate to present alternative measures of risk to test the sensitivity of the results to various elements of the analyses. For example, how risk is measured, what costs and benefits are included, and/or how risk is converted to a dollar value can have an impact on cost/benefit analysis results.

The measure chosen to estimate risk may emphasize off-site risk but ignore on-site risk. For example, when risk is exclusively measured by potential person-rem of exposure, on-site property risks that result in little or no release of radiation off-site are not considered. Current NRC guidance calls for on-site cost to be presented separately.

The determination of what accident costs to include in cost/benefit analysis can significantly affect the results. According to NRC guidance, identifying all appropriate cost components--such as replacement power, cleanup, and property damage--is more important than precision in estimating these costs.

The method of converting risk to dollars and accounting for the future value of money can affect the results of cost/benefit analyses. Further, the appropriate dollar value of human life and health affects is potentially controversial. NRC's proposed safety goals for nuclear power plants, discussed in detail in chapter 5, specify that public exposure to radiation be assigned a dollar value of \$1,000 per person-rem. However, NRC has used other health-effects cost estimates that significantly deviated from this rate. For example, NRC has presented and sometimes compared three different values for a latent cancer fatality in testimony and documents. They are

--\$10 million, when the \$1,000 per-person-rem criteria are used;

--\$1 million, on the basis of a recommendation from the ACRS; and

--\$100,000, on the basis of the NRC report entitled Estimates of the Financial Consequences of Nuclear Power Reactor Accidents.

The choice of a discount rate, which is used to estimate the present value of future costs and benefits, affects estimates of future costs. At NRC, a 10-percent rate is prescribed, but the sensitivity of the results to this rate is disclosed by also presenting alternative rates.

For example, NRC presented dollar-value estimates of the risk posed by the Indian Point 2 plant both before and after proposed plant modifications in testimony concerning the safety of those plants. Because the health effects and property damage that would result from an accident are uncertain, and the appropriate dollar value of these effects is potentially controversial, the following three estimates were presented.

Dollar Value of Risk Per Year
for Early Fatalities at Indian Point 2

	<u>Expected loss in dollars</u>		
	<u>Low</u>	<u>Medium</u>	<u>High</u>
Before plant modifications	\$21,000	\$70,000	\$350,000
After plant modifications	4,440	14,800	74,000

These figures can be netted to show that the risk aversion savings (i.e., the dollar value of the lives saved) resulting from the fixes at Indian Point 2 are between \$16,560 and \$276,000.

NRC officials said that high-quality, quantitative cost/benefit analyses generally provide more information for decision-makers than such analyses that are mainly qualitative. This is because such analyses tend to

- more carefully and thoroughly explore the subtleties of the issues under examination,
- alert decisionmakers to the magnitude of the risks and costs involved in a particular decision, and
- highlight inconsistencies among analyses performed by different people.

CONCLUSIONS

NRC uses PRA as a supplement to conventional evaluation techniques to enhance safety and make regulatory processes more consistent and rational. Further, PRA forces the decisionmaker to explicitly consider and display areas of uncertainty more than is required with deterministic analyses. Finally, PRA results in a more complete understanding of risk-important systems and functions, interactions among systems, and the importance of human actions.

NRC's use of PRAs has been timely and reasonable in light of the evolving nature of PRA methodology and the lack of PRAs of new plants prior to 1983. For example, the NRC staff used PRA to prepare severe accident risk assessments for inclusion in environmental statements for new plants. Because few PRAs had been completed when the NRC Commissioners adopted this policy in 1980,

the NRC staff used available generic PRA results as a basis for plant-specific consequence analyses. Using generic PRA results avoided the delay and expense that would have been necessary if NRC had requested plant-specific studies for the plants under examination. NRC's intention to use plant-specific PRAs as they become available is appropriate since plant-specific PRAs of good quality would be more reliable.

The availability of an increasing number of plant-specific PRAs, however, is not a certainty. NRC requires future construction permit applicants to perform PRAs, but no applications have been submitted since 1978, and none are expected in the near future. NRC officials say that PRAs are in progress for two or three plants that already have construction permits, but this is a small fraction of the approximately 50 new plants with construction permits. NRC does not require owners of these plants to perform PRAs. Also, since utilities are not required to submit self-initiated studies to NRC, those that do perform PRAs may not submit them to NRC, which would lose a valuable source of information on plant operations and safety.

PRA has already provided valuable insights and an orderly means of analyzing the safety of operating plants. However, PRA could be potentially of even greater value as a tool for regulatory analysis as the methodology matures and as the use and understanding of it grows.

NRC's use of PRA in its analysis of individual issues in the Systematic Evaluation Program demonstrates how PRA can be successfully used in analyzing the safety of operating plants. In addition, applying PRA to analyses of utility requests for license amendments has shown that limited PRAs, which are much less costly and time-consuming than more broadly scoped PRAs, can be useful in this aspect of regulatory decisionmaking. In both cases, NRC used PRA to enhance its understanding of the reliability and workings of plant systems. Although risk-reduction figures were sometimes calculated, they appear to have been used only to determine the relative importance of various issues.

Further, NRC has effectively used PRA in analyzing risk-significant systems, regulations, and generic issues. Generally, NRC has recognized PRA limitations and imprecise quantitative results and has used PRA as a supplemental tool in ranking and examining generic issues. For example, to assist in resource allocation decisionmaking, NRC used PRA as an aid in placing generic issues into broad categories reflecting their relative importance to risk. This use of PRA is appropriate because precise PRA results are not necessarily required. In addition, NRC used PRA to examine generic issues and provide information for rulemaking. Generally, no specific PRA requirements will result from these actions.

The one exception to NRC's appropriate use of PRA is in the area of cost/benefit analysis. NRC states that it is using PRA to increase the objectivity and thoroughness of cost/benefit analyses. However, estimates of benefits--potential risk reduction--are based on "bottom-line" PRA results, which are the most uncertain aspect of PRA. Further, converting the potential risk reduction of alternative actions to dollar values increases the uncertainty of cost/benefit analyses and provides little additional information to decisionmakers. The appropriate dollar valuation of risk is controversial and inconsistent--and likely to remain controversial even if NRC establishes a uniform cost-conversion factor as proposed in its draft safety goals. The major benefit of quantified cost/benefit analysis is the indication of relative risk, and this can be determined without assigning dollar amounts to risk calculations.

Because of the added uncertainty and controversy associated with assigning dollar values to potential risk reduction alternatives, this procedure appears to be of little use in determining what can be spent to achieve a particular risk-reduction benefit. Therefore, caution is warranted in the use and presentation of dollar value estimates of risk aversion savings in cost/benefit analyses because it adds an additional level of uncertainty to the risk assessment and focuses on the "bottom-line" of the analysis--the most uncertain and least useful aspect of PRA. The principal benefit of quantified cost/benefit analyses--determining relative risk of alternative actions--can be realized without assigning dollar values to risk calculation.

In summary, with the exception of PRA use in cost/benefit analysis, NRC's use of PRA has been timely and reasonable given its developing nature. Further, use of PRA has led to safety and operational improvements at nuclear plants that otherwise would not have been made.

CHAPTER 5

NRC'S USE OF PRA IS LIKELY TO INCREASE

Largely as the result of recommendations to NRC by groups that investigated the March 1979 accident at the Three Mile Island plant, NRC is considering several programs and regulations which, if effected, will expand the use of PRA in nuclear power regulation. They include

- development of safety goals for nuclear power plants,
- an integrated assessment of Three Mile Island-related and other generic safety issues at selected plants,
- a reliability assurance program at each operating plant, and
- consideration of potential accidents more severe than the design-basis accident for each plant.

Although it is not clear to what extent PRA will be used in implementation of these programs, NRC officials told us that PRA will be used only to supplement NRC's current deterministic decisionmaking process. The proposed safety goals, however, may encourage the inappropriate use of unreliable PRA results by comparing the results to safety-goal design objectives to determine whether nuclear power plants meet the goals or require corrective actions. This could occur unless NRC's Commissioners clearly establish that NRC and industry are not to use the goals as standards for minimum compliance.

SAFETY GOALS MAY ENCOURAGE BOTTOM-LINE PRA USE

In 1979, the President's Commission on the Accident at Three Mile Island recommended that NRC establish and explain safety/cost trade-offs as part of its primary mission in ensuring the safety of nuclear power reactors. In its response to the President's Commission, NRC stated that it was moving forward with an explicit policy statement on safety philosophy and the role of safety/cost trade-offs in its decisions. To that end, in March 1983, NRC issued a Policy Statement on Safety Goals for the Operation of Nuclear Power Plants.

NRC's objective is to establish safety goals that limit to an acceptable level the radiological risk to the public from nuclear power plant operations. NRC officials say safety goals could lead to more coherent and consistent regulation of nuclear power plants, a more predictable regulatory process, a public understanding of the regulatory criteria that NRC applies, and public confidence in the safety of operating plants.

The policy statement contained two proposed qualitative safety goals supported by four proposed quantitative design objectives. The first safety goal is that nuclear power plant operations should not be a significant contributor to a person's risk of accidental death or injury. The intent is to require a level of safety such that individuals living or working near nuclear power plants should be able to go about their daily lives without special concern.

The safety goal policy statement says that although protection of individuals inherently provides a substantial protection to society, a limit should also be placed on societal risks. Thus, the second qualitative safety goal states that societal risks to life and health from nuclear power plant operations should be comparable to or less than the risks of generating electricity by competing technologies and should not be a significant addition to other societal risks.

As used in the policy statement, design objectives are "aiming points" for public risk reduction, which nuclear power plant designers and operators should meet, where feasible. Since they are not firm requirements, there may be instances in which a nuclear power plant may not achieve all of the objectives. NRC adopted the following design objectives:

- The risk of prompt fatality to an average individual in the vicinity of a nuclear power plant should not exceed one-tenth of 1 percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the population are generally exposed.
- The risk of cancer fatalities to the area population from nuclear power plant operations should not exceed one-tenth of 1 percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.
- The benefit of an incremental reduction of societal mortality risks should be compared with the associated costs on the basis of \$1,000 per person-rem averted.
- The likelihood of a nuclear reactor accident that results in a large-scale core-melt should normally be less than 1 in 10,000 per year of reactor operation.

The policy statement established a 2-year period, ending in early 1985, to (1) evaluate the practicality of the goals and objectives and (2) identify specific instances in which applying the safety goals would lead to different regulatory decisions. To do this, the safety goals will be compared to present deterministic criteria that will continue to be used in regulatory decisions. PRA techniques will be used to evaluate the quantitative design objectives against specific generic issues (e.g., anticipated transients without SCRAM and pressurized thermal shock).

Although the generic issues will be evaluated against the safety goals, the purpose is to gain experience using PRA, not to use safety goals in the decision process to resolve the specific issues. Until the evaluation period is complete, NRC is not in a position to propose how to use safety goals.

Safety goals point to the
"bottom-line"

Reactions to the safety goals have ranged from praise and endorsement to vigorous rejection. Many electric utilities say that the safety goals can lead to a more coherent and consistent regulatory process. However, other commentators, such as the ACRS and the Union of Concerned Scientists, foresee problems in using PRA to define safety aspects of nuclear power plants. Some commentators are concerned that the safety goals will lead to the use of the "bottom-line" (numerical) results of PRAs despite their limitations. For example, there is concern that too much attention will be placed on comparing the calculated likelihood of a large-scale core-melt accident at a specific plant with the design objective of 1 in 10,000 per year of reactor operation.

Such comparison can be misleading due to the large uncertainties in PRA results. For example, a table prepared by NRC staff compares results from existing PRAs. The table shows that two plants have the same core-melt frequency of 1 in 2,500 per year, a frequency higher than the safety goal design objective of 1 in 10,000 per year. However, text that accompanies the table states

". . . the numbers in the table have large uncertainty bounds associated with them. In general, these uncertainty bounds should extend on the order of plus or minus a factor of ten about the values presented."

If uncertainty bounds of plus and minus a factor of 10 are applied to the previously mentioned core-melt frequency, the result is a range between once in every 250 years and once in every 25,000 years. This means that although the two plants have the same single point estimates for frequency of core melt, these estimates are uncertain, and the actual frequency could fall anywhere within the range between the uncertainty bounds. If the actual core-melt frequencies for the two plants fall at opposite ends of the range, the frequency at one plant could be once in every 250 years, while the frequency at the other plant could be once in every 25,000 years, or 100 times less frequent. Under such circumstances, it is difficult to determine which, if either, plant would meet the safety goal or whether the plants require possibly extensive and costly changes to meet the safety goal.

A then-NRC Commissioner, who did not support the policy statement, also expressed concern about the reliance on PRA "bottom-line" results as follows:

". . . the Commission appears to be headed toward an over-reliance, in its regulatory decisions, on estimates of the overall nuclear power plant risks which are based on uncertain and unreliable calculational techniques. These techniques cannot bear the weight the Commission intends them to support."

The Acting Director of the Division of Risk Analysis told us that the basic strengths of PRA are the insights gained as to the type and nature of the most important accident and risk sequences. He also said that the use of PRA in regulation often focuses on the magnitude of the bottom-line numbers, which is PRA's weakest element. It is his opinion that avoiding the bottom-line numbers would be difficult given the safety goal's structure. He told us that the substantial insights to be drawn from PRA with regard to accident sequences, system reliability, and human performance will be downgraded or even lost if analysts focus on bottom-line results.

In a September 1982 letter to the NRC Chairman, two members of the ACRS wrote that there "is no way in which the currently proposed safety goal policy will serve any useful public safety purpose as long as its main assessment basis is PRA." They noted several methodology limitations that do not allow current PRA studies to be properly scrutinized. They said that the most serious of these limitations is the claim that PRA can estimate core-melt probability.

A Union of Concerned Scientists representative said that the principal limitation of PRA is its quantitative results, which are almost always of a bottom-line or comparative nature. According to him, the safety goals represent the epitome of the bottom-line use of PRA. In his opinion, the quantitative results are so uncertain as to be essentially useless in a regulatory setting. He added that even the qualitative goals cannot be shown to be met without quantitative analysis.

Some commentators on the core-melt design objective said that it is not practical because of the difficulties in performing and using PRAs. For example, an attorney representing a public interest group wrote that the core-melt objective rests implicitly on a claimed ability to make reliable absolute probability calculations and that this ability has not been demonstrated to exist.

PROPOSED INTEGRATED ASSESSMENT OF SAFETY ISSUES COULD REQUIRE PLANT-SPECIFIC PRAS

The NRC staff is considering combining individual plant evaluations related to the Systematic Evaluation Program, issues raised by the Three Mile Island accident, and other generic safety issues into one integrated assessment of plant performance. An important part of this program would be a requirement for a

plant-specific PRA for each plant evaluated that would include considering severe accident risks and identifying individual plant vulnerabilities.

The proposal, entitled the Integrated Safety Assessment Program, calls for selected licensees to perform level-one PRAs (i.e., plant systems analyses) in accordance with procedures laid out by NRC. NRC would then perform the final two segments, the containment and consequences analyses, on the basis of the licensee's plant systems analysis. In the future, as PRA methods develop and become more stable, performance of additional segments could be required of the licensee. The Integrated Safety Assessment Program would not require compliance with a prescribed safety goal or standard.

NRC officials said that the program will be conducted on a trial basis and that they are not likely to begin requiring licensees to perform PRAs against their will. The first groups of plants evaluated would probably be those for which a plant-specific plant systems analysis exists. In addition, NRC officials told us that some licensees had volunteered to participate. This program has been deferred until fiscal year 1987 due to budget constraints.

PRA MAY BE USED QUALITATIVELY FOR RELIABILITY ASSURANCE

Reliability assurance programs at nuclear power plants would attempt to systematically and continually identify circumstances and situations that would make the plants less safe than originally believed. NRC does not require this type of research program. However, NRC is planning a program that would attempt to maintain an acceptable level of safety over the lifetime of a plant through the use of reliability assurance. Although PRA's role in the research program has not been fully defined, the NRC program manager stated that it is likely to be used as an aid to qualitative decisionmaking.

Following the accident at Three Mile Island, NRC began to evaluate whether it could apply reliability engineering techniques to nuclear power. The 1980 NRC Action Plan Developed as a Result of the TMI-2 Accident noted that reliability engineering techniques can complement quality assurance and provide a disciplined approach to systems engineering in the design of nuclear power plants. The plan called for the Office of Nuclear Reactor Regulation to "apply reliability engineering practices to nuclear plant activities on a comprehensive and consistent basis."

Subsequently, the need to make nuclear power plants safer through reliability assurance has been reiterated by several other sources, including

--the Indian Point Atomic Safety and Licensing Board, which recommended that NRC require licensees to develop and

implement a safety assurance program embodying 10 reliability elements;

--the Policy Statement on Safety Goals for the Operation of Nuclear Power Plants, which states that NRC will begin developing reliability assurance program criteria and risk-based reliability criteria for those systems and components most important to safety; and

--NRC's statement in a proposed rule urging utilities to voluntarily develop reliability assurance programs for reactor trip systems.

NRC's Office of Nuclear Regulatory Research has developed a draft plan to evaluate the reliability assurance program elements used in other industries as well as those envisioned by the Three Mile Island action plan, the Indian Point Atomic Safety and Licensing Board, and the anticipated transient without SCRAM rule-making. Many of these elements are quantitative or risk-based and call for using PRA results to identify critical items.

NRC will then combine this information to develop elements that appear cost effective for power plant operations. Cost/benefit analysis will then be made to determine which reliability elements will give the greatest risk reduction potential when compared with the cost. A trial-use period at a nuclear power plant may follow after NRC identifies the most appropriate and cost-effective reliability elements. If the trial-use period is successful, the last phase of the program would be to set lowest acceptable failure standards.

The NRC reliability assurance program manager told us that it is not clear how large a role PRA will play in either the standards development or the type of analysis a utility will have to perform to comply with the reliability standards. He also noted that one of the purposes of the reliability assurance program is to use PRA insights and quantitative results for qualitative decisionmaking. PRA will be helpful in determining what factors are important to risk and to performing cost/benefit analyses.

PRA COULD SUPPLEMENT NRC'S SEVERE ACCIDENT DECISIONMAKING

Design basis accidents are a set of hypothetical accidents evaluated during the safety reviews of nuclear reactors. Nuclear power plants are required to have safeguards to ensure that off-site radiation releases will be within NRC limits should any of these accidents occur. The 1980 NRC Action Plan Developed as a Result of the TMI-2 Accident recommended that NRC and the nuclear industry consider accidents more severe than the design basis. NRC's Proposed Commission Policy Statement on Severe Accidents and Related Views on Nuclear Reactor Regulation, published in April 1983, provides NRC's views on the process for arriving at severe accident decisions for operating plants.

The proposed policy statement suggested a three-step process for arriving at severe accident decisions for existing plants:

- Quantitative risk assessments will be used to estimate the relative importance of potential nuclear power plant accident sequences for which insufficient data exist to make comparisons.
- A range of possible design and operational changes to improve accident prevention and consequence mitigation capabilities will be studied to determine the costs and safety benefits of backfitting them to plants in operation or under construction.
- Engineering and policy judgment, supplemented by PRA where appropriate, will be used to decide whether reductions in severe accident risk are necessary.

The ACRS criticized this approach as placing too much reliance on PRA. Accordingly, the NRC staff proposed a combined deterministic/probabilistic approach that places primary reliance on deterministic engineering analysis and assigns a role to PRA that the staff feels is consistent with the known strengths and weaknesses and technical state of the art. The staff noted that it is difficult to prescribe the weight to be given PRA in severe accident decisionmaking. However, PRA will be valuable in categorizing and arranging in order of significance the most important accident sequences and associated containment responses for internal events and in providing additional perspective on risk judgments.

NRC issued a final severe accident policy statement (NUREG-1070) for review in January 1984. As of August 1984, NRC was revising the policy statement to reflect the comments received. The final rulemaking on severe accidents is not anticipated until mid-1986.

CONCLUSIONS

NRC is likely to use PRA increasingly as one tool in supplementing its current deterministic regulatory decisionmaking process. Programs relating to safety goals, Three Mile Island and generic issues, reliability assurance, and severe accidents will expand PRA's role in decisionmaking, although it is at present uncertain what PRA's precise role will be. Use of PRAs in these programs is appropriate providing that decisions are not based exclusively on PRA results. The substantial limitations of PRA in terms of the uncertainties of the results provide strong arguments against such use for the foreseeable future.

A safety goal for nuclear power plant operations can add consistency and rationality to the regulatory process. The proposed PRA-based safety goals, however, should not be used as the primary

or sole criteria for related decisionmaking. Because PRA is a developing methodology, strict comparison of plant-specific PRA bottom-line results to numerical safety goals is not warranted at this time. Therefore, NRC's policy should continue to emphasize that safety goals and design objectives indicate a desired goal but are not to be used by nuclear power plant designers, plant owners, and the NRC staff as a compliance standard.

However, since full-scope PRAs performed by licensees have proven beneficial on the basis of the insights they provide on plant operations and potential risk contributors and are becoming more widespread, it may now be appropriate for NRC to formally incorporate such studies into its regulatory activities. A program such as the Integrated Safety Assessment Program, recently approved by NRC but not yet funded, would do this by using PRA to examine outstanding generic and Three Mile Island-related safety issues to identify individual plant systems and components that present the greatest risks and evaluate alternative corrective actions to identify the most appropriate actions. This use is consistent with most experts' opinions that PRA can be effectively used to determine the relative risk of individual plant systems and components and evaluate alternative actions. Further, the Integrated Safety Assessment Program would not require compliance with a prescribed safety goal or standard, which is a use of bottom-line risk estimates generally considered by PRA experts as unreliable and inappropriate given the state of the art of PRA.

The Integrated Safety Assessment Program also would give NRC some control over the way PRAs are done by licensees. As we will discuss in chapter 6, PRAs are not currently performed in accordance with any prescribed format or procedures. This has resulted in inconsistencies in scope and methodology among existing PRAs and has made their review a time-consuming and subjective process. Requirements as outlined in the Integrated Safety Assessment Program would set the scope and, to some extent, the methodology used, resulting in more comparable and easier to review PRAs.

CHAPTER 6

NRC IS ADDRESSING PROBLEMS THAT

HAVE HINDERED EFFICIENT REVIEW AND USE OF PRA

NRC's ability to efficiently review and use PRAs has been hindered by the limited availability of PRA expertise and by the lack of standardized procedures for performing and reviewing these studies. These limitations are diminishing due to increased staff experience and training and the development of procedures manuals for the performance and review of PRAs. Increased expertise has already improved NRC's ability to review the increasing number of voluntarily performed utility-sponsored PRAs that are taxing NRC's resources. Use of the new procedures manuals should further improve NRC's ability to review and use PRA results.

PRA REVIEWS TAX NRC'S RESOURCES

NRC reviews industry-sponsored PRAs to determine their quality and credibility. As of January 1984, NRC had reviewed four full-scope industry-sponsored PRAs. The studies cost about \$200,000 to \$600,000 to review and required from 9 to over 18 months to complete. Differences in format and how PRAs are done make NRC's reviews difficult and even more time-consuming. NRC must tailor its reviews to each study, investigating the assumptions, data, and methods used. As the Assistant Director of the Division of Safety Technology told us, NRC must deal with "custom-made PRAs" as well as "custom-built plants."

The scarcity of experienced PRA practitioners and reviewers has limited the number of PRAs that could be performed and reviewed at any one time. Between 1981 and 1983, NRC received more industry-sponsored PRAs than it had resources to review. In 1982, review of the Zion PRA was delayed so that resources could be concentrated on the Indian Point PRA and related hearings. Further, NRC had not yet begun its review of the Yankee Rowe PRA, which was submitted in the spring of 1983, as of the end of that year because the NRC staff was concentrating on PRA reviews of new plants undergoing licensing review.

NRC officials received two or three additional PRAs in 1984. However, submittals of industry-sponsored PRAs may not continue at the same rate in the future as they did between 1981 and 1983 because they are expensive to conduct and not required by NRC. Further, some utilities we contacted stated they had no plans to perform PRAs unless required to do so by NRC.

PRA EXPERTISE AVAILABLE TO NRC HAS IMPROVED

NRC's PRA expertise has grown substantially since the 1975 performance of the Reactor Safety Study. A concerted effort to

improve NRC's PRA expertise and to transfer this expertise to other offices within the agency began in 1980 when it became apparent that NRC would need improved capability to deal with the rapidly increasing use of PRA in the nuclear power industry. This effort included establishing a new branch in the Office of Nuclear Reactor Regulation to serve as the center of its PRA expertise and instituting a PRA training program.

NRC officials said these efforts have been successful as indicated by the following:

- NRC's goal of transferring PRA expertise from the Office of Research to the Office of Nuclear Reactor Regulation has been largely accomplished. The Office of Nuclear Reactor Regulation now has surpassed the Office of Research in practical PRA experience.
- Although PRA experts are centered in one division of NRC's Office of Nuclear Reactor Regulation, other divisions within the Office now have staff members who are knowledgeable users of PRA.
- The NRC staff's ability to review such studies has increased since 1982, mostly because of on-the-job experience.

NRC officials credit staff involvement in a wide variety of PRA-related activities as the main contributor to improved staff capability. Some staff members have been directly involved in the performance and review of PRAs, while others have become knowledgeable about PRA because of its usefulness as a tool for analysis of certain generic issues. These activities are discussed in chapter 4.

Since 1981, NRC has developed a comprehensive PRA training program. It consists of a series of courses designed to accommodate the needs of inexperienced staff as well as those with some PRA expertise. The first courses were offered in August 1982. By October 1983, approximately 100 staff members had completed one or more PRA courses. The Office of Nuclear Reactor Regulation, which is involved in most of the practical applications of PRA, provided approximately one-half of the participants.

Officials that we talked with are supportive of the training program and say that it complements practical experience in the use of PRA. In addition, the program provides an overview of the general uses of PRA for staff members, such as attorneys, who are not directly involved in detailed PRA work but need some understanding of its uses.

Although some courses have been modified for 1984 to better meet the needs of the staff, plans call for the program to continue without major modification through fiscal year 1985. In

fiscal year 1986, the program may be reduced to a level deemed adequate to maintain skills that have been developed.

In addition to its own staff expertise, NRC draws on the PRA expertise of contractors. Like NRC, the expertise of these contractors has grown as PRA use has increased. NRC has relied on DOE's national laboratories, especially Sandia, for large amounts of its PRA-related work. Contractors have been heavily involved in PRA research, the performance of NRC-sponsored PRAs, NRC's PRA training program, and detailed reviews of utility PRAs.

In late 1982, the Deputy Director of NRC's Division of Risk Analysis told us that NRC's staff and contractors who had some PRA expertise were overwhelmed with PRA review work. By late 1983, however, this official told us that the disparity between the availability of and the demand for PRA expertise had diminished and that it was no longer difficult for NRC to obtain contractor expertise.

Officials at NRC and Sandia told us that additional practical experience will improve the NRC staff's ability to manage contracted work. However, in some areas, mainly reviews of industry-sponsored PRAs, it is difficult for the NRC staff to get the experience it needs because NRC's contractors perform most of this work. In these areas, NRC staff efforts are restricted to conducting reviews of contractors' work and writing summaries and interpretations for use within NRC.

STANDARDIZATION OF SOME PERFORMANCE
AND REVIEW PROCEDURES MAY IMPROVE
NRC'S USE OF PRA

PRA is a rapidly evolving field without standardized procedures for performing PRA studies. Therefore, practitioners have relied on their own judgment in choices of methods, data, and assumptions. In addition, some have introduced innovative procedures and expanded the scope of their studies to include contributors to risk that were previously omitted. Although such innovations have contributed to the development of PRA methods, they have also increased the subjectivity of these studies and the time needed to review them.

No single, widely accepted methodology exists for performing a PRA of a nuclear power plant. The major reason for this is that the application of PRA to commercial nuclear power is still relatively new and is, therefore, still subject to controversy, innovation, testing, and further development. For example:

- Analysts disagree on what statistical methods are best.
- Methods are relatively new and unvalidated for external events analysis.

--Analysts' understanding of what happens during core-melt and what releases of radiation could result is changing rapidly.

Because PRA methodology is evolving, too much standardization too soon would stifle advances in the state of the art. Officials that we talked with have mentioned the following drawbacks to early standardization:

--Too much standardization could lock in current methods and stifle innovation.

--Prescribed data and models could lessen the ability of analysts to make each PRA as plant-specific as possible.

--Even when experts agree that an element of PRA should be standardized, they sometimes disagree on which of several alternatives should be designated as the best.

Because existing PRAs vary
in scope and methodology,
they are difficult to compare

Existing PRAs are so varied in scope and methodology that comparisons of their results are difficult. Of 20 major PRAs published as of December 1983:

--Eleven are level-three studies, which analyze accident sequences through core-melt, release of radiation, and adverse consequences to public health and the outside environment.

--Five are detailed level-one studies, which analyze accident sequences through core-melt only.

--Four are level-two analyses of limited depth, which analyze accident sequences and containment response through release of radiation but do not examine the consequences of these releases.

--Some include considerations of external events, while others do not.

In addition to these variations in scope, existing PRAs have also varied in methodology. Generally, the methods used in NRC-sponsored PRAs closely follow those that were used in the Reactor Safety Study, although the performances of some industry-sponsored PRAs have modified these methods and developed some new methods of their own. For example, the analysts who performed the Indian Point and Zion PRAs modified NRC's methods of event-tree and fault-tree analysis and used innovative methods for the development of component failure rates and for uncertainty analysis.

NRC is moving toward some standardization of PRA performance and review procedures

NRC officials are aware of the problems involved in attempting to standardize a developing methodology such as PRA. However, they told us that some standardization is needed if NRC is to efficiently review these studies and compare their results. Officials at Sandia National Laboratories also agreed that some standardization in format, generic data sources, and models would be appropriate to speed up reviews.

NRC has sponsored the development of three PRA procedures manuals. One was a joint effort by industry and NRC to catalog the various PRA methods, while the other two were developed as part of NRC programs.

The PRA Procedures Guide, published in 1983, was developed by the American Nuclear Society and the Institute of Electrical and Electronic Engineers under a grant by NRC. The guide, which includes discussions of all three segments of PRA analysis--plant systems, containment, and consequences--is a compilation of PRA procedures. It does not prescribe what methods are best.

The Interim Reliability Evaluation Program Procedures Guide documents procedures used during the NRC program of the same name. The guide covers only plant systems analysis, since studies performed as part of this program were limited to that aspect of PRA, but is more prescriptive than The PRA Procedures Guide.

NRC is developing another procedures guide that incorporates elements of the two guides described above for use in the Integrated Safety Assessment Program. This program will require some licensees to perform PRAs in accordance with the new guide. (This program is discussed in ch. 5.) Like the Interim Reliability Evaluation Program Procedures Guide, it covers only the performance of plant systems analyses. Procedures for considering external events are being included, and plans call for the guide to eventually cover containment analyses.

To provide guidance for reviewers of industry-sponsored PRAs, NRC developed a PRA audit manual and published it for public comment in September 1983. During 1984, NRC planned to revise the manual in response to comments received. The manual should

- provide, in conjunction with the new procedures guide, official standards against which a PRA can be measured;
- make PRA reviews less prone to individual judgments concerning what should be reviewed and in what detail; and
- alert the reviewer to search for problems and irregularities that have been found in other PRAs.

Like the procedures guides developed for NRC programs, the review manual covers only plant systems analysis. However, NRC plans to expand its scope in the near future to other segments of PRA, such as containment and consequence analysis. NRC has not established a time frame for expanding the scope of the review manual.

CONCLUSIONS

The PRA expertise of NRC and its contractors has increased with the increasing use of PRA by licensees. Since 1981, several licensees have performed innovative, full-scope PRAs of their own, and NRC's research efforts have been supplemented with a substantial amount of work involving the review and practical application of PRA and PRA results. During this period of about 3 years, 1981-83, NRC's Office of Nuclear Reactor Regulation, in conjunction with contractors, has completed reviews of four industry-sponsored PRAs and has used PRA in a wide variety of NRC's regulatory activities.

NRC has taken appropriate steps to develop its PRA expertise by instituting a comprehensive PRA training program offering a variety of courses to meet varying staff needs. This effort has provided staff from diverse offices an opportunity to learn about PRA, thus broadening the base of PRA understanding throughout NRC.

Additional practical experience would further increase the NRC staff's PRA expertise and, therefore, its ability to review industry-sponsored PRAs. However, it is difficult to see how this experience will be gained. Most of the plant-specific PRA work performed since 1981 and currently in progress is sponsored by utilities. The detailed review of this work has been, and is likely to continue to be, performed mainly by NRC's contractors. For these reasons, there are few opportunities for NRC staff to become involved in the details of performing and reviewing PRAs.

NRC's development of PRA procedures manuals could lead to more efficient and timely reviews of industry-sponsored PRAs. Further, NRC's development of a prescriptive procedures guide for the proposed Integrated Safety Assessment Program is a reasonable step toward making PRA results more comparable and easier to review. Such standardization will allow for more accurate determination of relative risk, which is often cited as one of the most useful aspects of PRA. Finally, NRC's PRA audit manual should improve the consistency and thoroughness of PRA reviews by providing useful guidelines for both NRC contractor and staff reviewers.

ORGANIZATIONS CONTACTED
BY GAO IN OUR PRA REVIEW

NUCLEAR REGULATORY COMMISSION

Advisory Committee on Reactor Safeguards (ACRS)
Executive Director for Operations
NRC Regions 1 (Philadelphia) and 2 (Atlanta)
Office of Analysis and Evaluation of Operational Data
Office of Inspector and Auditor
Office of Nuclear Reactor Regulation
Office of Nuclear Regulatory Research
Office of Policy Evaluation
Office of the Executive Legal Director

DEPARTMENT OF ENERGY

Office of Converter Reactor Deployment
Office of Nuclear Safety
Brookhaven National Laboratory
Oak Ridge National Laboratory
Sandia National Laboratory

NUCLEAR POWER PLANTS VISITED

Calvert Cliffs, Calvert County, MD
North Anna, Louisa County, VA

PUBLIC INTEREST GROUPS

Friends of the Earth
National Audubon Society
New York Public Interest Research Group
Union of Concerned Scientists

UTILITIES

Alabama Power Company
American Electric Power Service Corporation
Baltimore Gas and Electric
Boston Edison Company
Carolina Power & Light Company
Commonwealth Edison
Consolidated Edison Company of New York, Inc.
Consumers Power Company
Dairyland Power Cooperative
Duke Power Company
Duquesne Light Company
Florida Power Corporation
Georgia Power Company
Iowa Electric Light and Power Company

Louisiana Power and Light
Mississippi Power & Light Company
Nebraska Public Power District
New York Power Authority
Northeast Utilities
Omaha Public Power District
Pacific Gas and Electric Company
Philadelphia Electric Company
Portland General Electric Company
Public Service Company of Colorado
Rochester Gas and Electric Corporation
Southern California Edison Company
South Carolina Electric & Gas Company
Toledo Edison Company
Vermont Yankee Nuclear Power Corporation
Virginia Electric and Power Company
Yankee Atomic Electric Company

UTILITY SERVICE GROUPS

Atomic Industrial Forum, Inc.
Electric Power Research Institute
Institute of Nuclear Power Operations
NUS Corporation
Pickard, Lowe and Garrick, Inc.

CONFERENCES ATTENDED

American Nuclear Society 1982 Winter Meeting
Eleventh Water Reactor Safety Research Information Meeting

NRC- AND UTILITY-SPONSORED PRASNRC-SPONSORED PRAS

NRC sponsored four PRAs in its Reactor Safety Study Methodology Applications Program (RSSMAP). The objectives of these level-two studies (i.e., plant systems and containment analyses) were to apply the methods developed in the Reactor Safety Study to nuclear reactors and containment designs different from those examined in that study to determine the sensitivity of major accident sequences to plant design features. These were limited studies that did not include consequence analyses, risk estimates, or external event analyses.

In addition, five plant systems analyses studies were done as part of NRC's Interim Reliability Evaluation Program. Two objectives of the program were to identify accident sequences that were dominant contributors to core-melt probability and to expand the number of PRA practitioners. These Interim Reliability Evaluation Program studies were limited in scope; they estimated core-melt probabilities but they did not consider external events, their containment analyses were limited, and risk estimates were not included. The following table shows the major NRC-sponsored studies performed to date.

Major NRC PRA Studies

<u>Plant</u>	<u>Report issuance</u>	<u>Scope (level)</u>	<u>NRC program</u>
Surry 1	1975	3	RSS ^a
Peach Bottom 2	1975	3	RSS
Oconee 3	1981	2	RSSMAP ^b
Sequoyah 1	1981	2	RSSMAP
Grand Gulf 1	1981	2	RSSMAP
Calvert Cliffs 2	1981	2	RSSMAP
Crystal River 3	1982	1	IREP ^c
Browns Ferry 1	1982	1	IREP
Arkansas 1	1982	1	IREP
Millstone 1	1983	1	IREP
Calvert Cliffs 1	1983	1	IREP

^aRSS - Reactor Safety Study.

^bRSSMAP - Reactor Safety Study Methodology Applications Program.

^cIREP - Interim Reliability Evaluation Program.

UTILITY-SPONSORED PRAS

Nine utility-sponsored PRAs have been submitted to NRC for review, as of February 1984, and others are in progress. These studies are generally more comprehensive than NRC-sponsored studies, and their purposes vary widely. For example:

- Commonwealth Edison commissioned a level-three PRA, including an external events analysis, of its Zion reactors to use as the basis for requesting relief from certain regulatory requirements.
- Consolidated Edison Company of New York and the New York Power Authority commissioned a level-three study, including an external events analysis, to assess the safety of the two Indian Point plants.
- Philadelphia Electric Company and Northeast Utilities conducted level-three PRAs of the Limerick 1 and 2 and Millstone 3 reactors. NRC requested these studies because the plants are located near high population centers and their operation might represent a high level of risk to the public.
- The Yankee Atomic Electric Company (Yankee Rowe plant), the Long Island Lighting Company (Shoreham plant), and the Pennsylvania Power and Light Company (Susquehanna 1 plant) initiated level-three studies to determine the risk of the plants, to identify what plant characteristics were most important from a risk perspective, and to build their own PRA capabilities.

The following table shows the major industry-sponsored PRAs. All of these are level-three PRAs.

Major Industry PRA Studies

<u>Plant</u>	<u>Report issuance</u>	<u>Study sponsor</u>
Indian Point 2 & 3	1982	Consolidated Edison Company of New York, New York Power Authority
Zion 1 & 2	1981	Commonwealth Edison
Big Rock Point	1981	Consumers Power Company
Yankee Rowe	1982	Yankee Atomic Electric Company
Limerick 1 & 2	1983	Philadelphia Electric
Shoreham	1983	Long Island Lighting Company
Millstone 3	1983	Northeast Utilities
Susquehanna 1	1983	Pennsylvania Power Light Company
Oconee 3	1983	EPRI/NSAC ^a
Seabrook 1 & 2	1983	Public Service Company of New Hampshire
Midland 1 & 2	1984	Consumers Power Company
GESSAR (BWR) Standardized Design	1983	General Electric

^aEPRI/NSAC - Electric Power Research Institute/Nuclear Safety
Analysis Center.

NINETY-SEVENTH CONGRESS

ROOM H2-316
HOUSE OFFICE BUILDING ANNEX NO. 2
PHONE (202) 228-2424

RICHARD L. OTTINGER, N.Y., CHAIRMAN

ANTHONY TOBY MOFFETT, CONN.	CARLOS J. MOORHEAD, CALIF.
EDWARD J. MARREY, MASS.	MATTHEW J. RINALDO, N.J.
ALBERT BORE, JR., TENN.	JAMES M. COLLINS, TEX.
PHIL GRAMM, TEX.	TOM CONCORAN, ILL.
L. SWIFT, WASH.	BOB WHITTAKER, KANS.
JOEY LELAND, TEX.	THOMAS J. TAUKE, IOWA
HARD C. SHELBY, ALA.	DON RITTER, PA.
KE BYRNE, OKLA.	HAROLD ROGERS, KY.
ION WYDEN, OREG.	CLYDE BENEDICT, W. VA.
RALPH M. HALL, TEX.	JAMES T. BROTHILL, N.C.
BOUB WALKER, PA.	(EX OFFICIO)
CARDIS COLLINS, ILL.	
JOHN D. DINGELL, MICH.	
(EX OFFICIO)	

U.S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON ENERGY CONSERVATION
AND POWER
OF THE
COMMITTEE ON ENERGY AND COMMERCE
WASHINGTON, D.C. 20515

August 20, 1982

W. MICHAEL MCCABE
STAFF DIRECTOR

The Honorable Charles A. Bowsher
Controller
General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Bowsher:

In compliance with the recommendations of various organizations including the General Accounting Office, the Nuclear Regulatory Commission has been increasing its use of a risk evaluation methodology known as "probabilistic risk assessment," or PRA. The President's Commission on the Accident at Three Mile Island and the General Accounting Office among others have found that PRA may be a valuable tool to identify high probability accidents, determine the need to implement new design requirements on nuclear powerplants, and evaluate alternative approaches to resolve outstanding safety issues.

Using PRA techniques, it is apparently NRC's goal to evaluate each operating powerplant to determine its reliability and susceptibility to various types of reactor accidents. This process is to identify operating or design deficiencies which might have previously been ignored.

For this reason and considering the current state of development of this methodology and the relative inexperience of the NRC staff in using it, I am specifically concerned about the extent to which NRC will rely on PRA techniques in its licensing and safety evaluation programs.

In this context, NRC is evaluating a recent Probabilistic Risk Assessment of the Indian Point plants, prepared by Commonwealth Edison and the Power Authority of the State of New York for use in the safety reassessment hearings being conducted on Indian Point Units 2 and 3. As you are aware, these plants are in close proximity to New York City and pose possible catastrophic consequences in the event of a major nuclear accident. Can I and the people of New York State be assured that the NRC is properly applying PRA, in conjunction with other evaluation techniques, to determine whether Indian Point plants are safe to operate in close proximity to a major population area?

2

I request that GAO undertake a study of NRC's reliance on PRA techniques in its regulatory process with particular emphasis on the Indian Point safety reassessments. Specific questions are (1) What is the current state of the art regarding PRA? (2) To what extent has NRC incorporated PRA into the regulatory process and does this appear reasonable considering the staff's experience and training? (3) What are the problems and potential disadvantages associated with the use of PRA and has NRC adequately considered these? and (4) Are there any specific problems associated with the use of PRA in the reassessment of the Indian Point plants.

If possible, I would like the information relating to the Indian Point plants by the end of September. The remainder can be provided at a later date depending on agreements reached between your staff and mine. I would also like to be kept informed on your progress and request a meeting within a few weeks to discuss your review efforts. If you have any questions pertaining to this request, please contact Jeanine Hull at 226-2424.

Sincerely,


Richard L. Ottinger
Chairman

RLO:mb



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

APR 24 1985

Mr. J. Dexter Peach
Director, Resources, Community and Economic
Development Division
U.S. General Accounting Office
441 G. Street, N.W.
Washington, DC 20548

Dear Mr. Peach:

We appreciate the opportunity to comment on the draft GAO report "Probabilistic Risk Assessment: An Emerging Aid to Nuclear Power Plant Safety Regulations." We found the report to be an excellent document describing the nature of probabilistic risk assessment (PRA) and its use in dealing with complex nuclear power plant safety issues under conditions of high uncertainty. The report, in general, is accurate and provides a clear perspective on the subject. In particular, we are pleased to note its major conclusion which states, "GAO believes that in view of the evolving nature of PRA, the time and expense required to prepare and review major PRA studies, and the staff's experience and training, NRC is making timely and reasonable use of PRA in the nuclear regulatory process." We are also in agreement, "---that NRC should not use end-result numerical risk estimates as the sole or primary basis for regulatory decisions."

Enclosed are some suggestions for factual modifications or clarifications that we believe, would strengthen the report. In addition, some information has been provided to update the status of programs which have changed and PRAs which have been completed since the GAO inquiry was performed.

If you have any questions, please contact Dr. Gary Burdick (443-7960).

Sincerely,

A handwritten signature in dark ink, appearing to read "William J. Dircks".

William J. Dircks
Executive Director for Operations

Enclosure:
Comments on GAO Report

COMMENTS ON DRAFT GAO REPORT ENTITLED, "PROBABILISTIC
RISK ASSESSMENT: AN EMERGING AID TO NUCLEAR POWER PLANT SAFETY REGULATION"

Page iii, line 12: Change "GAO found that...not unique to PRA" to "GAO found that PRAs identify and assign probabilities to events that rarely occur. In addition, PRAs are able to identify and quantify uncertainties. These uncertainties are not caused by PRA."

Page v, line 4: Change "develop" to "improve".

Page vi, last paragraph: Replace by the following: "In preparing cost/benefit analyses using PRA techniques, however, NRC develops estimated risk reductions for potential remedial actions based on PRA results (either surrogate or plant specific). The costs and benefits are converted to a common unit of measure. The cost in dollars of a required modification is compared to the estimated averted consequence of the accident scenario under consideration, i.e., person-rem or fatalities. The result of the analysis is in the form of dollars per health effect averted (e.g., latent cancer) or cost per immediate fatality averted. This practice is controversial and the appropriate cost for decisionmaking has not been determined, nor has NRC consistently applied the same measure in dollar values to human life and health effects."

Page vii, line 16: Change "program" to "research program".

Page vii, last paragraph, line 7: Change "over 18 months" to "about 9 months to over 18 months".

Table of Contents: Chapter 3, Title: Change "BUT...RESOLVE THEM" to "BUT CANNOT ELIMINATE THEM".

Chapter 5, line 5: Change "PRA will be" to "PRA may be" (as used in page 104 of the report).

Page 7, line 7: Change "to establish the design..." to "to establish multiple levels of protection in nuclear plant design against hazards to public health and safety."

Page 17, line 13: Change "1000 years of reactor operation" to "1000 years of reactor operation with about 90 percent confidence."

Page 19, line 20: Replace bottom statements by the following:

--The lack of recognition of fires, earthquakes and human actions as important accident initiators due to incomplete knowledge and unsophisticated techniques in quantification of these events.

--The uncertainty of the sequence probabilities was greatly understated."

Page 21, line 20: Change "are statements of" to "are probabilistic, and are capable of dealing with."

Page 22, line 22: Replace "PRA" by "plant operation".

Page 23, Second paragraph, last sentence: Delete. Reactor vessel rupture has been considered in WASH-1400 and in the recent study on Pressurized Thermal Shock for bounding estimates of risks.

Page 23, After the last line, add: "Nevertheless, subjective judgment of experts may contribute valuable information to allow better decisions to be made."

Page 26, line 1: Replace "models" by "techniques".

Page 26, line 6: Add: "although current and planned data collection programs are expected to improve the situation."

Page 29, last sentence: Change "Technique for Human Reliability Event Rate Prediction" to "Technique for Human Error Rate Prediction."

Page 31, line 2: Change "treats operator..." to "treats some operator..."

Page 31, line 5: Change "frequency reflects...fail to subdue" to "frequency does not reflect the probability that the recovery action will subdue."

Page 39, line 17: Replace "However...large variances" to "However, both procedures have large overall uncertainties".

Page 45, last paragraph, line 7: Change "...science of risk assessment" to "science of risk assessment or are stochastic and inherently irreducible".

Page 47, line 15: Change "will primarily...severe accident environment" to "will include multiple failure rates due to common cause events and component failure rates under severe environments".

Page 49, line 3: Change "provide data" to "provide a complete set of data".

Page 49, line 14: Change "not address" to "not completely address". RES does have an effort ongoing in this area.

Page 50, line 7: Delete "for NRC". These data are being collected for multiple users.

Page 50, end of first paragraph: Insert as the penultimate sentence, "The NRC is closely monitoring and evaluating this activity".

Page 51, line 11: Change "NRC started to develop" to "NRC began initial planning on development of".

Page 51, line 30: Change "study of...pipe breaks" to "study of internal and external flood hazards".

Page 52, line 14: Change "from four plants" to "from eleven units at seven different plants".

Page 52, line 18: Change "from four plants" to "from plants".

Page 53, line 6: Delete "a 3 year...year 1986".

Page 53, line 10: Change "This is not...accidents" to "The staff conclusion was that such data did exist, but was proprietary; thus no NRC harsh environment data base could be constructed".

Page 54, middle paragraph, last line: Change "Further...recovery actions" to "The human reliability research program, to date, has developed methods for treating both human errors of omission and commission under a variety of performance shaping conditions. A Multiple Sequence Failure Model has been developed to assess dependencies among behavioral steps in human action sequences. The NRC is initiating a comprehensive cognitive process modeling project that will address most aspects of human information assimilation and decisionmaking, including recovery actions."

Page 55, line 5: Change "However...comparable" to "That project involved, among other things, development and testing of procedures for comparing and combining data from diverse sources, for inclusion in the data bank."

Page 55, line 21: Change "NRC is also...data" to "The NRC is completing a 3 year study examining the feasibility and advisability of a voluntary, anonymous, nonpunitive, independent third party managed data collection system patterned after the Federal Aviation Administration (FAA) Aviation Safety Reporting System".

Page 57, first paragraph: Replace the last sentence by: "The analytic tools described in NUREG/CR-3688 and 4016 are task independent and thus capable of analyzing non-control room tasks. More specifically, the MAPPS computer simulation model described in NUREG/CR-3626, is directed toward analysis of maintenance technicians, electricians, instrumentation and control technicians and supervisory personnel."

Page 66, at the end of the second paragraph, add: "In addition, the Seismic Design Margin Research Program is providing a means of judging the adequacy of seismic margins in plants based on existing PRAs".

Page 67, last paragraph: After the first sentence, add "Improvements are in process on fire growth models".

Page 67, second line from end: Change "nuclear fuels...these fuels" to "materials which could fuel a power plant fire and on the size of fires caused by these fuels. Current work does address these two data needs, through fire testing to develop vulnerability profiles of components in a fire environment, and through a limited survey of materials which could fuel fires".

Page 68, at the end of first paragraph, add: "The Office of Research does intend to reevaluate external flood research and to begin a program in 1986 if warranted".

Page 87, line 2: Change "PRA in its...proceeding" to "PRA in developing the technical basis for rulemaking".

Page 94, line 24: Delete "and does not plan to require".

Page 97, line 3: Change "has proposed" to "is considering".

Page 97, line 14: Change "deciding these issues" to "implementation of these programs".

Page 100, line 6: Change "not to resolve" to "not to use safety goals in the decision process to resolve".

Page 100, line 27: Change "well below...safety goal" to "a frequency higher than the safety goal".

Page 103: Change last sentence to read "Implementation of the program has been deferred until FY 1987 due to budget constraints".

Page 104, line 7: Change "a program" to "a research program".

Page 105, line 4: Change "NRC's statement...programs" to "The Statement of Considerations in the ATWS rule urging utilities to voluntarily develop reliability assurance programs for reactor trip systems."

Page 107, line 15: Change "the end of 1984" to "mid-1986".

Page 109, second paragraph, line 4: Change "over 18 months" to "from 9 to over 18 months".

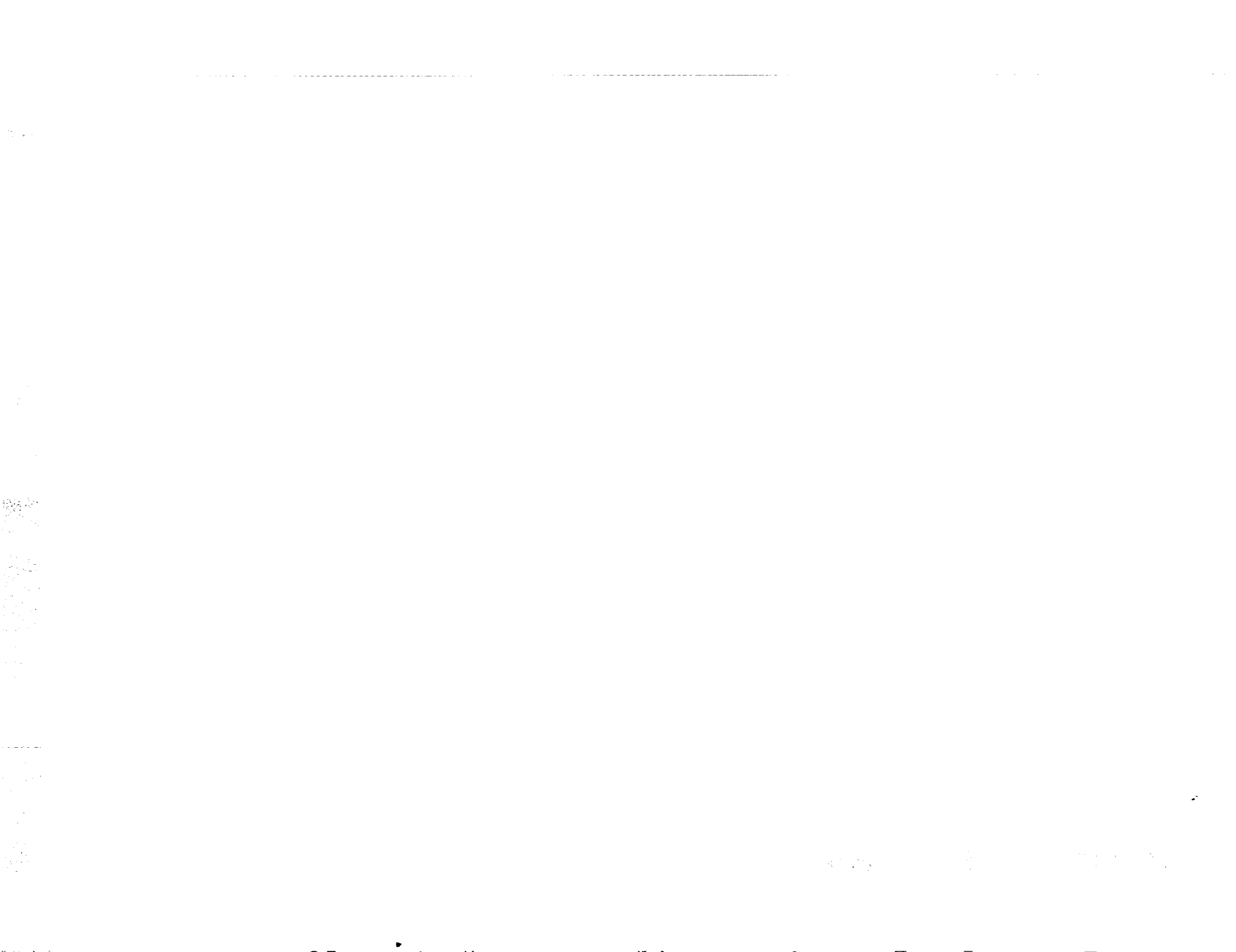
Page 110, middle paragraph: Change "center of PRA expertise" to "center of NRR PRA expertise,"

Page 111, line 1: Change "Although...Regulation" to "Although NRR PRA experts are centered in one division,".

Page 121, Table: Replace "Calvert Cliffs 1" by "Calvert Cliffs 2" and "Calvert Cliffs 2" by "Calvert Cliffs 1".

Page 123, Table on MAJOR INDUSTRY PRA STUDIES: Add:

Seabrook 1 and 2	1983	Public Service Company of New Hampshire
Midland 1 and 2	1984	Consumers Power Company
GESSAR (BWR Standardized Design	1983	General Electric



.....

31514

AN EQUAL OPPORTUNITY EMPLOYER

UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE \$300

**BULK RATE
POSTAGE & FEES PAID
GAO
PERMIT No. G100**

AE