#2
5/8/80

ALO-65
EI-79-23

PHASE I
TECHNICAL REPORT
ON

LWR DESIGN DECISION METHODOLOGY

MASTER

ENERGY INCORPORATED
1134 INDUSTRY DRIVE
SEATTLE, WASHINGTON 98188

ENERGY
INCORPORATED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use or the results of such use of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Printed in the United States of America

Available from
National Technical Information Service
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

Price: Printed Copy \$4.50; Microfiche \$3.00

ALO-65
EI-79-23

PHASE I
TECHNICAL REPORT
ON
LWR DESIGN DECISION METHODOLOGY

Prepared by

Energy Incorporated
1134 Industry Drive
Seattle, Washington 98188

Prepared for

U. S. Department of Energy
Light Water Reactor Safety Technology Management Center
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sponsored by

U. S. Department of Energy
Division of Nuclear Power Development
Washington, D.C. 20545

Work performed under Sandia Contract No. 42-4229

Submitted: October 1979
Printed: March 1980

DISCLAIMER

This book was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

TABLE OF CONTENTS

	<u>PAGE</u>
1.0 INTRODUCTION	1
2.0 REVIEW OF CURRENT DESIGN DECISION PROCESS	2
2.1 Basic Safety Philosophy	2
2.2 Implementation of Design Philosophy	5
2.3 Key Safety Issues and Decision Criteria	7
2.3.1 Accident Evaluation	7
2.3.2 Basic Criteria for Safety Design	8
2.4 Current Decision Techniques	10
2.5 Interface of Existing Process with Probabilistic Techniques	12
2.6 Rationale for Utilization of Probabilistic Techniques	13
2.6.1 Regulatory Recognition of Techniques	13
2.6.2 Examples of Utilization of Probabilistic Techniques in Reactor Systems Design	15
3.0 PROBABILISTIC DESIGN DECISION METHODS	21
3.1 Event Tree Analysis	25
3.1.1 Accident Initiating Events	25
3.1.2 Individual Event Sequence Quantification	26
3.2 Fault Tree Analysis	26
3.3 Failure Modes and Effects and Criticality Analysis	28
3.4 Reliability Block Diagrams	29
3.5 Uncertainty Analysis	30
3.6 Cost Estimating	31
3.6.1 Scope of Cost Estimates	32
4.0 PHASE II: DESIGN DECISION METHODOLOGY DEVELOPMENT	34
4.1 Phase II - Methods Development	36
4.1.1 Design Decision	37
4.1.2 Design Criteria Compliance	37
4.1.3 Identification of Analysis Techniques	37

Table of Contents (cont'd)

	<u>PAGE</u>
4.1.4 Design Decision Process	38
4.1.5 Scope of Analysis Activity	38
4.1.6 Level of Design Detail	38
4.1.7 Alternative Design Generation	39
4.1.8 Quantitative Design Criteria	39
4.1.9 Uncertainty Evaluation	39
4.1.10 Optimization of Factors	40
4.2 Phase II - Methods Demonstration	40
4.2.1 WASH-1400 Surry Systems	40
4.2.2 Baseline Designs	41
4.2.3 Proposed "New" Design Alternatives	41
4.2.4 Design Alternative Assessment	42
4.2.5 Optimize Design	42
4.2.6 "Backfit" Designs	42
4.2.7 "Backfit" Impact	42
4.2.8 Implication of Design Decision Demonstration	43
4.3 Phase II - Documentation	43
4.4 Phase III Plan	43
5.0 REFERENCES	45

LIST OF FIGURES

	<u>PAGE</u>
2-1 Existing System Design Decision Process	3
3-1 Task Flow for Risk Based Design Evaluation	22
3-2 Key Elements of LWR Risk Evaluation Methodology	24
4-1 System Design Decision Methodology Flow Chart	35

1.0 INTRODUCTION

Energy Incorporated (EI) was selected by Sandia Laboratories to develop and test an LWR design decision methodology. Contract Number 42-4229 provided funding for Phase I of this work. This technical report on LWR design decision methodology documents the activities performed under that contract.

Phase I was a short-term effort to thoroughly review the current LWR design decision process to assure complete understanding of current practices and to establish a well defined interface for development of initial quantitative design guidelines. Phase II, to be accomplished during FY '80, will include the development and demonstration of a quantitative based design decision process primarily at the system level.

A design decision methodology will be developed utilizing probabilistic techniques to determine a figure of merit for safety system design and allow optimization of cost versus safety on a relative basis. This methodology will be demonstrated on existing safety system designs.

Phase III (the final phase) is an extension of the methods developed in the previous phase wherein component, subsystem, and system design and operational parameters will be related to an overall plant and its associated risk characteristics. The method will allow the determination of the contribution to plant risk from individual elements and assessment of the degree of risk improvement or degradation which may be expected through design or operational changes.

The following sections document information gained as a result of the Phase I effort. Section 2.0 provides a review and discussion of the current decision process and provides information and rationale to support the development of an integrated design decision methodology. Section 3.0 provides information on the key analytical techniques which will form the basis for the methodological development. Section 4.0 is a detailed outline of specific activities to be performed as part of the Phase II effort.

2.0 REVIEW OF CURRENT DESIGN DECISION PROCESS

Figure 2-1 represents the current design process in use in the nuclear industry. The present process utilizes various tools to derive the necessary information for design decisions. Engineering analyses utilizing computations and simulations provide information on functional and operational requirements; cost estimating provides the price of a particular design; and qualitative assessments (e.g., failure modes and effects analysis) and design reviews identify safety compliance information.

One difficulty with this process is that while quantitative information is available on functional achievement and cost, the safety level (probability of success or failure) of a design is usually qualitatively expressed. This situation makes it nearly impossible to choose between competing designs or allocate resources to optimize cost and safety. In addition, examination of the benefits in terms of improved safety of a proposed change or backfit is difficult utilizing the existing decision process.

Two major constraints exist which impact the design process: the operability and licensability of the reactor. However, in today's climate, the licensability of a design is the overriding consideration. Thus, many of the design decisions are made strictly to meet licensing requirements which may or may not actually add to the operability or even the safety of the plant.

The present design context and constraints are described in the following portions of this section. Areas where probabilistic techniques may be of some utility are identified. The concluding portion of Section 2.0 describes examples of current practice utilizing probabilistic criteria and/or techniques in the design of nuclear power plants or plant systems.

2.1 Basic Safety Philosophy

The Nuclear Regulatory Commission (NRC) is responsible for assuring the public health and welfare in matters relating to commercial nuclear facilities⁽¹⁾. In

FIGURE 2-1 EXISTING SYSTEM DESIGN DECISION PROCESS

carrying out this responsibility, rules and procedures have been established which form the basis for current industrial practice. An overall philosophy has been developed⁽²⁾ which forms the basis for design, construction, and operation of LWRs. This philosophy is generally referred to as "defense in depth." This concept refers to three identifiable levels of safety.

The first level of safety is to design for maximum safety in normal operation and provide maximum tolerance for system malfunctions. The intent is to prevent accidents through intrinsic design features such as quality, redundancy and fail safe states. Analyses are made and test programs conducted to identify various malfunctions or faults which could affect reliability of operation so they may be guarded against by design, quality assurance or fail safe features.

The second level of safety assumes that incidents will occur in spite of the prudence reflected in the first level of safety. Safety systems are provided to prevent the occurrence or minimize the damage from such incidents. Conservative design practices, safety margins, and independent, redundant detecting and actuating equipment are incorporated into the design of protection systems. Emergency core cooling systems (ECCS) and reactor shutdown systems are illustrative of second level safety considerations.

The third level of safety supplements the first two through features which add margin in the plant design as additional assurance that protection to the public is provided even in the event of the occurrence of extremely unlikely and unforeseen circumstances. This margin is evaluated primarily by testing the design concept against severe hypothetical accidents, involving the postulation of independent failures of some of the redundant protective systems simultaneously with the accident they are intended to control. From analyses of these postulated events, several accident sequences are selected as a basis for the design and incorporation of the plant features and equipment required for protection of public health and safety. The sequences selected for this purpose are called Design Basis Accidents (DBA's).

This multi-layered safety philosophy is characterized by subjective statements of desired safety goals or values. Typical are loosely defined states such as maximum level of safety, sufficient redundancy, adequate safety margins,

unlikely and extremely unlikely events, and high degree of freedom from faults and errors. It is in these areas that probabilistic techniques can be used to provide a better understanding of safety parameters and provide insights into the overall level of safety.

It should be noted that NRC is concerned only with assuring public health and safety and not directly with economic issues as they may relate to the design process. The owner/operator has primary responsibility for the safety and reliability of a particular facility. Since the facility cannot be operated unless requisite levels of safety are demonstrated to the satisfaction of the NRC, economics are closely tied to the design decision process both in capital costs associated with designing and building the facility as well as plant operation. However, no mechanism currently exists to systematically evaluate designs in terms of safety and cost and then optimize the designs with respect to these parameters.

2.2 Implementation of Design Philosophy

NRC promulgates various regulations, criteria, standards and guides to carry out this multi-layered design philosophy. LWR design decisions are based upon general design criteria contained in 10CFR100 Appendix A. These criteria establish minimum requirements for safety functions and systems which individual facilities must meet.

Regulatory Guides⁽³⁾ are issued to provide information on how certain criteria may be implemented by methods acceptable to the NRC. Each guide contains a discussion of a specific item and a regulatory position is stated. The NRC Standard Review Plan⁽⁴⁾ provides guidance to the staff for the review of applications for the construction and operation of a nuclear plant. This review plan provides acceptance and review procedures for various safety concerns. Additionally, applicable industry codes and standards such as ASME codes and ANSI standards are incorporated by reference into the documentation noted above.

Taken together, the government and industry criteria, requirements and accepted methods provide a prescribed approach for proceeding from conceptual

design to an operating facility. As previously shown, Figure 2-1 depicts the overall system design decision process and represents the basic decision points to provide the focus for this study.

Several steps precede the development of a proposed system design for any of the safety systems at a particular LWR. These steps are noted and briefly described below to allow some general understanding of the process that provides the basic input, i.e., the proposed design and design requirements for the plant.

- (1) Site selection -- The selection by a utility company of a particular site for an LWR plays a definite role in the designation of safety system design requirements. Selection of the plant location is one of the earliest decisions made that affects the present design process.
- (2) Reactor selection -- The particular type of plant (PWR, BWR, etc.) and plant size (number of MWe) play a significant role in the ultimate design of safety systems. This selection is made at about the same time as the site selection, or very shortly after site selection.
- (3) Selection of Design Basis Accidents (DBA's) -- The determination of which accidents are to be designed for provides the foundation upon which all design requirements for the various plant safety systems are developed.
- (4) Designate safety systems -- Once the DBA's have been determined, safety systems designed to prevent or mitigate the consequences of these accidents are specified. This process outlines which systems will be required to meet the siting criteria (10CFR100) under the designated DBA conditions. This process includes designating which systems will be engineered safety features and which will be seismic Category I, etc. Also, the list of functional and operational requirements for the particular plant design will be developed during this time.
- (5) Safety analysis -- A certain amount of analysis is generally performed during the development of the design requirements for the

safety systems. This includes preliminary analysis to confirm compliance with 10CFR50 Appendix A, 10CFR100, and various other forms of regulatory guidance.

Although the steps in the initial decision process for system design are shown in Figure 2-1 as sequential, most are overlapping and integrated during the design process. These decision processes are applied repeatedly at one time or another during the sequence of design activities.

2.3 Key Safety Issues and Decision Criteria

2.3.1 Accident Evaluation

Each applicant for a construction permit or operating license is required by Section 50.34 of 10CFR50 to provide an analysis and evaluation of the design and performance of the structures, systems and components of the facility with the objective of assessing the risk to public health and safety. These analyses are to include a determination of the margins of safety during normal operation and transient conditions expected during the life of the plant and the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of potential consequences.

These evaluations usually proceed by assuming various events or conditions and determining the response of the plant and estimating the resultant consequences. In general, three categories of events are considered. These include:

- (1) Anticipated operational occurrences which are not expected to lead to radioactive releases beyond the criteria for normal operation. Examples of such events might be loss of off-site power, loss of feedwater flow or inadvertent depressurization of the primary system.
- (2) Events with a small probability of occurrence with the potential for a small radioactivity release from the facility. Such events

might include complete loss of all ac power, small leaks or breaks in pipes or complete loss of normal forced reactor coolant flow.

- (3) Potentially severe accidents which are expected to have an extremely low probability of occurrence. Events of this nature are postulated to establish performance requirements for engineered safety features. Such events might include major pipe breaks (LOCA), and effects of naturally occurring phenomena such as floods, tornadoes, and earthquakes.

Events in category 3 above are referred to as design basis accidents (DBA's) and serve to establish maximum requirements which the facility and the engineered safety features must meet. In actual practice, nine classes of postulated accidents or occurrences are defined. Events are classified according to their potential severity in ascending order. Class 1 is the least severe and represents a trivial occurrence and Class 8 includes the DBA's. Any accidents beyond DBA's are referred to as Class 9 and are generally regarded as hypothetical accidents. Such an accident sequence would require successive failures of multiple barriers and design features are not specifically provided to respond to such abnormal conditions.

The probability of DBA's is estimated to be very small. If sequences of successive failures are more severe than those considered in the design basis are postulated, then the consequences can be expected to be more severe. Assumptions of successive failures can be made wherein safety systems can no longer cope with the postulated accident. However, it is expected that the probability of the required number of failures is so small, that the risk from such events are negligibly low. For these reasons, Class 9 accidents are presently considered beyond the design basis.

2.3.2 Basic Criteria for Safety Design

As indicated in Section 2.2 various criteria are set forth to guide the design process. Certain specific criteria are relied upon to provide adequate margins of reliability and safety. Some of the presently existing safety criteria are discussed below.

- (1) Single Failure -- Appendix A of 10CFR50 states that single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither a single failure of any active component (assuming passive components function properly) nor a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions. This is a most important criterion which is relied upon to provide a margin of safety for individual systems.
- (2) Redundancy -- This criterion is closely related to the single failure criterion. It is generally stated in terms of suitable or sufficient redundancy in components and features to assure that for a given condition, a particular safety system function can be accomplished assuming a single failure.
- (3) Independence - Isolation -- These criteria relate to maintaining systems required for safety to be independent or isolated from non-safety equipment and for redundant subsystems to be isolated from each other to prevent loss of safety functions. These criteria are also directly related to the single failure criterion and are generally stated in terms of requiring sufficient independence or isolation such that safety functions can be performed assuming a single failure has occurred.
- (4) Diversity -- Diversity involves using different methods, manufacturers, etc., in the design process in order to remove or lessen the likelihood of some common design flaw preventing successful system operation.

2.4 Current Decision Techniques

In the current process, there are many different design options available to meet each of the various requirements and criteria. In addition, many of the key safety issues involve the degree of safety margin available, e.g., sufficient redundancy, suitable independence. At present the designer, architect-engineer, and licensee must demonstrate to the regulatory reviewers that the particular design selected meets these criteria. Since the criteria are qualitative in nature, the decisions made become questions of engineering judgment. Decisions are primarily based upon similarity to previously accepted designs or closely following recommendations presented in Regulatory Guides and applicable codes and standards.

Most of the regulations, criteria, and guides concerning reactor safety give no explicit reference to probabilities, much less to any specific numerical probability values to be achieved or evaluated. There are certain requirements in the regulations which have implicit probabilistic connotations, such as usage of the single-failure criterion and the requirements for consideration of all credible accidents. More specifically, 10CFR100 states that the fission product release assumed for calculational purposes should be based upon a major accident, hypothesized for purposes of site analysis or postulated from considerations of possible accidental events, that would result in potential hazards not exceeded by those from any accident considered credible. The NRC staff has stated, in connection with its safety reviews, that its objective is to ensure that the spectrum of postulated events considered credible and used as design basis events, include all those whose frequency of occurrence exceeds approximately once-in-ten million per year. Since there may be up to about ten (10) such events that have a frequency of occurrence of approximately 10^{-7} per year, this implies that the overall frequency of occurrence of any such event, not included in the design basis envelope, is on the order of 10^{-6} per year or less. Because of the lack of explicit criteria to be met or guidelines to be used, the probabilistic approach, and particularly the probabilistic-risk assessment approach, has seen limited use by the NRC staff.

As noted in Section 2.3, various accident conditions are assumed and the capability of the facility to respond to those conditions are calculated. Generally, these events are considered singularly. Based upon the event under consideration, requirements are specified for system operation. Various standard engineering analytical techniques and computer programs are utilized to verify or demonstrate that system performance meets or exceeds the requirements. Generally, conservative assumptions are included in the evaluation process to account for possible uncertainties.

Probabilistic methods are not currently an integral part of the design decision process. Individual licensees or vendors may perform probabilistic evaluations on a specific system or subsystem in response to a specific concern. However, they are not generally applied in a manner which would support the selection of specific design configurations.

Probabilistic analysis techniques have been utilized to guide the decision process in selected areas to assure protection against certain phenomenological considerations such as hazards from aircraft crashes and internally generated missiles. Section 3.5.1.6 of the Standard Review Plan states that a plant shall be considered adequately designed against aircraft hazards if the probability of aircraft accidents resulting in radiological consequences greater than 10CFR100 exposure guidelines is less than 10^{-7} per year. Regulatory Guide 1.115 on low-trajectory turbine missiles states that the protection of essential systems located within the low-trajectory missile strike zone is acceptable if, in the event of turbine failure, the probability of damage summed over all such systems is less than 10^{-3} .

It should be noted that in these instances not only must probabilistic methods be used to support design, location and layout of the plant and particular safety systems, but specific numerical acceptance criteria are stated. The most notable example of utilization of numerical goals is associated with the concern of the occurrence of an anticipated transient without SCRAM (ATWS). WASH-1270⁽⁵⁾ provided guidance for the design of reactor protection system unreliability in setting an objective of less than 10^{-7} for failure of operation of the protection system following an anticipated transient. ATWS concerns and the manner in which individual plant designs accommodate such occurrences

have been the subject of much debate over the years. However, it is clear that numerical safety objectives or aiming points provide significant focus to the question of design adequacy of reactor protection systems.

2.5 Interface of Existing Process with Probabilistic Techniques

From the discussion of the current design decision process given in the preceeding sections, it is apparent that a loosely fabricated framework exists for the inclusion of probabilistic methods into the design decision process. The overall safety philosophy which guides the decision process is based upon three levels of safety that rely on probabilistic considerations. The terms anticipated, likely, unlikely, and extremely unlikely are used variously to describe event occurrence frequencies. Design criteria contain expressions such as "suitable redundancy" or "sufficient independence" that would be more meaningfully addressed through relative quantitative expressions.

A major finding of the review of the current design decision process is that most decisions are made relative to an individual function, system or event. Design or operational adequacy is based upon individual evaluations of specific systems and how they respond to a specific set of conditions. Currently there is no means for judging the relative value of particular systems in meeting overall plant safety objectives. Using the current process, it is very difficult to evaluate the system-to-system interactions and dependencies that may have significant safety impact.

It appears that the current design process can benefit considerably from an integrated probabilistic approach. Although limited applications have been made, uncertainties and unfamiliarity with probabilistic techniques and the inability to set specific safety goals to determine "how safe is safe enough" have limited the utilization of these techniques. Recent LWR applications of these methods and more general acceptance of their validity make it appear they may be utilized much more directly in the decision process.

2.6 Rationale for Utilization of Probabilistic Techniques

2.6.1 Regulatory Recognition of Techniques

Probabilistic methods for safety and reliability evaluations were originally developed in the aerospace industry. For more than twenty years these techniques have been an integral part of the engineering process, particularly in the area of DOD weapon systems. These techniques were proven to be amenable to the evaluation of complex electrical, mechanical and structural systems. In many cases specific numerical reliability and safety goals are set for system design and operation, and economic incentives are provided for meeting such goals.

WASH-1400⁽⁶⁾ was the first major application of such techniques to nuclear power plants. Although it was an after-the-fact assessment (i.e., not part of the design development process) it was extremely important in the demonstration of the applicability of the techniques to nuclear systems and greatly enhanced the general understanding of such methods.

Following the issuance of WASH-1400, the NRC stated⁽⁷⁾ that they anticipated that future usage of the study and the use of a probabilistic approach would slowly work its way to a greater extent into the NRC's licensing of nuclear power plants. The approach might be used to look at the likelihood of different types of events within a facility, particularly for an assessment of the relative likelihood of such occurrences, and extended to the determination of reliability of small subsystems and larger systems. It was stated that probabilistic methods could be useful for providing an overall perspective of the licensing process and for determining the relative importance of selected concerns. Some NRC staff feel probabilistic analysis might be used in making more balanced judgments concerning selected events and for making the licensing approach more systematic.

More recently the NRC has stated⁽⁸⁾ that the general methodology contained in WASH-1400 should be used to perform risk assessments of all

elements of the nuclear fuel cycle and that it was now clear that the safety review of nuclear power plants can be assisted by the engineering insights and techniques developed in WASH-1400 and that these techniques can be used as an additional effective tool to help decision making processes.

In the recent review of the WASH-1400 methodology, commonly referred to as the Lewis Report,⁽⁹⁾ it was stated that the fault tree/event tree methodology used in WASH-1400 is sound and that both can and should be more widely used by NRC. It was also stated that proper application of the methodology can provide a tool for the NRC to make the licensing and regulatory process more rational. The Lewis Committee specifically recommended that fault tree/event tree analyses should be among the principal means used to deal with generic safety issues, to formulate new regulatory requirements to assess and revalidate existing regulatory requirements and to evaluate new designs. It also recommended the re-evaluation of NRC's inspection and quality assurance system and licensing criteria to determine the extent to which they should incorporate those things that were learned from WASH-1400 and other relevant literature.

As a result of the TMI accident, further emphasis has been placed on increased utilization of probabilistic approaches. As an example, the ACRS recommended⁽¹⁰⁾ that studies be made to reduce the probability of accidents through evaluation of the interfacing and interconnection of supporting systems and the evaluation of the safety effects of shared systems or locations in multiple reactor stations. Most recently, in commenting on the long term lessons learned from TMI, NRC addressed the area of design requirements and stated⁽¹¹⁾ that they are considering recommendations for application of fault tree analysis to fluid systems, instrumentation and control systems and on-site and off-site electric power in the safety analysis report and staff reviews. It was noted that this would be "one step forward" of the present practice of applying single failure criteria.

From the brief foregoing discussion it is clear there has been a gradual and growing acceptance and understanding of probabilistic techniques and their

utilization in the LWR design decision process. Recent occurrences have set the stage for a comprehensive demonstration that such techniques can be integrated into the decision process and have a positive impact on LWR safety.

2.6.2 Examples of Utilization of Probabilistic Techniques in Reactor Systems Design

Various applications of probabilistic methods to the nuclear design decision process have been made which serve as illustrative examples of their utilization. Following is a brief description of some recent efforts which indicate the broad scope of such applications.

(1) Clinch River Breeder Reactor Plant (CRBRP) Licensing Approach

The CRBRP project incorporated a probabilistic approach into its licensing process. Although CRBRP licensing activities have been temporarily suspended for political reasons, the approach taken to achieve licensing of this new reactor concept is of interest.

CRBRP employed a comprehensive reliability program.⁽¹²⁾ Quantitative reliability analyses played an important role in that program. Its primary uses were: (a) as a tool for the evaluation of systems to provide the system equipment designers with reliability aiming points, (b) as a means for evaluating random independent failure modes, (c) as a decision aid for selecting between alternative designs, (d) as a guide for the design of the testing program and (e) as the basis for sensitivity studies to evaluate the range of unreliability due to common cause failures. For the purpose of these evaluations, a top level system failure probability was selected for the loss of coolable core geometry. It was specifically noted in the CRBRP PSAR that all the primary uses for the numerical reliability analyses are as aids in decision making. The analyses are not intended to demonstrate compliance with a top level system failure rate.

In official comments on this approach, NRC stated⁽¹³⁾ that they would use the safety objective that there be no greater than one chance in one million per year for potential consequences greater than the 10CFR100 dose guidelines for the CRBRP and that this would be a design objective rather than a fixed number which must be demonstrated for a given plant. However, they believed that the numerical evaluations of system reliability and accident risks undertaken by the CRBRP Project, as well as the traditional systematic and disciplined evaluations of the plant design, are of significant value in indicating whether the safety objective "aiming point" is being adequately approached; and that these activities should be continued.

(2) DOE Lines of Assurance (LOA) Program

The DOE has initiated a Breeder Reactor Safety Technology Program⁽¹⁴⁾ with the objective to "provide the safety technology which will permit Breeder Reactor designers to achieve and substantiate requisite levels of safety for protection of the public from Breeder Reactor accidents without unacceptable penalties in plant economics." The program is designed to achieve this objective through development, verification, and application of quantitative assessment of risk to public health from postulated Breeder Reactor accidents.

The concept of Lines of Assurance (LOA) has been developed to help meet program objectives. Four specific LOA's have been identified.

- LOA 1: Prevent Core Disruptive Accidents (CDA's)
- LOA 2: Limit Core Damage
- LOA 3: Control CDA Progression
- LOA 4: Attenuate Radiological Consequences

Overall reliability goals have been postulated and numerical criteria assigned to each LOA. It is the intent to allocate these numerical goals to the various systems and develop an overall breeder reactor

design which is supportive of these numerical criteria. Appropriate analysis, tests, etc., would be accomplished to assure goals have been met. This DOE program is formative in nature and directed at advanced reactor development, but is indicative of the increasing role of quantitative approaches.

(3) Comparative Evaluations Supporting the Licensing Process

NRC has stated⁽¹⁵⁾ that one of the most useful applications of probabilistic techniques is the analysis of postulated accident sequences to determine their importance relative to similar sequence probabilities given in WASH-1400. In one case an analysis was performed to investigate the risk from seismically induced fires to determine if fire protection systems should be designed to seismic Class I requirements. The analysis performed indicated that the probability of a seismically induced fire was small compared to the probability of a randomly-induced fire occurring from causes not associated with an earthquake. The study served as a basis for the NRC decision that fire protection systems should be designed to seismic Class II instead of Class I.

Probabilistic techniques were used internally by the NRC to determine the importance of a number of safety issues raised by members of the regulatory staff. These issues were suspected of being treated inadequately in the licensing process. The study showed that of those items related to plant safety, the majority involved potential accident sequences which would not have significant releases of radioactivity or which would have lower probabilities than other accident sequences having similar releases of radioactivity. Thus, those items would not significantly affect the risks predicted in WASH-1400 and need not be considered further.

An operating utility⁽¹⁶⁾ experienced a wiring error in the emergency diesel load sequencer. They utilized engineering analyses and probabilistic techniques to determine the impact of such an occurrence on plant safety. Accident sequences were evaluated which represented

the plant conditions of interest. Results of the analysis showed the probability of unacceptable consequences were much smaller than those of similar consequences as documented in WASH-1400. The utility demonstrated that operation of the plant with a faulted load sequencer did not result in any appreciable increase in plant risk and did not degrade the level of safety of the plant.

(4) Contractor Design Reliability

Some vendors and A&E's use probabilistic techniques to support various aspects of their individual design decision process. One such application by an A&E employing fault tree analyses to determine the optimum design of an auxiliary feedwater system is described in the following paragraphs.⁽¹⁷⁾

For a particular LWR design, the preferred source of water for the auxiliary feedwater system (AFS) was the condensate storage tank (CST). Backup sources were available from the two trains of the essential service water system. Early in the AFS design effort it was recognized that a water source qualified as an engineered safety feature must be available to the AFS without operator intervention. This meant that either the CST must be built to seismic Category I standards with tornado missile protection, or else the admission of service water to the AFS must be automatic in the event that the CST fails to sustain sufficient suction head for the AFS pumps.

Although qualifying the CST was estimated to be much more expensive than automating service water admission, several arguments seemed to dictate the more expensive option. Some of these include:

- (a) The AFS must start very promptly in an emergency.
- (b) Earthquakes and tornadoes can cause a loss of off-site power, thereby causing a demand for auxiliary feedwater as well as hazarding an unqualified CST.

- (c) The AFS incorporated diversity in motive power - ac powered pumps and a steam-turbine-driven pump. The essential service water system is ac powered. Insofar as the AFS depends upon the essential service water system, this diversity is compromised.
- (d) Service water does not meet the standards for feedwater chemistry control. While steam generator contamination by service water can be tolerated in a genuine emergency, the requirement of a major cleanup effort could force a costly outage. Thus, the unnecessary use of service water in the AFS should be minimized.

The last three points appear to be powerful arguments for the extra expense of a seismic Category I, missile-protected condensate storage tank. As it turned out, these arguments are not quantitative, and ignored the role of human error.

The fault tree analysis of the AFS showed that the availability of the CST is important to the reliability of the AFS, but human error rather than geophysical hazards dominates the risk that the CST might fail to meet AFS needs. Even a conventional CST would survive a near miss by a tornado or a low-intensity earthquake. Upgrading the CST to safety-feature standards would not change the likelihood of human error, such as the chance that maintenance personnel might leave closed the manual isolation valve at the CST.

Even when the common-mode effects noted in points b and c above were factored into the analysis, it was found that the diverse and redundant water supply offered by automatic service water admission did more to improve the reliability with which the AFS would start promptly in an emergency than did upgrading the CST.

It was found that the risk of unnecessary steam generator contamination with service water was very small with either design option. It is dominated by operator error. By taking the principal responsibility

for admitting service water from the operators and placing it in an automatic system, the risk of contamination via operator error could be reduced. Therefore, both safety and feedwater purity considerations actually favor automatic service water admission.

Altogether, the fault tree analysis of the AFS took 4 manmonths to perform and entailed a few hundred dollars in computer charges. In the course of the study one design flaw was identified, two instances were found in which a cheaper design variant (including the case above) would actually improve system reliability, and numerous minor recommendations for the improvement of the design or operating procedures were formulated. The projected cost avoidance by following the recommendations was well in excess of \$500,000 per unit, and the projected probability of AFS failure on demand was one-eighth of that for the original design.

3.0 PROBABILISTIC DESIGN DECISION METHODS

This section describes probabilistic engineering techniques which are applicable to design decision processes. The attributes of each technique will be discussed as well as the interrelationships of techniques in the overall probabilistic evaluation process. Informational input required for each method is described as well as the informational output of each method. The specific techniques to be discussed are listed below. These will be incorporated into the design decision methodology as appropriate in Phase II.

- (1) Failure modes, effects and criticality analysis
- (2) Event tree analysis
- (3) Fault tree analysis
- (4) Reliability block diagrams
- (5) Uncertainty analysis
- (6) Cost estimating

Each of these techniques supplies a distinct, but necessary element to the completion of a design decision methodology. The first four techniques are basic to quantitative accident analysis and risk assessment. Other quantitative techniques exist which may be utilized in the design decision process and will be evaluated as appropriate in the next phase of this work. However, the first four methods noted above are fundamental to development of a probabilistic design process and are appropriate to utilize due to the increasing familiarity with these techniques within engineering and regulatory organizations. The last two activities provide evaluations of statistical uncertainty and monetary cost, which are necessary to make rigorous and comprehensive design decisions.

These techniques come into use at various stages in the overall design decision process. Figure 3-1 presents a task flow chart for a risk based design approach for a nuclear power plant. This example chose core melt accidents as the source of risk. The chart is structured in terms of data packages. Each box represents an intermediate set of data which is necessary for the completion of the overall risk assessment. The type of analysis and supplementary information which is

FIGURE 3-1 TASK FLOW FOR RISK BASED DESIGN EVALUATION

required at each successive step is also shown on the chart. The flow chart depicts a complete methodology for the evaluation and system designs and their relation to public health.

This type of plant-wide risk based design approach would be the aiming point of the overall study activities and would be pursued as part of the Phase III effort. Phase II would represent only selected activities from those shown on Figure 3-1 and reflect system level conditions.

Design decisions of interest will be made to achieve a cost-effective reduction of overall risk. It is therefore essential to develop a correlation of system performance and reliability to the overall risk of the plant. System performance and function serve as inputs in various places in the flow chart. They are integrated into the accident sequence determination, along with the performance and functional considerations of other systems. The reliability performance of each system is calculated to derive the probability of each accident event sequence. Any probabilistic design decision methodology will utilize an analogous task flow structure although in Phase II it will only entail a portion of the overall process (limited scope). However, the working relationship of analytical techniques to one another will be much the same.

Uncertainty analysis and cost evaluation are not included in the chart. Standard risk assessment does not involve itself with system design costs. Uncertainty analysis is a necessary evaluation to complement a risk assessment, but is usually done as a supporting exercise. These two techniques are essential to a probabilistic design decision methodology. Their place in the overall methodology will also be discussed in the following sections (Sections 3.5 and 3.6).

Event tree analysis and fault tree analysis are the major analytical techniques which will be utilized in Phase II to develop a system level probabilistic design decision process. In a rigorous analysis, these two activities are not independent and separate. Each technique requires several intermediate steps. Fault trees and event trees are continually serving as input for each other. Figure 3-1 shows risk assessment in terms of the intermediate data sets required. This does not detail the relationship between event trees and fault trees. Figure 3-2 presents the fundamental steps of event tree and fault tree analyses and the relationship between them.

FIGURE 3-2 KEY ELEMENTS OF LWR RISK EVALUATION METHODOLOGY

The six techniques to be considered in Phase II are discussed in further detail in the following sections.

3.1 Event Tree Analysis

In support of a risk based design approach, the event tree is the fundamental analytical tool which allows the organization and characterization of potential accidents. Based upon plant design information, potential accident initiating events are identified. These events are defined in a manner to encompass the effects of all realistic and physically realizable potential accidents involving sources of risk. This provides reasonable assurance that all significant causal factors have been accommodated in the analysis and that the results reflect a realistic bounding of potential reactor accidents. Shortly after initiation of event tree analysis, fault tree analysis can commence, to be conducted concurrently. The interrelationship between event trees and fault trees is shown in Figure 3-2.

Once the initiating events have been described, functional event trees are developed. At the same time that the event trees are being constructed, the initial system fault tree analyses can commence as it is apparent that certain safety systems will be required, and their failure potential must be evaluated. The initial event trees develop the functional relationships, among relevant safety systems, into the binary event tree logic structure. When these functional relationships have been established, the events are expanded to depict the response of the various safety systems which may mitigate the effects of a particular accident initiator. These detailed event trees define specific system responses and requirements which are translated into top events for the system fault tree analyses. The fault trees are developed to determine the probability of occurrence of individual system failures.

3.1.1 Accident Initiating Events

Identification and selection of initiating events is a key element in any risk evaluation. In a probabilistic design methodology, there must be a process to identify all the initiating events which require particular system responses. Initiating event definition is a required prerequisite to commencement of the event tree analysis activity.

Various accidents associated with a nuclear power plant may be postulated which could lead to releases of radioactive material from the plant. These potential accidents could involve the reactor core, the spent fuel pit, spent fuel shipping casks, the refueling apparatus, waste gas storage tank, and the liquid waste storage tank. Design decision methodology must be capable of handling all these risk sources.

A second condition for choosing an event (or group of events) as an initiating event or event group is that the event can be characterized by a unique safety system response. The reason for this is that event tree analysis is simplified without loss of significant information if initiating events can be grouped such that safety system response is essentially identical for a given class of events. This approach also ensures that all initiating events are addressed.

3.1.2 Individual Event Sequence Quantification

The end product of the event tree process is a listing of all relevant sequences of events associated with a particular accident initiator. The logic inherent in the structure of the event tree provides the mechanism whereby each of the identified sequences may be quantitatively evaluated. Numerical values for each of the event tree headings are determined primarily by detailed system fault tree analyses. If sufficient detail does not exist to support fault tree analysis, event tree heading quantification can be done by reliability block diagrams or estimates based upon engineering judgment. Details of the system fault tree analyses are discussed in Section 3.3 and reliability block diagrams are discussed in 3.4. In some cases, such as in evaluating the occurrence frequencies of the accident initiators, estimates are taken directly from experience data, as might be the case for common events such as loss of offsite power.

3.2 Fault Tree Analysis

Fault tree methodology is one of several engineering analytical techniques used to predict the reliability or safety of complex systems and functional inter-relationships. Because of its extensive use in the U. S. aerospace industry over

the past 15 years and recent applications in the nuclear industry, the fault tree method has become the analytical approach most relied upon to determine critical system fault paths and their associated probability of occurrence.

The fault tree method is a deductive process whereby the undesired event of interest is postulated and then all possible means for that event to occur are systematically deduced. The fault tree may be thought to provide three important functions:

- (1) A means for a systematic, exhaustive search and identification of all possible events or combination of events which could lead to the occurrence of the identified undesired event.
- (2) A graphical depiction of the analysis process which is a logical representation and historical record of the analytical process.
- (3) A means for evaluation of alternate methods or designs and an assessment of the sensitivity of the analysis results to changes in various input parameters.

The actual manner in which a fault tree is constructed and evaluated is well documented and will not be treated in detail. It can briefly be stated, however, that in the nuclear industry application the fault tree is structured so that the undesired event is directly related to the headings of the event trees. The combination of events that lead to the undesired event are depicted below the top event and are logically linked by branches to the undesired event by standard OR and AND logic gates. Those events that have a more basic cause are developed even further until the development finally leads to the primary causes for which there are failure rate data available. These primary causes appear as circles or diamonds on the bottom of the fault tree and represent its limit of resolution. The fault tree technique has the advantage of locating only those system elements that contribute to the occurrence of the undesired event. Inductively finding these contributory component states (i.e., by a bottom-to-top evaluation) can be a quite tedious and almost unworkable task because of the large number of component states that must be considered, particularly with complex systems. When the fault tree structure is complete, both qualitative

and quantitative evaluation is possible. A qualitative determination may be made of the minimal sets of components or events that, when failed, will cause the system to fail. These sets represent the critical fault paths and give the unique modes by which the top event can occur and represent, in an objective and communicative manner, the causes of system failures. Quantitative evaluations can then be performed to determine the likelihood of the top event and the numerical ranking by importance of individual failure modes.

The fault tree approach is very useful because of the systematic, rigorous approach to fault identification and evaluation. It provides a method for including all significant analysis considerations. Its usefulness can be limited by the unavailability of input data. The fault tree can only be developed and evaluated to a level of resolution commensurate with existing design and failure data. Hence, for events which cannot be readily broken down into contributory fault mechanisms, the fault tree does not provide any additional perspective. In cases where contributing fault mechanisms can be identified but not readily assessed, the fault tree still provides a useful function in focusing all pertinent information on the event of interest, allowing for a comprehensive qualitative or intuitive approach to the problem.

3.3 Failure Modes and Effects and Criticality Analysis

FMECA's are generally the initial step in the reliability analysis of any complex system. FMECA's are logical, systematic examinations of systems and components to identify potential failure modes in the system, their causes, and their effects on higher levels of assembly. Failures critical to operational success can be identified and ranked according to both severity and the probability of occurrence. The purpose of such analysis is to assure recognition of failure modes inherent in the design.

The FMECA provides a structured, disciplined basis for further reliability analysis. It facilitates tracing of failure propagation from the lowest level of assembly to the highest. They provide necessary inputs to event tree and fault tree analysis.

To perform an FMECA, a significant amount of hardware related input data are required. These data include system level drawings, design specifications, parts lists, information pertaining to the operating environment, and any other descriptive information pertaining to systems operation that may be available. Every part for the system or subsystem under study must be listed in the FMECA, all failure modes are identified for each of these parts, and their effects on the established system or subsystem are determined. Failure rates associated with each failure mode are necessary for the analysis, either as rankings or as direct estimates of the failure rate. Critical failure modes are identified in the analysis. Through a quantifying procedure, the criticality of these failure modes can be established and ranked according to severity (i.e., highest criticality number corresponds to most severe effect). The amount of quantitative analysis included in an FMECA can vary, depending on the application.

The output of an FMECA consists of a series of predesigned forms containing the identified failure modes, their causes, and their effects for each part considered. The output may include a criticality and probability assessment or a criticality number calculation used to determine key components of a particular system design.

3.4 Reliability Block Diagrams

In some instances, it may be desirable to determine system failure or success characteristics without utilizing the fault tree process. In these cases, there are two other widely used techniques for the quantification of system failure probabilities. These are:

- (1) reliability block diagrams
- (2) success state diagrams

Both of these techniques provide an estimate of the probability of system success (or failure) and require less detail than fault tree analysis.

Reliability block diagrams entail the representation of system operation in a Boolean Algebra format and are often used to allocate system level reliability

goals to lower level elements. The level of resolution is usually at the system functional level or major system component level. Accident sequences may be constructed using the appropriate Boolean operators.

The success tree diagram is a logic diagram where the top event is defined as system success. When it is more convenient to work with successes than with failure, we use the tree which has as the top event a specified system probability of success. The logic symbols used in the fault tree are also used in the success tree diagram. The success tree diagram is dual to the fault tree. Using the duality principle, the top event is changed into system success by interchanging AND and OR and replacing the inputs by their complements. The quantitative evaluation procedure for a success tree is similar to the fault tree evaluation.

3.5 Uncertainty Analysis

The results of probabilistic analyses often yield a range of values rather than a single value. This could be due to the uncertainties of the input data, modeling technique or the variability of experience. Because measures of safety contain this uncertainty, it is not simply a matter of comparing results to determine which design exhibits a higher degree of safety. One must assess the significance of the differences in the results to identify if the analysis results do indeed indicate a difference in the relative safety of alternative designs.

Another area of potential variance is in the cost estimate of a particular design. Due to the many variables which can impact cost, estimated costs are often only a gauge of the expected area in which actual costs will fall. The uncertainty of these estimates can be used to define the bounds of the costs of a design. As with probabilistic analysis results, it is important to be able to differentiate costs between competing designs.

Various methods exist to test the analytical results for significance (i.e., do the results imply a different safety level or cost?). The simplest techniques are statistical based upon "goodness of fit" tests. To utilize these techniques, it is hypothesized that the probabilistic result (cost estimate) for the alternative design indicates the same result as the baseline design (i.e., not significantly different). Based upon an assumed statistical distribution for the results, a

Kolmogorov-Smirnov or Chi-Square test may be performed. If a significant match is found based on the test statistics, the analysis results can be judged to indicate the safety (cost) of the two designs is not different. If a significant match is not found, then the results would indicate a different safety level in the two designs. A short coming of these tests is that for an evaluation of a model, a sample size must be assumed since none is present. Secondly, the underlying distribution must be assumed to utilize these tests.

Other methods exist which involve comparison of means, ratios of error bands and worst case propagation of errors. There may be an application of Bayesian inference techniques to reduce the uncertainties of the analysis results thereby aiding the determination of the significance of the results.

Whatever the specific method of analysis employed, uncertainty analysis will provide information to allow the analyst to distinguish between the estimated safety and cost properties of alternative designs. This information will support the optimization process in which the alternative which exhibits the optimum mix of acceptable safety, simplicity and cost will be identified.

3.6 Cost Estimating

The unified purpose of the probabilistic design decision methodology is to enable cost-effective reduction of risk. It is essential that cost estimating techniques are integrated into the overall process. The methodology must be developed in a manner which allows cost and risk considerations to compete on an equal basis.

Cost considerations arise from capital costs, installation, backfitting, operation, and maintenance activities. Various techniques exist which enable estimation of these costs in a number of ways. Cost estimates have uncertainties associated with them, much the same as probabilistic analysis. These uncertainties must be calculated and factored into the overall decision process.

The total cost of the system throughout the life of the plant must be considered when making a design decision. In Phase II, various cost estimating methods will be examined for potential application to each contributor to the total cost. The uncertainties associated with each method will be evaluated. A preferred

method will be selected for each cost contributor, based on the reduction of the overall uncertainty.

In calculating the cost, the following contributors will be addressed:

- (1) Capital cost of equipment.
- (2) Installation cost of equipment as near as it can be separated from construction costs of the remainder of the plant.
- (3) Backfitting costs if applicable.
- (4) Operating costs throughout the life of the plant. This includes maintenance, repair, and replacement costs.
- (5) Increased operational costs of other systems due to perturbations caused by system under evaluation.
- (6) Costs due to plant unavailability caused by the system under evaluation.

3.6.1 Scope of Cost Estimates

The cost estimates will be performed at a level of detail commensurate with the system modeling efforts. It will often only be necessary to calculate cost differential between two systems. Auxiliary systems, subsystems and components which are identical to both systems under consideration do not need to be included in the cost estimate.

The preparation of cost estimates will address the following considerations.

- (1) Capital costs will be calculated at the component level, i.e., pump, valve, pipe when required. A complete inventory of components will be made. Costs will be calculated based upon current prices of similar equipment. In instances where components require research and development, this will be noted and the price will be escalated. Capital costs of required auxiliary systems and I&C systems will be charged to the system under evaluation. Capital costs of rooms and buildings required to house these systems will also be calculated.

- (2) Construction costs and installation costs will be based on labor, materials, time, and construction equipment. Installation and wiring of auxiliary systems and I&C systems will also be included. This cost estimate will address the complexity of the system through the installation time and equipment required. Costs of construction materials will also be included. It is the intent to separate the costs attributable to a particular system from those costs which would be accrued in the construction of a nuclear plant regardless of particular system configuration.
- (3) Cost estimates for backfitting will include materials, labor, specialized equipment, and costs of replacement power due to disruption of service.
- (4) Maintenance costs will address frequency, complexity, required personnel, required equipment, duration, and interruption of service.

4.0 PHASE II: DESIGN DECISION METHODOLOGY DEVELOPMENT

The purpose of the Phase II activities is to develop a set of techniques to augment the existing design process at the component and system level in order to optimize cost and safety between alternative system designs. Therefore, the basic approach to Phase II is to identify the decisions which can be made utilizing probabilistic criteria and the appropriate analysis techniques to apply to the design to provide the necessary information in support of those decisions. A new design decision process will be defined including the appropriate analysis techniques. Specific items to be included in the design decision process will be:

- (a) System design criteria (functional and operational)
- (b) System reliability considerations
 - component reliability
 - human error
 - common cause failure considerations
- (c) Design cost implications and estimating
 - construction
 - operation
 - test and maintenance
- (d) Simplicity of design
- (e) Alternative design generation
- (f) Optimum design selection

Figure 4-1 represents an outline of the decision process which will be utilized to develop and apply the methodology. This does not imply a final solution, but does illustrate the important elements of the methodology which must be addressed and included. The method will consist of utilizing the initial design activity as an input, reviewing the functional and operational requirements, and

FIGURE 4-1 SYSTEM DESIGN DECISION METHODOLOGY FLOW CHART

performing the cost estimating and probabilistic analysis. All designs with acceptable safety or better will be subject to the optimization activity.

An important element of the process is the definition of "acceptable safety." In the absence of quantitative criteria, a system will be deemed safe if it meets all its functional and operability requirements and the quantitative level (probability) will be determined by analysis of existing similar designs, the initially proposed design or NRC evaluations. Efforts will be made to characterize acceptable quantitative levels of system safety based upon various system unavailability predictions and the apparent acceptance of that particular design in the current decision process.

Although the initial design information will be an input to the decision process, a feedback feature of the method will provide additional design suggestions based upon the insight gained through the system modeling and evaluation process. This will integrate the designers' knowledge with the evaluators' insight to further optimize the results. One important design feature is simplicity. Part of the feedback and optimization process will be to utilize a measure of simplicity in the design selection criteria. This measure, which will consider modes of operation, measure of redundancy, sophistication of components, and ease of maintenance, test and operation, will be developed as part of the study.

The key to the design optimization process will be to identify a measure of safety in terms of the probability of system failure which can be related to a specific system design. This measure of safety can then be utilized, along with estimated cost and design simplicity, to choose between competing designs. Phase II activities will identify and demonstrate the utility of this measure of safety in the design process.

4.1 Phase II - Methods Development

The specific framework and analytical methods for safety design optimization will be defined by this effort. The output of this activity will identify the decisions to be made, the basis for those decisions and the techniques to be utilized to generate the information to support those decisions. In addition, the questions of quantitative safety design criteria and the uncertainties in system

model evaluation will be addressed so that effective design decisions can be made. The methods development activity will consist of the elements described in the following sections.

4.1.1 Design Decisions

Each design decision which can be enhanced by utilization of probabilistic analysis techniques will be identified. Both system and component level decisions will be addressed. These decisions are expected to be related to the following:

- safety of system design
- reliability of components
- cost of design implementation

4.1.2 Design Criteria Compliance

A basic assumption of the Phase II development activity will be that if existing criteria for system design is met, then the system is an example of an acceptable design. Therefore, each design must meet applicable functional and operability criteria. This activity will define the relationship of design criteria compliance and the possible basis it can provide for definition of an acceptable safety level for systems.

4.1.3 Identification of Analysis Techniques

The expected new information required for the decision process will include quantitative failure (or success) probabilities, cost ranges, measures of design simplicity and significance determination of analysis results. Appropriate analytical techniques will be identified which can be utilized to generate this necessary probabilistic and other design information to support the decision process. Each technique will be associated with the decision(s) it supports.

4.1.4 Design Decision Process

The process will be defined for incorporating the "new" information into the decision process for component selection and system design. The juxtaposition of each decision and its impact on other portions of the process will be identified. Process definition will include when a decision should be made, how it can be made, and what data is necessary.

The analysis techniques will be related to the decision process by describing how they may be accomplished at the various stages of the design process, what data is expected to be available from the design process for the analyses, and how iterations of an analysis can impact the process. Information flow to and from the analysis activity will be identified to assure that the "lessons learned" from the analytical activity provide meaningful input to the decision process.

4.1.5 Scope of Analysis Activity

The issues included in the analysis activity will be carefully delineated. Ideally, inclusion of all secondary failure causes (environment, manufacturing, interfaces) is desirable. However, during the design process a portion of the information necessary to assess all failure impacts is not available. Therefore, it is necessary to identify the scope of the analysis so that it is well understood what is specifically included and excluded. This scoping will define the treatment of component reliability, human error and common cause failures in the analyses.

4.1.6 Level of Design Detail

Another situation which can effect the analysis results as greatly as the scope is the level of detail of the design information available. The expected level of detail will be defined for each stage of the design process and related to the analysis activity. Availability of information such as system flow diagrams, component specifications, system layout drawings, operating procedures and technical specifications will be identified. The

possible impact on the analysis results of the unavailability of specific design information will be identified.

4.1.7 Alternative Design Generation

One major benefit which will accrue from the probabilistic analyses of the system designs is suggested alternative designs. How these alternatives may be generated and evaluated will be described as part of the design decision process. The activity for verification of the functional and operational acceptability of designs which are the result of the analysis process will be identified.

4.1.8 Quantitative Design Criteria

Specific quantitative criteria for various safety functions or system design will be developed. The difficulties in establishing such criteria which in effect is a statement of "how safe is safe enough?" is well recognized. However, some quantitative measure of safety is necessary to provide required guidance and reference points to the decision process. Initial efforts at establishing quantitative design criteria will be directed toward the quantitative evaluation of existing designs and determining the relative acceptance within the current decision process. It is expected that these efforts will be augmented with other experience data and current state-of-the-art developments in setting acceptable limits on safety performance.

4.1.9 Uncertainty Evaluation

Both the probability and cost estimate results for a particular system design will be defined within a range of values due to uncertainties in the data base and the modeling techniques. In order to evaluate if a significant safety or cost difference exists between design alternatives, the uncertainties must be evaluated and compared. Techniques will be identified for determining the significance of the analysis results and related to the design decision process.

4.1.10 Optimization of Factors

The thrust of the Phase II activity will be to provide a decision process for selection of an optimum design in terms of safety, simplicity and cost. This optimization will maximize safety and simplicity while minimizing cost within the existing design and regulation context.

The specific factors utilized in the optimization process will be identified. This will provide a basis for the Phase III activity to modify for consideration of the possible impacts of the design decision process on the design criteria along with plant level design issues.

4.2 Phase II - Methods Demonstration

Design decision methods will be applied to the Surry plant and systems design. Initial cost estimates in today's dollars will be made and the Surry design updated, as applicable, to meet the 1979 version of 10CFR50. The demonstration will address safety related systems in the Surry design including I&C, ECCS, AFWS, and component cooling and service water. The component data from WASH-1400 will be utilized to provide a consistent data base for analysis.

The entire design decision process will be exercised including the generation of alternate designs and the optimization of system designs. Refinements to the design decision methodology will be made as indicated by working the demonstration example. The Phase II method demonstration effort will involve the activities described in the following sections.

4.2.1 WASH-1400 Surry Systems

Safety related systems from the WASH-1400 Surry analysis will be selected to serve as examples for the design decision process demonstration. The systems will be selected on the basis of the ease of applicability of the particular analytical technique being demonstrated. The systems selected will include:

- Low Pressure Injection
- High Pressure Injection
- Safety Injection Signal System
- Containment Spray
- Containment Spray Actuation System
- Auxiliary Feedwater System
- Component Cooling Water

The example systems will be utilized to demonstrate the method on "new" designs and "backfit" designs.

4.2.2 Baseline Designs

A baseline design will be identified for each example. This will be utilized to establish the existing configuration, safety level and cost for comparison purposes. The baseline definition for each system will include:

- Major Component Operating Characteristics
- Equipment Configurations
- Functional Capability
- Operability
- Procedures & Technical Specifications
- Safety Level
- Simplicity Measure
- Estimated Capital Costs
- Estimated Life Cycle Costs

4.2.3 Proposed "New" Design Alternatives

Design alternatives will be identified for selected examples. These design changes will be postulated as though the design process were in progress. The design alternatives will include suggested changes in equipment type, configuration, operation, and function. Each design change will be defined to the level of detail that will support analysis by the previously identified techniques.

4.2.4 Design Alternative Assessment

Each suggested design alternative will be analyzed to determine its level of safety, measure of simplicity and estimated cost. Any promising additional design alternatives generated by this process will be defined and subject to the same scrutiny as the originally postulated alternatives.

4.2.5 Optimize Design

Based upon the analysis results of the example systems, optimum component and system designs will be identified. This optimization will examine the "new" alternative designs and the example baseline designs from the WASH-1400 Surry analysis. The probabilistic analysis and cost estimating results will be utilized to select the optimum mix of safety, simplicity and cost.

4.2.6 "Backfit" Designs

"Backfit" designs will be postulated for selected example systems. The design for the "backfit" will include an apparent qualitative safety improvement. Selection of "backfit" examples will be based in part on recent NRC retrofit suggestions for safety reasons.

4.2.7 "Backfit" Impact

The proposed "backfit" designs will be analyzed for impact on system safety and simplicity and the cost associated with the "backfit" identified. The significance of the impact will be determined as compared to the assessment of the existing level of safety for the example system. Potential alternative "backfit" designs generated as a result of the assessment process will also be examined and "recommendations" to backfit or not will be made based upon the results.

4.2.8 Implication of Design Decision Demonstration

The demonstration activity will have an impact on the development of the design decision method. This impact will result, if required, in a redefinition of the decision process. Any new features affecting component and system design incorporated into the design decision process will be demonstrated.

A number of issues will be examined as a result of the Phase II demonstration. The implications of these items for system level decisions and Phase III activities will be identified. The subjects to be addressed will include:

- Resources required for implementation
- Relationship to regulatory process
- Cost optimization
- Analysis data requirements
- Acceptable level of safety
- Design criteria changes
- Safety importance of systems
- System interface impact on safety
- Context of the safety evaluation
- Potential Phase III activities

4.3 Phase II - Documentation

A final report will be issued at the end of the Phase II activities. The report will document and describe the established design decision methodology. A complete description of the application and demonstration of the methodology to specific system designs will also be provided.

4.4 Phase III Plan

A technical approach and set of tasks for Phase III will be developed. The object of the Phase III activity will be to expand the scope of the design decision process to consider plant level decisions and to determine the safety importance

of various systems and system design criteria. It is intended that the Phase III plan will incorporate information developed during the Phase II activity and will reflect the latest developments and approaches to incorporating a probabilistic based plant-wide design decision process.

5.0 REFERENCES

1. "Code of Federal Regulations," 10CFR Energy Parts 0 to 199, Revised as of January 1, 1979.
2. "The Safety of Nuclear Power Reactors and Related Facilities," WASH-1270, July 1973.
3. "U. S. NRC Regulatory Guides for Power Reactors," December 1978 with continuous update.
4. "U. S. NRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," November 24, 1975.
5. "Technical Report on Anticipated Transient Without SCRAM for Water Cooled Power Reactors," WASH-1270, September 1973.
6. "Reactor Safety Study: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants," WASH-1400, October 1975.
7. "Current Plans of the Regulatory Staff for the Use of Probabilistic Assessment," Paper presented at the ANS Winter Meeting, November 17, 1975.
8. "Probabilistic Methods in Reactor Licensing," Paper presented at the Thermal Reactor Safety Meeting, August 3, 1977.
9. "Risk Assessment Review Group Report to the U. S. Nuclear Regulatory Commission," NUREG/CR-0400, September 1978.
10. Atomic Energy Clearing House, Volume 25 Number 35, August 27, 1979.
11. Nucleonics Week, Volume 20 Number 37, September 13, 1979.

12. "Clinch River Breeder Reactor Plant Safety Analysis Report," Volume 13 Appendix C Amendment 36, March 1977.
13. CRBRP Docket Number 76-5393, "NRC Comments on CRBRP Design Approach," Letter from R. Denise to L. Caffey dated May 6, 1976.
14. "Draft Safe Shutdown Reliability Program Plan for Large Breeders," May 1978.
15. "U. S. NRC Confirmatory Safety Research Program," Paper presented to the Japanese Atomic Research Institute, December 1977.
16. Docket Number 50-346, License Number NPF-3, "Supplement to Reportable Occurrence 78-055," July 21, 1978.
17. "The Role of System Reliability Prediction in Power Plant Design, Power Plant Engineering," February 1977.

DISTRIBUTION:

TID-4500 Distribution UC-78 (197 copies)

M. P. Norin, Chief
Quality Assurance & Standards
& Operational Safety Branch (5)
B-107
U. S. Department of Energy
Washington, DC 20545

J. Carlson
B-107
U. S. Department of Energy
Washington, DC 20545

R. Di Salvo
Probabilistic Analysis Branch
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Lawrence L. Conradi
Energy Incorporated
515 West Harrison
Suite 220
Kent, WA 98031

H. L. Latin
Energy Incorporated
P. O. Box 736
Idaho Falls, ID 83401

Energy Incorporated
1134 Industry Drive
Seattle, WA 98188

4400 A. W. Snyder
4410 D. J. McCloskey
4440 G. R. Otey
4443 H. Jones (50)
4443 A. R. DuCharme
8266 E. A. Aas
3141 T. L. Werner (5)
3151 W. L. Garner (3)
For DOE/TIC (Unlimited Release)