Final Report, September 1980
MIT-NE-241

# GENERIC NUCLEAR SAFETY ISSUES: METHODS OF ANALYSIS

Principal Investigator
Carolyn D. Heising

Prepared by
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Cambridge, Massachusetts 02139

# GENERIC NUCLEAR SAFETY ISSUES: METHODS OF ANALYSIS

Final Report, September 1980
MIT-NE-241

Prepared by

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Cambridge, Massachusetts 02139

Principal Investigator
Carolyn D. Heising

Research Assistants
E.S. Gordon
J. Lepervanche-Valencia
A. Dykes

Prepared for

Nuclear Safety Analysis Center
3412 Hillview Avenue
Palo Alto, California 94304

NSAC Project Managers
E.L. Zebroski
R. Breen

# FORWARD

The accident at Three Mile Island has impacted upon the global perception of nuclear safety in a way formally unprecedented. As a result, government and industry response to the accident has been prompt and comprehensive. This report represents the first of several studies sponsored by the Nuclear Safety Analysis Center (NSAC) that address important nuclear safety issues. In particular, this work concentrates on developing a methodological framework by which utility and regulatory engineers can approach the analysis of safety related problems in a consistent and rigorous fashion.

The goal of this work is to stimulate interest in the establishment of guidelines by which safety analysis can be conducted and also by which they can be evaluated and finally used to guide the decision making process. If such guidelines can be established on a nationwide joint industry-government basis, much can be gained in reaching concensus on important issues whether or not they are currently unresolved. The adoption of logical analytic methods by which to assess licensing and safety issues - not only in theory but in practice - by establishing a consistent framework to be applied in all cases by all actors will help the nation to move toward insuring the safe operation of its nuclear power stations.

It is extremely important that industry and government join together rather than play adversaries in the process of safety decision making. This goal can be reached in significant part by the adoption of on both a federal and industrial level the same analytic framework for the resolution of nuclear safety issues. This report documents such an analytic framework; it is proposed that it or a similar version be considered for use by industry and government in the very near future.

C. D. Heising
Cambridge MA 02139
September 1980

# ABSTRACT

The accident at Three Mile Island (TMI) has led to a thorough re-evaluation of federal safety regulations and utility operating procedures in addition to engineered safety features in plant design. The Nuclear Regulatory Commission has made several recommendations for changes in nuclear plant design as well as several modifications to existing operating facilities as outlined in the "lessons learned" document NUREG-0578. However, many of these recommendations have not been analyzed quantitatively to determine the incremental safety benefit, if any, that may result from their implementation. Utilities who must take the responsibility for implementing these new recommendations are in need of a simplified risk-benefit analytic structure that can provide sound technical backing for positions taken on licensing and design issues.

This study develops a risk-benefit framework for quantitatively analyzing generic nuclear safety issues. Existing reliability analysis methods are used to develop a simplified methodological framework that nuclear engineers can readily apply to safety issues. To provide examples of how this framework can be applied, four issues are separately analyzed:

(i) the anticipated transient without scram (ATWS) issue;

(ii) the containment inerting issue;

(iii) the issue of hydrogen control in PWRs; and

(iv) the issue of the reactor core melt frequency after TMI.

The examples make use of the most recent studies available on each issue and present original results forthcoming from the analyses

performed at MIT. Use of WASH-1400 and recent EPRI-NSAC studies are included. Also, in analyzing the containment inerting problem in BWRs the Vermont Yankee plant was specifically examined. Reference to the included nuclear safety analyses should provide nuclear engineers with detailed examples to guide similar endeavors.

Additionally, a reference handbook on reliability methods designed specifically for nuclear engineers is included as a separate section of this report. The handbook provides the basic information required to acquaint nuclear engineers with the principles of safety reliability analysis. Simple examples on a textbook level are included to demonstrate discussed principles.

## TABLE OF CONTENTS

*Basis for handbook.

## LIST OF FIGURES

Section I

Section II (Handbook)

Section III.A

Section III.B

Section III.C

Section III.D

## LIST OF TABLES

# I. ANALYTIC METHODS FOR THE RESOLUTION OF NUCLEAR SAFETY ISSUES

In this section, analytic methods for the resolution of nuclear safety issues are discussed. First, the methods are discussed in the general context of operations research, the field of research which applies scientific methods to management problems of decision-making. Secondly, application of analytic methods to nuclear regulatory problems is outlined with respect to two broad classes of generic nuclear safety issues: (i) assessment of human reliability factors, and (ii) assessment of engineered safety systems. Characteristics of an analytic framework for generic nuclear safety issue resolution are also defined and described. Finally, a description of a methodological approach for implementing these methods is presented.

## A. Scientific Methods of Decision-Making

In the United States today, the energy debate has led to a subdebate over how decisions regarding the regulation of technology should be made.[1] One perspective is that such decisions should be made apart from the scientific method.[2,3,4] Critics of the scientific method argue that analysis (particularly in cost-benefit application) fails to integrate important aspects of policy questions and leads to erroneous conclusions. Further, they argue that quantitative scientific methods cannot handle ethical issues and instead may obscure them.

The ethical question has been addressed by proponents of the scientific method.[5-8] These proponents contend that ethics and science are not separate entities, and that scientific approaches to issue resolution are, in fact, quite ethical. In defense of cost-risk-benefit analysis, Maxey has pointed out:

> "What is really at issue in risk assessment methodologies is not the propriety or impropriety of putting some callous "dollar value" on human life or injury as a moral judgment of individual worth, much less of economic losses to society as a measure of personal expendability. The public should have long since been confronted with a threefold ethical justification for cost/risk/benefit quantifications (emphasis added), namely:
>
> (1) we are in fact maximizing the value we as a society place on human life when we endeavor to allocate public monies in such a way as to reduce widespread hazards, thereby preventing as much loss of life and protection from injury as possible;
>
> (2) by utilizing this method, we minimize arbitrary, piecemeal, isolated, selective decisions, and instead aim at the most socially responsive and responsible process of decision-making about the cost-effectiveness of finite resources and public revenues;
>
> (3) with this method we have visible and verifiable standards for judging the accountability of elected or appointed officials in their allocation of public monies in a just and equitable manner."'

Further supporting the use of scientific methods in regulatory and technological decision making, O'Donnell has pointed out the need for a cost-benefit perspective in the nuclear regulatory process.[9] Reviewing the trends of past nuclear regulatory policy, O'Donnell showed that new regulatory requirements have produced a dramatic impact on the cost of new nuclear plants:[9]

> "Although escalation contributes a significant portion of the increase in cost, the effect of new regulatory requirements is the predominant factor (Figure 1) and has affected the relative advantage of nuclear vis-a-vis coal-fired electricity production: in 1969, nuclear enjoyed a 26% advantage over coal; in 1978 this advantage had essentially disappeared. Regulatory requirements have resulted in about 50 NRC-licensed systems installed on plants currently entering operation; in 1972, 35 such systems were required (Figure 2). The difference reflects the addition of new safety systems or the upgrading of certain formerly non-safety systems to satisfy new NRC requirements. The list now includes systems such as hydrogen recombiners and safety grade fuel pooling cooling systems not considered in WASH-1400. "

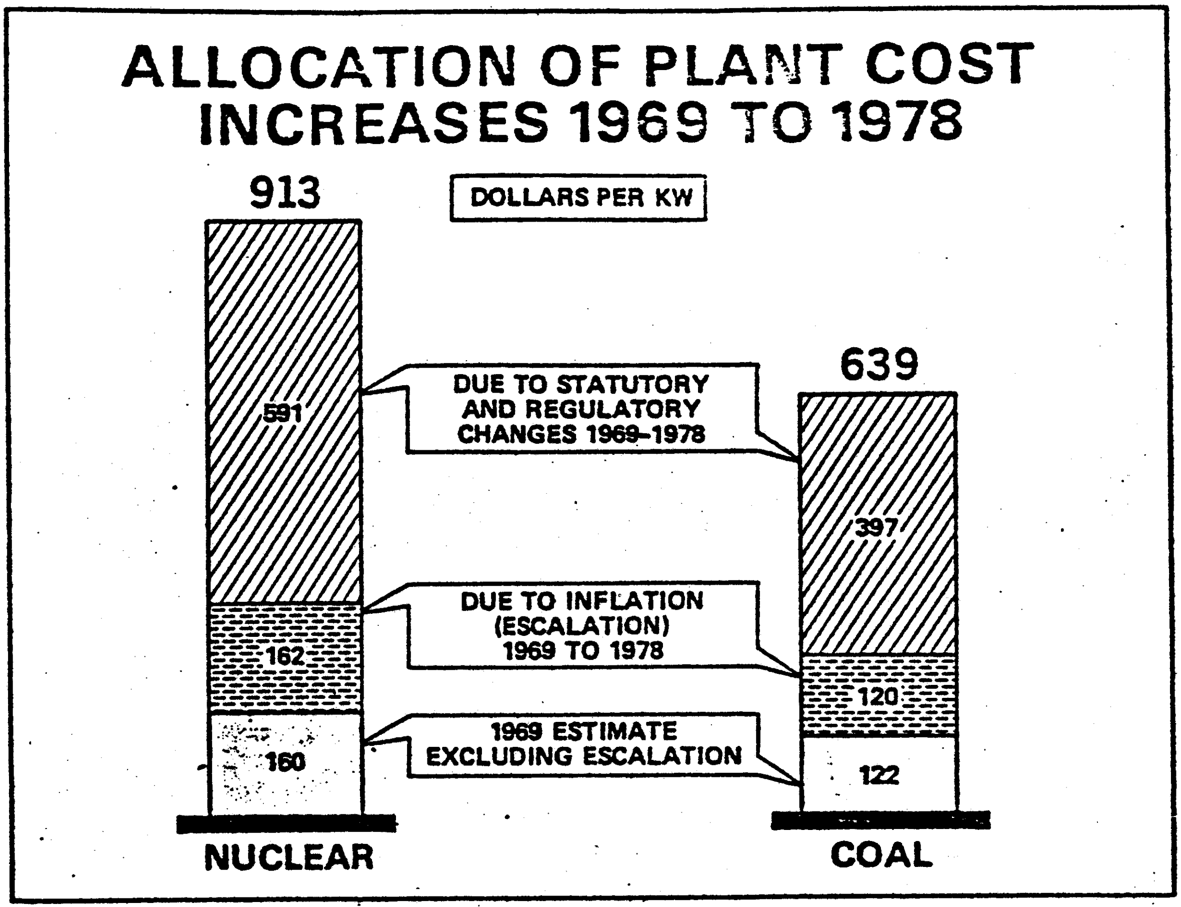


Figure 1 Allocation of Plant Cost Increases (1969-1978).

On the basis of his investigations, O'Donnell suggests that a consistent approach to regulatory and government policy be taken by adopting a uniform standard for cost-benefit analyses.

The history of operations research and the quantitative approach to decision-making, including regulatory decisions, began in the war years of the 1940's. Evolving out of defense planning for distribution and production of wartime equipment and goods, operations research first dealt deterministically and linearly with resource allocation problems. George Dantzig, father of linear programming, in recalling his early memoirs of these times once remarked that his was a linearized world of objective functions subject to constraints of a most unique nature. Since then, the field has broadened and grown becoming both probabilistic and non-linear.

Operations research is applied to problems that concern how to conduct and coordinate the operations or activities within an organization.[10] The approach of operations research is the scientific method. The process begins by carefully observing and formulating the problem and then constructing a scientific typically mathematical model that attempts to abstract the essence of the problem. It is then hypothesized that this model is a sufficiently precise representation of the essential features of the situation so that the conclusions (solutions) obtained from the model are also valid for the real problem. This hypothesis is then modified and verified by suitable experimentation. Thus, in a certain sense operations research also is concerned with the practical management of the organization. Operations research attempts to find the best or optimal solution to the

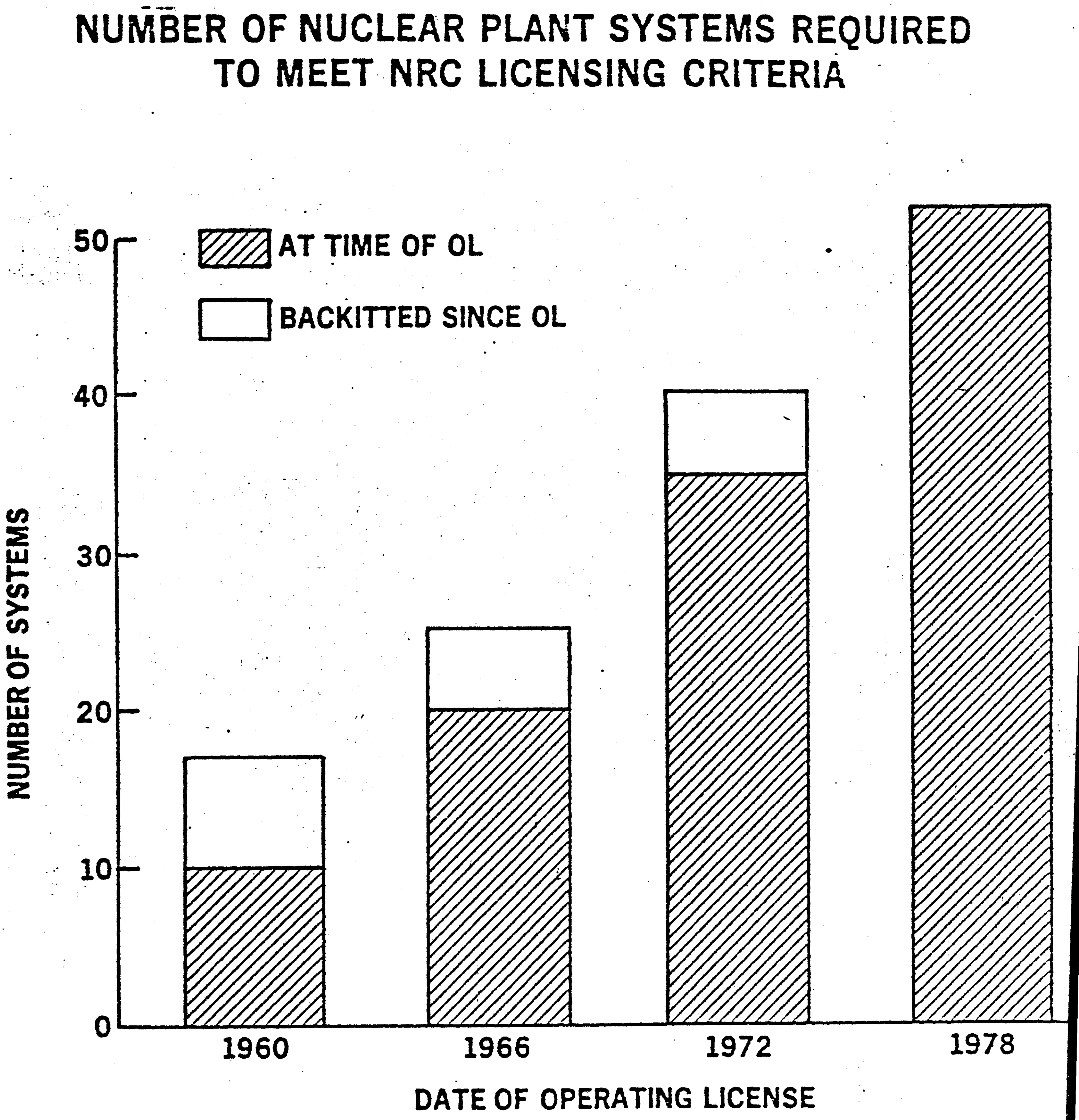


Figure 2 Number of Nuclear Plant Systems Required to Meet NRC Licensing Criteria.

problem under consideration. Rather than being content with merely improving the "status quo", the goal is to identify the best possible course of action. Although it must be interpreted carefully, the "search for optimality" is a very important theme in operations research.

Among the many operations research methods available for deciding between projects, allocating funds, and determining time schedules, the probabilistic approach of Bayesian decision analysis emerges as very promising. The Bayesian perspective of probability asserts that uncertainty reflects a subjective state-of-mind or state-of-knowledge lending itself naturally to an interesting viewpoint on the value of research and development. From this perspective, a decision based on the best available state-of-knowledge is accomplished through the consultation of experts whose concensus opinion provides a basis upon which to act. A major benefit of the explicit quantitative approach is that it synthesizes the opinions of a diverse group of experienced experts more effectively than alternative qualitative approaches.

Explicit numerical representation of expert opinion are a regular input to the evaluation of important problems in the subjective probability approach. A substantial literature exists recommending subjective probability judgment as the most appropriate basis for decision making under uncertainty (see, for example, the work of the Stanford Research Institute's Decision Analysis group[11]). Much of the theoretical basis for this approach comes from the influential work of Reverend Thomas Bayes, a brilliant statistician and thinker who lived in England during the 1750's (see Section II of this report).

Reverend Bayes devised a theorem by which the state-of-information existing prior to the decision or problem at hand could be updated with new information gained either through direct experimentation or upon consultation with experts. The result of the new information combined with the old is called the posterior information and in mathematics is usually a probability distribution of some type. Bayes theorem and its resulting interpretation by others later on provides the foundation upon which the Bayesian approach to probability and statistics is based. That is, Bayesians view probability as a reflection of our state-of-knowledge of a given phenomenon - if perfect information were known, than all uncertainty would vanish. Bayesians assert that statements on likelihood, frequencies and probabilities simply reflect our imperfect state-of-knowledge and that therefore probability is a "state-of-mind" and not a "state-of-matter". From this perspective then, the approach of encoding experts' subjective probability estimates on various important uncertain parameters is theoretically justifiable. Moreover, in common practice the Bayesian approach can be shown to be quite representative of what is actually done in coming to decisions.

The process of probability encoding is one that usually involves intensive interviews of experts by analysts. The SRI Decision Analysis group has established advanced methods for accomplishing the transformation of expert opinion into the quantitative probability distributions required to apply decision analysis methods. Spetzler and Staël von Holstein[12] describe the probability encoding methods currently used by SRI, which are based on several years of experience as well as on evidence from experiments. One such method is based on the use of a probability wheel , which is a disk with two sectors one blue and the other red with a fixed pointer in the center of the disk. The disk is spun finally stopping with the pointer either in the blue or the red sector. A simple adjustment changes the relative size of the two sectors and thereby also the probabilities of the pointer indicating either sector when the disk stops spinning. The subject is asked whether he would prefer to bet either on an event relating to the uncertain quantity, e.g., that next year's production will not exceed x units or the pointer ending up in the red sector. The amount of red in the wheel is then varied until the expert becomes indifferent. When indifference has been obtained, the relative amount of red is assigned as the probability of the event. Use of the probability wheel is called a "reference process" whereby the subject can relate his probability judgment to a tangible reference point that more easily visualizes the encoding process.

In utilizing the Bayesian approach, it is important that the expertise used in the analysis be carefully scrutinized for validity and appropriateness; a high-energy physicist is not a nuclear scientist just as a psychologist is not a sociologist; though the areas are related, the best available expert in one area must be relied upon over others in related but separate areas. Expertise must be incorporated in such a way as to minimize any overt human biases an individual expert may harbor and this responsibility is left to the analysts to ensure.

The use of scientific methods is becoming widely accepted in the area of regulation particularly in nuclear power applications.

Economic methods are used extensively to provide estimates on project potential for benefit. Combined, these approaches can be applied to assess priorities among any set of competing projects. Expert opinion and public value judgments can also be quantitatively included in these analyses to help reflect the best available knowledge and the past and present attitudes of society. Risk acceptability levels and perceptions of benefit may also fluctuate with time; these uncertainties can also be handled quantitatively. The results of these analyses can help guide the regulatory decision making process (they do not replace this process). Problems of a political type such as pressures of suasion by peers and others will still exist; there is no substitute for our present legal regulatory system. However, greater application of quantitative approaches can lead to greater acceptance and credibility for such processes helping to minimize undesirable influences. Properly integrated and exercised, scientific analytic methods can be powerful and useful in the most complicated of situations.

## B. Application to Regulatory Problems

Two broad classes of generic nuclear safety issues have been identified as a result of the accident at Three Mile Island (TMI).[13,14] These include:

1. Assessment of Human Reliability Factors (assessing the Value of Added Improvements in Man-Machine Systems). Given that engineered safety systems are in place and operable, a more important aspect related to the final safe operation of a nuclear power plant concerns the operator's ability to make use of available systems in a correct, efficient and more importantly, a timely fashion. In order to assess

the impact of various proposed equipment and/or operations changes in modifications of the plant (such as inerting Mark I/II reactor containment structures), it is important to ensure that the human reliability aspect is adequately analyzed. Therefore, any analytic framework developed to assess the overall safety impact of a proposed regulatory change must address human reliability directly within the analysis.

2. Assessment of Engineered Safety Systems (assessing the Value of Improvements in the Machine Response to Accidents). Traditionally, this has been the aspect most studied in system safety evaluations. While important, the legacy of TMI has indicated the greater significance of human-machine interactions perhaps indicating that existing safety systems are reliable to the degree that human error predominates. However, the TMI event also revealed some key flaws in machine interactions; the impact of the repairs on the polisher unit in triggering the initial failure of the feed water pumps is perhaps the most interesting; secondarily, the failure of the pressure relief valve (PORV) to close after opening is of interest as well as the later problems related to hydrogen control inside the containment. The NRC has recommended many changes in relation to these issues,[15] and utilities that must evaluate the impact of such changes on plant operations must carefully consider the impact of each. Moreover, a systematic framework for the analysis of such issues is imperative to develop and to consistently follow.

The principal characteristics that an analytic framework for the resolution of nuclear safety issues should possess include:

(1) Basis in Mathematical Theory (Rigorous). Any method used to assess accident/failure probabilities should be statistically valid and tested; likewise, methods used to determine relationships between equipment failures, man-machine interactions, etc. should also be based on known methods. Examples of acceptable approaches include fault or event tree analysis.

(2) Consistancy of Application (Consistant). The approach and steps followed in applying the procedure should be independent of the problem analyzed (though, obviously, the results of the procedures will be dependent on the problem).

(3) Facility for Checking Results and Testing Sensitivity (Scrutability). It is of upmost importance that the framework be easy to comprehend and logically follow. Calculations should be followable to the end result allowing for ease in correction. Scrutiny of results relies on the scrutability of the method employed; the framework for analysis must facilitate this scrutability. (A major criticism of WASH-1400 was its apparent lack of scrutability[16].)

(4) Identify the Accident Sequences and Key Interactions Between Machine-Machine and Man-Machine That Most Impact Upon the Results of the Analysis: Ease of Significant Event Identification (Revealing).

It is imperative that the methodology be able to identify those key interactions between equipment and operators that most impact upon the safety assessment. It is important that the method be able to display these relationships in a clear and understandable manner. Pictorial graphical descriptions can help facilitate such a display (e.g., fault trees can satisfy such a criterion if applied in a careful and thoughtful fashion). Guidelines for the correct application of these methods are needed to help the analyst proceed in the process.

(5) Perform Bounding Procedures to Insure the Assessment of Probabilities is Based on the Best Possible Event Definitions (Completeness).

To a great extent, the assessment of probabilities of event occurrence rely on the careful definition of the event and its relationship to other events. Therefore, it is often necessary to break down the event into its sub-components to try to arrive at those components which facilitate probability definition. Procedures for breaking down events into sub-components include such methods as "influence diagrams", which proceed event tree construction. Such modeling tools can help determine system boundaries, which is often a non-trivial and elusive task and takes place at the beginning of the analysis. Available bounding techniques for model construction are included in the method development section of this report.

(6) Confirm Probability Estimates Based on Empirical Data With Estimates Based on Best Available Engineering Judgment (Intuitive).

A procedure is needed to help establish intuitive confidence in model results; skepticism arises when results are not based on assumptions and data that agree with experience data. The method must therefore be capable of incorporating expert judgment.

In short, the framework should be (1) rigorous, (2) consistent, (3) scrutable, (4) revealing, (5) complete, and (6) intuitive. If all of the above conditions hold, the method itself will be a useful tool in utility-government safety assessments.

## C. Description of a Methodological Approach

The following methodological approach toward analyzing key nuclear safety issues is based in part on a Bayesian perspective of uncertainty. (The Bayesian approach is described in detail in

Section II, part A of this report). The Bayesian perspective is taken to make explicit those assumptions and data values that are based on engineering judgment rather than on experimental evidence since, in many cases, the experimental data is not available. Also, the Bayesian perspective provides a notational mechanism whereby all probability statements are made relative to a given state-of-information S. (Notational definitions are also provided in II.A.) As an aid in the modeling process, the approach suggested here makes use of the technique of influence diagrams, a procedure described in detail by Owen[18] which permits a better representation of the conditionality and dependence relationship between probabilistic variables. Also, the technique is well suited for the later structuring of event and/or fault trees based on the influence diagram.

The methodological approach is now outlined as a series of steps to be followed by the analyst in the process of dissecting and analyzing a nuclear safety problem:

<u>Structuring Models of the Interrelationship Between Key Variables</u>

1. Use influence diagrams to identify the significant events (variables) that affect the problem at hand and identify their interrelationships;
2. Develop an event tree from the influence diagram to indicate different possible routes to a given consequence;
3. Identify the key uncertainties that must be quantified and the relevant conditionality relations;

e.g.,

$$\left\{\begin{matrix}\text{Release of radiation to environment}\\ \text{of major order}\end{matrix} \;\middle|\; \underset{\substack{\uparrow\\ \text{experience}\\ \text{data base}}}{\varepsilon}\right\}$$

$$= \left\{\begin{matrix}\text{overpressurization}\\ \text{of containment}\end{matrix} \;\middle|\; \begin{matrix}\text{gaseous}\\ \text{explosion occurs,}\end{matrix} \quad \varepsilon\right\}$$

$$\times \left\{\begin{matrix}\text{degradation of fuel elements}\\ \text{with release of FP gases}\end{matrix} \;\middle|\; \begin{matrix}\text{reactor core}\\ \text{temperature increase,}\end{matrix} \quad \varepsilon\right\}$$

4. Develop fault trees to estimate the probabilities of events modeled in the event tree;

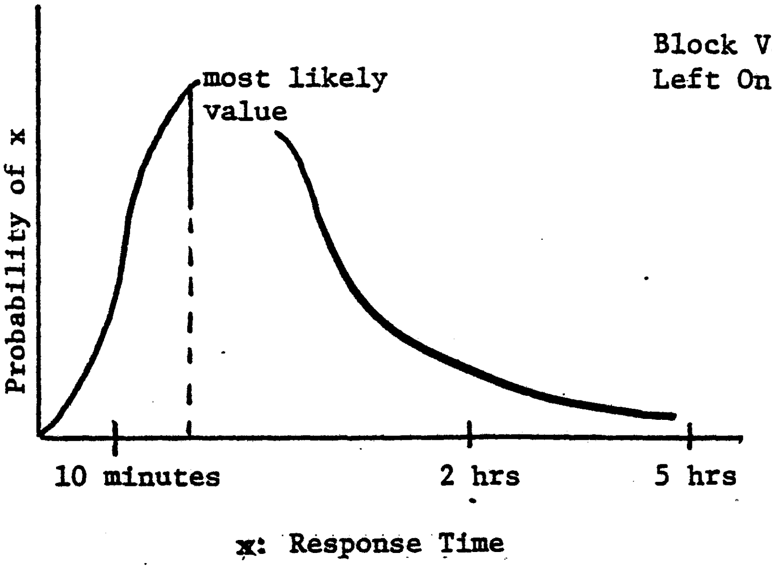
5. In calculating the TOP event probability, use Bayes theorem to calculate conditional probabilities;

6. Determine whether human error or mechanical failure is more likely to dominate in causing failure of systems to respond when needed; if human error predominates, go to 7;

<u>Modeling of Human Error: Additional Analysis</u>

7. Probability estimates of human reliability may be estimated on a plant-by-plant basis after acquaintance with plant personnel and operations procedures are known; advice from human reliability experts with this information can also be used to encode probability estimates. Further analysis involves construction of "human response functions" (step 8);

8. Human response functions can be determined where upper and lower limits on such functions can be estimated for various tasks that require performance, e.g.:



Block Valve Closed or ECCS Left On (After Failure of PORV)

The above hypothetical distribution measures the probability that the failure of the PORV is correctly identified and the proper response is determined in that the block valve is finally closed or the ECCS is left on  i.e., that at least one of the many alternative  correct actions is taken in the indicated time period. (In generic studies, allowance must be made for possible improvement with time in human response functions.)

Sensitivity Studies

9. After determining the role of human error in the problem, additional sensitivity studies are useful in establishing error bounds on results and the degree of confidence expressed in the "most likely" or "best" estimate.

Presentation of Results

10. Graphical and/or pictorial representation of study results should include the degree of uncertainty and/or error; use of probability vs consequence graphs is one of the most common methods of result presentation; cost-benefit ratios are another method with respect to some baseline value.

An example of the use of influence diagrams in structuring the interrelationship between key variables is shown in Figure 3 for the hydrogen control problem in the event of a class 9 accident. From this diagram, event trees may be constructed which map the possible routes available that lead to the top and final event: "release of radiation to the environment of major order". The influence diagram helps the analyst determine the major variables of importance and the chronological sequence of events that can lead to their occurrence. For example, the event of a gaseous explosion can take place if either a hydrogen and/or steam explosion were to occur; the question of the independence of the separate events "hydrogen explosion" and "steam explosion" can be identified in the diagram as to whether or not an arrow should be drawn between the two events. The assumption placed on the link between the two events will later influence calculations of the frequency of a gaseous explosion.

Use of the general framework described here for the structuring of a safety analysis is applied in Section III.B to the containment inerting problem. Variations of the general framework are applied to other examples in Section III. Strict adherence to the ten steps described above is not necessary to achieve a well performed analysis. However, a well performed analysis will usually exhibit at least the following three characteristics:

(1) Structured Model of Event Relationships;

(2) Identification of Key Uncertainties; and

(3) Sensitivity Study/Error Analysis.

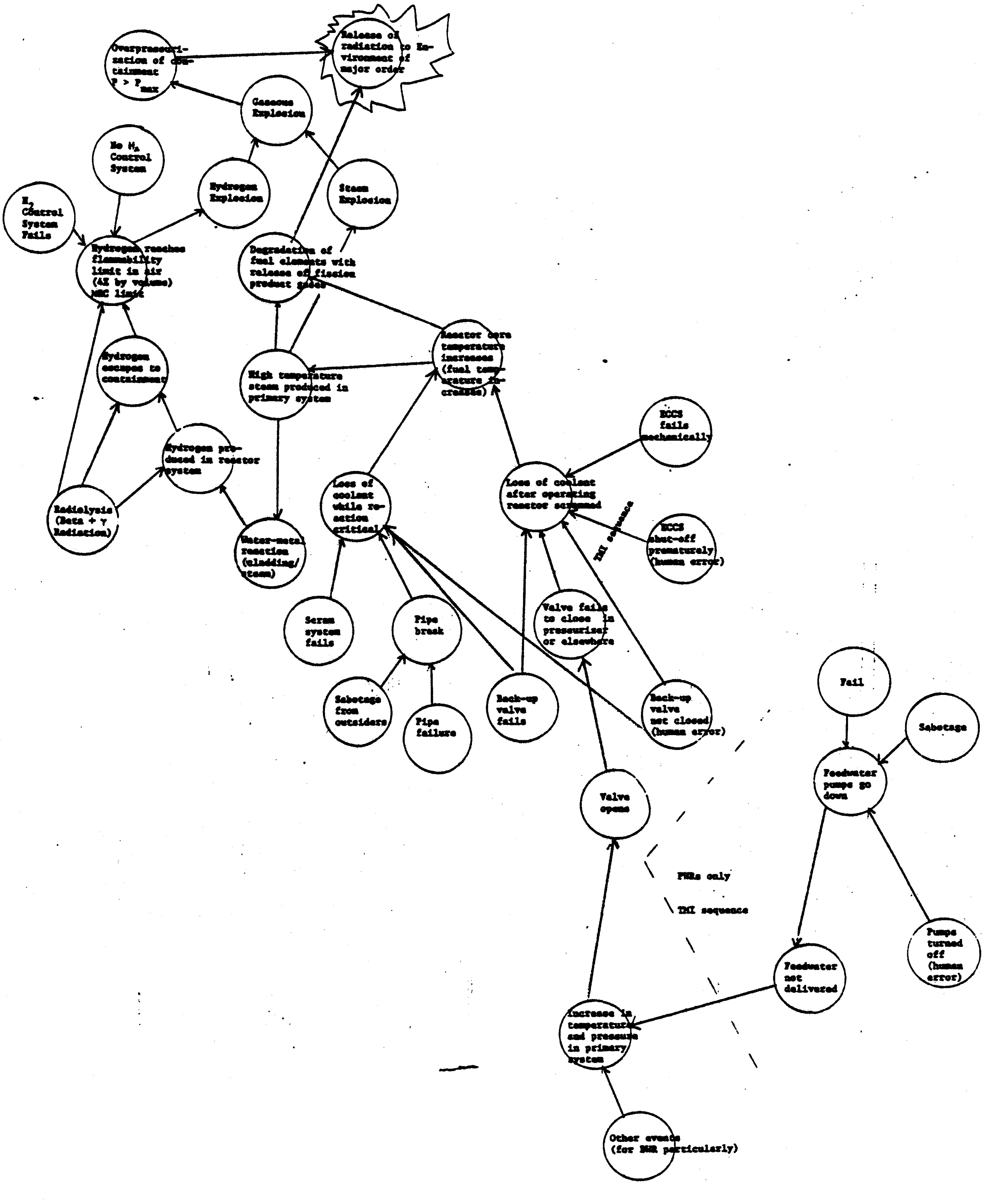

Overpressurization of containment $P > P_{max}$
Release of radiation to Environment of major order
Gaseous Explosion
No $H_2$ Control System
Hydrogen Explosion
Steam Explosion
$H_2$ Control System Fails
Hydrogen reaches flammability limit in air (4% by volume) NRC limit
Degradation of fuel elements with release of fission product gases
Reactor core temperature increases (fuel temperature increases)
Hydrogen escapes to containment
High temperature steam produced in primary system
ECCS fails mechanically
Hydrogen produced in reactor system
Loss of coolant while reaction critical
Loss of coolant after operating reactor scrammed
TMI sequence
Radiolysis (Beta + γ Radiation)
Water-metal reaction (cladding/steam)
ECCS shut-off prematurely (human error)
Scram system fails
Pipe break
Valve fails to close in pressurizer or elsewhere
Sabotage from outsiders
Pipe failure
Back-up valve fails
Back-up valve not closed (human error)
Fail
Sabotage
Feedwater pumps go down
Valve opens
PWRs only
TMI sequence
Pumps turned off (human error)
Feedwater not delivered
Increase in temperature and pressure in primary system
Other events (for BWR particularly)

Figure 3 Influence Diagram of Hydrogen Control Problem in the Event of a Class 9 Accident.

# II. RELIABILITY AND RISK ANALYSIS METHODS

## A. Introduction to Probability Theory

### A.1 Viewpoints on Probability

Before the basic equations and concepts of probability theory are dealt with, it is perhaps more important to begin first by introducing three different ways of looking at probability and uncertainty. Each way of looking at probability produces differences in the way in which probabilities are represented and manipulated and also influences the engineer in the way in which data is used to derive probability estimates. There are at least three ways in which probability and uncertainty are viewed by statisticians. These perspectives are known as "schools-of-thought" and are often named after the first person who conceived of them. These schools are:

(i) the CLASSICAL school;

(ii) the BAYESIAN (or SUBJECTIVIST) school; and

(iii) the FISHERIAN school.

To begin with, there is the traditional (or classical) school-of-thought that claims that uncertainty is a state of nature; i.e., that uncertainty is a property of matter and living things. So, just as an object has a measurable weight, shape and color, the classicists claim an object also has a measurable uncertainty factor known as a probability. An example is a coin which, upon being tossed, either produces a head or a tail. The classicists claim that the coin has a property of uncertainty or a probability of 0.5 (if fair) of being either in a heads or tails state. A different coin might exhibit a different probability of being in these states just as it might exhibit a different weight, shape or color.

The Bayesian school-of-thought on uncertainty and probability is often called the subjectivist school (see Ref. [5]) because instead of viewing uncertainty as a property of matter, uncertainty is viewed as a human perception that does not reflect nature so much as it does cognitive learning processes. Whereas classicists see uncertainty as a state-of-nature, Bayesians see uncertainty as a state-of-mind. Thus, since learning and experimentation can often expand horizons and contribute to clarification, uncertainty can actually be reduced through the learning process. The concept of "up-dating" probability estimates as new information becomes learned is thus a central tenet of the Bayesian school.

Finally, the Fisherian school claims that uncertainty resides neither in the object (observed event) upon which data is based nor in the data itself (perception of the viewer), but in the mechanism that transforms the unobservable into the observable. In a sense, then, Fisherians see probability as a measurement of a state-of-transformation from a certain "true" data point to a certain "observed" data point. Both true and observed data are certain; the uncertain quantity is the vector difference between them.

Of the three schools mentioned here, the most prevalent is the classical school closely trailed by the Bayesian followed at a much further distance by the Fisherian school. However, the Bayesian school is becoming more widely accepted and may in fact become the dominant theory of statistics in the future. In what follows, both the classical and Bayesian approaches will be utilized and noted. Also, after presenting some basic probabilistic notions, these schools-of-thought will be returned to and more specific details given (see A.4).

## A.2 Definitions and Notation

Some of the more relevant properties of probabilities are described here particularly for the use of Bayes theorem, one of the more important theorems of probability theory. Beginning with some notational definitions, we move on to define simple properties of probabilities, then moving on to Bayes theorem in both classical and inferential notation.

Let A and B be events; then P(A) and P(B) are the probability of these events. Some simple probabilistic properties are as follows: (U ≡ union, "OR"; $\cap$ ≡ intersection, "AND")

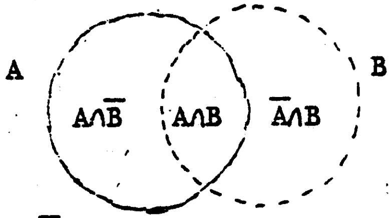
(1) For A and B disjoint; i.e., if $A \cap B = \emptyset$ (the empty set), then:

Addition $\quad P(A \cup B) = P(A) + P(B) = P(B) + P(A)$

(2) For A and B not necessarily disjoint:

$$P(A \cup B) = P(A)+P(B) - P(A \cap B)$$

where



Converse $\left\{ \begin{array}{l} P(\bar{A}) = 1 - P(A) \\ P(\bar{B}) = 1 - P(B) \end{array} \right.$

Identity $\left\{ \begin{array}{l} P(B) = P(A \cap B) + P(\bar{A} \cap B) \\ P(A) = P(B \cap A) + P(\bar{B} \cap A) \end{array} \right.$

Conditionality [10]: Let A and B be two events such that $P(A) > 0$. Then the conditional probability of B given A written $P(B|A)$ is defined to be:

$$P(B|A) = \frac{P(B \cap A)}{P(A)}$$

If $P(A) = 0$ the conditional probability of B given A is undefined.

Independence [10]: Two events A and B are independent if and only if $P(A \wedge B) = P(A)P(B)$

Definition: $P(B|A) = P(B)$ if A,B independent

Example: Suppose that the population of a certain city is 40% male and 60% female. Suppose also that 50% of the males and 30% of the females smoke. Find the probability that the smoker is male.

Let M denote the event that a person selected is male and let F denote the event that the person selected is a female. Also, let S denote the event that the person selected smokes and let N denote the event that he does not smoke. The given information can be expressed as $P(S|M) = 0.5$, $P(S|F) = 0.3$, $P(M) = 0.4$ and $P(F) = 0.6$. The problem is to compute $P(M|S)$. By the definition of conditionality given above:

$$P(M|S) = \frac{P(M \cap S)}{P(S)}$$

Now $P(M \cap S) = P(M)P(S|M) = (0.4)(0.5) = 0.20$ so the numerator can be computed in terms of the given probabilities. Since S is the union of the two disjoint sets $S \cap M$ and $S \wedge F$, it follows that:

$$P(S) = P(S \cap M) + P(S \wedge F)$$

Since $P(S \wedge F) = P(F)P(S|F) = (0.6)(0.3) = 0.18$, we see that

$$P(S) = 0.20 + 0.18 = 0.38.$$

Thus

$$P(M|S) = 0.20/0.38 \approx 0.53$$

The problem discussed in this example is a special case of the following general situation. Suppose $A_1$, $A_2$ ... $A_n$ are n mutually disjoint events with union $\Omega$. Let B be an event such that $P(B) > 0$ and suppose $P(B|A_K)$ and $P(A_K)$ are specified for $1 \leq K \leq n$. What then is $P(A_i|B)$? To solve this problem, note that the $A_K$ are disjoint sets with union $\Omega$ and consequently

$$\begin{aligned} B &= B \cap (A_1 \cup A_2 \cup A_3 \ \dots \ \cup A_n) \\ &= (B \cap A_1) \cup (B \cap A_2) \cup \ \dots \ \cup (B \cap A_n) \end{aligned}$$

Thus, $$P(B) = \sum_{k=1}^{n} P(B \cap A_K)$$

But $P(A_K \cap B) = P(A_K)P(B|A_K)$

so we can write (from the conditionality relation above):

$$P(A_i|B) = \frac{P(A_i \cap B)}{P(B)}$$

and substitute in our relationship for $P(B)$ and $P(A_i \cap B)$:

$$P(A_i|B) = \frac{P(A_i)P(B|A_i)}{\sum_{k=1}^{n} P(B \cap A_K)}$$

$$\rightarrow \qquad P(A_i|B) = \frac{P(A_i)P(B|A_i)}{\sum_{k=1}^{n} P(A_K)P(B|A_K)}$$

This formula is Bayes Theorem and finds frequent application both in probability theory in general and in nuclear safety applications.

Example of Bayes Theorem in Application [10]:

Suppose there are three chests each having two drawers. The first chest has a gold coin in each drawer, the second chest has a gold coin in one drawer and a silver coin in the other, and the third chest has a silver coin in each drawer. A chest is chosen at random and a drawer opened.

(a) If the drawer contains a gold coin, what is the probability that the other drawer also contains a gold coin? [Note: the correct answer is not 1/2].

| CHEST (1) | CHEST (2) | CHEST (3) |
|---|---|---|
| G | G | S |
| G | S | S |

G = Gold coin; S = Silver coin

(b) What is the probability that the second drawer has a silver coin given the first had a gold coin?

Solution:

Construct a probability space where the events $A_1$, $A_2$ and $A_3$ correspond respectively to the first, second, and third chest being selected. These events are disjoint (mutually exclusive) and their union is the whole space $A = (A_1 U A_2 U A_3)$ since exactly one chest is selected. We also assume that since the chests are being drawn at random, each chest is equally likely to be chosen so $P(A_1) = P(A_2) = P(A_3) = 1/3$. Now, let B be the event that the coin observed is gold. Then: $P(B|A_1) = 1$, $P(B|A_2) = 1/2$, and $P(B|A_3) = 0$.

(a) The problem asks for the probability that the second drawer has a gold coin given that there was a gold coin in the first. This can only happen if the chest selected was the first chest, so the problem is equivalent to computing $P(A_1|B)$:

$$P(A_1|B) = \frac{P(A_1)P(B|A_1)}{P(A_1)P(B|A_1)+P(A_2)P(B|A_2)+P(A_3)P(B|A_3)}$$

$$= \frac{(1/3)(1)}{(1/3)(1)+(1/3)(1/2)+(1/3)(0)} = \frac{1/3}{1/3+1/6}$$

$$= \frac{1/3}{1/6} = 6/9 = 2/3$$

(b) The second half asked what the probability would be of the second drawer having a silver coin given the first had a gold. This can only happen if chest (2) is chosen, so we must compute $P(A_2|B)$:

$$P(A_2|B) = \frac{P(A_2)P(B|A_2)}{P(A_1)P(B|A_1)+P(A_2)P(B|A_2)+P(A_3)P(B|A_3)}$$

$$= \frac{(1/3)(1/2)}{(1/2)} = 1/3$$

## A.3 Inferential Notation

Inferential notation is a nomenclature developed by Howard et al. [12] to better describe and utilize the Bayesian viewpoint of statistics. The basic concept of inferential notation is that every probability assignment is conditional on some state-of-information, which we may call S. Then $\{A|S\}$ = probability of A given state-of-information S. If x is a random variable, then $\{x,y|S\}$ is the joint density function of x and y. The conditional density function of x given y is $\{x|y,S\}$. A particularly important state-of-information brought to any problem is the prior experience defined $\varepsilon$. Thus, $\{A|\varepsilon\}$ is the prior probability of the event A and $\{x|\varepsilon\}$is the prior probability density of the variable x. Bayes' Theorem expressed in inferential notation is

$$\{x|y,S\} = \frac{\{y|x,S\}\{x|S\}}{\{y|S\}} = \frac{\{x,y|S\}}{\{y|S\}}$$

where $\{x|S\} = \int_y \{x|y,S\}\{y|S\}$ is called the expansion function which allows knowledge about random variable x to be expressed in terms of knowledge about another variable y. The expected value or expectation of the random variable x given state-of-information S is defined as: $<x|S> = \int_x x\{x|S\}$.

Inferential Notation: Probability and Statistics Definitions

$A$ = event

$\{A|S\}$ = probability of A given state-of-information S

$x,y$ = random variables

$\{x|S\}$ = density function of x given S

$\{x,y|S\}$ = joint density function of x and y

$\{x|y,S\}$ = conditional density function of x given y

$\{A|\varepsilon\}$ = prior probability of event A

$\{x|\varepsilon\}$ = prior probability density function of random variable x

$<x|S>$ = expectation (expected value or mean) of random variable x given state-of-information A

${}^v<x|S>$ = variance of x

Operations

$$\{x|y,S\} = \frac{\{y|x,S\}\{x|S\}}{\{y|S\}} \qquad \text{Bayes' Rule}$$

$$\{x|S\} = \int_y \{x|y,S\}\{y|S\} \qquad \text{Expansion}$$

$$<x|S> = \int_y <x|y,S>\{y|S\} \qquad \text{Expectation}$$

Example: The Coin-Tossing Problem Re-Visited

Let H represent the event of getting a head on the next coin toss and $\phi$ be the fraction of heads observed after a large number of tosses n. Since $\phi$ is an uncertain quantity, the probability density function of $\phi$ is defined $\{\phi|\varepsilon\}$. This is also called the prior distribution on $\phi$ which encodes all prior information known about the coin.

To express H in terms of $\phi$, we use the expansion function defined earlier: $\{H|S\} = \int_\phi \{H|\phi,S\}\{\phi|S\}$. Given we know $\phi$, then $\{H|\phi,S\} = \phi$ would be the best estimate we could make on the probability of getting a head on the next toss. Thus, $\{H|S\} = \int_\phi \phi\{\phi|S\} = <\phi|S>$ from the definition of expectation given above, or the expected value of getting a head on the next toss is $\phi$ based on our state-of-information S.

Learning from Observations/Updating the Prior Distribution

The question arises concerning how knowledge of $\phi$ is changed by the observation of additional tosses. Suppose an individual observes an additional head on toss (n+1). From Bayes' Theorem, this new information effects the new estimate of $\phi$ as follows: $\{\phi|H\}=\{H|\phi,S\}\{H|S\}$. We can think of $\phi$ as the mean value $\mu$ with distribution $\eta(\overline{x},\sigma^2/n)$ as described by the Frequentist/Fisherian notation. But $\{H|\phi,S\}=\phi$ from our earlier discussion, and $\{H|S\}=<\phi|S>$, i.e., the "best guess" we can make about the probability of getting a head on the next toss is the expected value, or mean, of the $\{\phi|S\}$ distribution. Thus, the pdf for $\phi$ given an observation of an additional head "H" is: $\{\phi|H,S\}=[\phi\{\phi|S\}]$ $<\phi|S>$ where $\phi$ is simply a random variable, $\{\phi|S\}$ is the probability distribution function on $\phi$, and $<\phi|S>$ is the expected value (or mean) of $\{\phi|S\}$. The pdf for $\phi$ given the observation of an additional tail "T" is:

$$\{\phi|T,S\} = \frac{(1-\phi)\{\phi|S\}}{1-<\phi|S>}$$ where $(1-\phi)$ is a line with slope -1.

Quantititative Example

Suppose we are given a prior density function for the coin-tossing problem with mean $<\phi|S>=0.5$, $\sigma=0.05$ and prob $\{.45\leq H\leq .55\}=.67$. Our prior estimate of $\phi$, the fractional number of heads, is $<\phi|S>=0.5$. Now assume that 100 tosses of the coin are thrown and 54 tosses turn up heads. Suppose further that we choose to describe the prior distribution by a beta distribution (this will aid us because the posterior distribution will also be a beta function).* This is done by equating the mean $r'/n'=.5$ and the variance $\sigma^2=0.0025=((r'/n')(1-r'/n'))/(n'+1)$. Solving, we find $r'=50$, $n'=100$. Having thus encoded the prior, the

*Beta and gamma functions are often used in Bayesian estimates of the prior and posterior because they are conjugate families of distributions; when the prior is a beta or gamma function, the posterior will be also. (See an application of the gamma distribution in Apostolakis and Mosleh, "Expert Opinion and Statistical Evidence: An Application to Reactor Core Melt Frequency", Nuclear Science and Engineering, Vol. 70, pp. 135-149 (1979).)

posterior is found by adding the number of heads observed r=54 to the prior parameter r'=50. Then, the number of tosses n=100 are added to the prior parameter n'=100. Thus, r"=r'+r=104; n"=n'+n=200. The posterior is a beta function with mean r"/n"=104/200=0.52 and variance $\sigma^2$=(r"/n")(1-r"/n")(n"+1)=(.52)(.48)/201=.0012.

## A.4 Viewpoints on Statistics Revisited

### 1. The Frequentist (or Classical) School

Define a random variable x to be described by a normal distribution with mean $\mu$ and variance $\sigma^2$; then we can use the following notation to signify this relationship:

$$\underset{\substack{\uparrow\\ \text{random}\\ \text{variable}}}{x} \sim \underset{\substack{\uparrow\\ \\ \\ \text{normal distribution}}}{\eta} \; (\underset{\substack{\uparrow\\ \text{mean}\\ \text{(deterministic)}}}{\mu}, \sigma^2) \longleftarrow \text{variance}$$

Suppose we observe n values $x_i$, i=1...n where each $x_i$ is a random variable; then the observed average $\bar{x}$ is a random variable with probability distribution function as follows:

$$\bar{x} \sim \eta \; (\mu, \frac{\sigma^2}{n}) \text{ where, as } n \to \infty,$$

$\bar{x} \sim \eta \; (\mu, 0)$ or, as the number of observations increases, the observed mean value $\bar{x}$ is equal to the idealized "true" value of the mean $\mu$, i.e.,

$$\lim_{n \to \infty} \bar{x} = \mu \text{ where } \bar{x} = \sum_{i=1}^{n} \frac{x_i}{n} = \hat{\mu} \text{ is the estimation}$$

for the true value of $\mu$ and is the simple arithmetic average of the observation values. The expected penalty for using $\hat{\mu} = \bar{x}$ as the estimation for the "true" value of the mean $\mu$ is:

$$E(\hat{\mu}-\mu)^2 = \frac{\sigma^2}{n}$$

(Gauss showed that the choice of $\hat{\mu} = \bar{x}$ as the best estimation for the mean $\mu$ minimizes $E(\hat{\mu}-\mu)^2$ for every value of $\mu$. However, Stein's Paradox describes cases where this might not be true: see Efron, B., et al., "Stein's Paradox in Statistics", Scientific American, 1970).

To the classicists, the variable which is considered to hold the quality of "uncertainty" is the $\bar{x}$ variable; the true value of the mean, $\mu$, or the true frequency of an event/object/etc., is a deterministic value known with absolute certainty. This viewpoint corresponds to a philosophy that uncertainty is a property of objects in nature - just like a coin might have a weight, mass and color, to the classicists, it also has a property of uncertainty that describes it; i.e., if it is a fair coin, the value assigned to the coin which describes it is 1/2. Thus, absolute certainty exists as a concept to classicists in that probability becomes a tangible, measureable quality such as mass, shape or color.

One last note with respect to the classicists; in the 1930's, J. Neyman developed the concept of confidence intervals. For a normal distribution, the probability that the true value ~~for~~ $\mu$ lies within 95% of the observed mean value $\bar{x}$ was established as:

$$\text{Prob}\{\bar{x} - 2\sigma/\sqrt{n} \leq \mu \leq \bar{x} + 2\sigma/\sqrt{n}\} = .95$$

The interval $[\overline{x} - 2\sigma/\sqrt{n}, x + 2\sigma/\sqrt{n}]$ is the "95% confidence interval" for $\mu$.

<u>Example</u>: Suppose $n=4$, $\sigma=1$ and $x_1=1.2$, $x_2=0.3$, $x_3=0.7$, $x_4=0.2$. Then $\overline{x}=(1.2+0.3+0.7+0.2)/4=2.4/4=.6$ and the 95% confidence interval for $\mu$ is $[-.4, 1.6]$.

What both Fisherians and Bayesians find controversial about this is whether the process of inference used by scientists/engineers in reasoning from noisy data to models is a process that can be handled by the classical philosophy. For example, the proper interpretation of a confidence interval is that it covers the true value of $\mu$ with a given frequency (say 95%) in a long series of independent repetitions of $\overline{x} \sim \eta(\mu,\sigma^2/n)$. Without a long series of independent repetitions available or possible the relevance of the classical approach is perhaps questionable.

## 2. <u>The Fisherian School</u>

A less well known school of statistical thought started by Ronald Fisher was very popular in the 1940's, although less so today. A critic of the classical perspective, Fisher proposed a novel theory:

> "Randomness lies neither in the data $\overline{x}$, or in the 'true value' of the data $\mu$: <u>Rather it lies in the mechanism which transforms the unobservable $\mu$ to the observable $\overline{x}$</u>"

Fisher argued that being concerned about what happens when infinitely many $\overline{x}$ values are randomly generated from $\eta(\mu,\sigma^2/n)$ with $\mu$ fixed is not important. Since there is <u>only</u> one observed value of $\overline{x}$ in any single inference problem, the inference process should concentrate on just that observed value. Fisher was equally hostile toward the Bayesians because he was familiar with problems in agriculture and genetics where assessment of prior distributions is very difficult. Since he didn't like either approach he developed his own by introducing something called "normal noise", written $\varepsilon$. According to Fisher, uncertainty lies in the normal noise $\varepsilon$ variable and not in $\mu$ or $\bar{x}$. Thus, he derived:

$$\bar{x} = \mu + \varepsilon, \ \varepsilon \sim \eta(0,\sigma^2/n)$$

which can be shown geometrically to be the sum of two vectors. Assuming $\mu$ is a known deterministic quantity, the uncertainty is found in $\varepsilon$ so when added to $\mu$ renders the observed fuzzy data point $\bar{x}$. Since $\varepsilon \sim \eta(0,\sigma^2/n)$, then $-\varepsilon \sim \eta(0,\sigma^2/n)$ because of symmetry of the normal distribution about its mean. Thus Fisher showed:

$$\mu|\bar{x} \sim \eta(\bar{x},\sigma^2/n)$$

The value of the true mean $\mu$ conditioned on the observed point $\bar{x}$ is a normal distribution with mean $\bar{x}$ and variance $\sigma^2/n$. (As will be shown, this corresponds to a Bayesian interpretation assuming a flat prior distribution on $\bar{x}$.) The corresponding confidence interval is:

$$\text{Prob}\{\bar{x} - 2\sigma/\sqrt{n} \le \mu \le \bar{x} + 2\sigma/\sqrt{n}|\bar{x}\} = .95$$

which Fisher called a "fiducial" (trustworthy) probability statement, meaning it is obtained as an average over the random transformation mechanism. The ficudial statement is now considered a form of Bayesianism or just plain wrong. However, Fisher's ideas on conditional inference and randomization are still very much in vogue.

### 3. The Bayesian School

Nuclear engineers have found the statistical concepts developed in 1750 by the Reverend Thomas Bayes to be most appropriate for the problems faced in assessing the safety of nuclear systems. This situation arises because of the limited data available from the testing of reactor systems and components such that professional engineering judgment must be relied upon to establish probability estimates. However, in most situations, engineering judgments can be used to establish a range on probability estimates with a high degree of accuracy. For example, consider the question of establishing a range on the probability that your car won't start when you go to use it tomorrow morning; a range of $10^{-2}$ - $10^{-4}$/demand seems a reasonable estimate of the limits on this probability based on experience with the system. The Nuclear Regulatory Commission (NRC) uses "engineering judgment" routinely in establishing safety guidelines and regulations. Engineering judgment combined with quantitative analyses based on that judgment is believed to be one of the best methods for nuclear safety analysis. The Bayesian school of statistics provides the theoretical foundation by which this can be done.

To compare the Bayesian school with that of the Frequentists and Fisherians, suppose that μ itself (i.e., the "true" mean value) is considered a random variable known to have a normal distribution with mean "m" and standard deviation "s". Then:

$$\mu \sim \eta(m,s^2)$$

where m and $s^2$ are constants known to the analyst. Now suppose an experiment is run and a particular value for μ is found, say $\bar{x}$, the arithmetic mean of the experimental data. That is, suppose $\bar{x}$ is considered an unbiased, normally distributed estimator of μ. Then:

$$\bar{x}|\mu \sim \eta(\mu,\sigma^2/n)$$

where $\bar{x}|\mu$ emphasizes that the distribution is conditional upon the particular value taken by the random quantity μ. This last statement is to be compared to the classicist's statement $\bar{x} \sim \eta(\mu,\sigma^2/n)$. Using Bayes' theorem, it is possible to show that the conditional distribution of μ given $\bar{x}$ is a function of m, $\bar{x}$, $s^2$, $\sigma^2$ and n:

$$\mu|\bar{x} \sim \eta(m + C(\bar{x}-m), D)$$

where $C = \dfrac{n/\sigma^2}{1/s^2+n/\sigma^2}$ and $D = \dfrac{1}{1/s^2+n/\sigma^3}$

This last relationship is the posterior distribution for μ given the observed value of $\bar{x}$. (This statement would not make sense from the classicist viewpoint because it is μ that is considered fixed - not the observed point $\bar{x}$.) Thus, the major difference between the classicists and Bayesians is that the classicists see μ fixed while $\bar{x}$ varies, while the Bayesians see $\bar{x}$ fixed (for any given experiment) while μ varies.

The Bayesian estimator of the mean μ is that quantity which minimizes the conditional expectation of $(\mu-\mu^*)^2$ given the observed value of $\bar{x}$. From the relation for $\mu|\bar{x}$:

$$\mu^*(x) = m + C(\bar{x}-m)$$

To demonstrate these relations, consider the example of I.Q. testing. Our prior information is that the mean I.Q. of an average population is m = 100 with $s \cong 15$. About 68% of IQ's are between 85 and 115, about 95% between 70 and 130, etc., i.e.,

$$\mu \sim \eta(100,225)$$

Suppose now that an IQ test is applied to the American population in 1981, and it is observed that the average score is $\bar{x} = 160$, $\sigma = 7.5$, what is now the Bayesian estimate of the mean $\mu$? It can be estimated from:

$$\mu^*(\bar{x}) = m + C(\bar{x}-m), \; C = \frac{n/\sigma^2}{1/s^2+n/\sigma^2}$$

with $m=100$, $s^2=225$, $\bar{x}=160$, $\tilde{\sigma}=7.5 \rightarrow \sigma^2=56.3$, $n=1$.

Then

$$\mu^*(160) = 100 + C(160-100), \; C = \frac{1/56.3}{1/225+1/56.3} = \frac{.018}{.0044+.018} = .802$$

or

$$\mu^*(160) = 100 + .8(60) = 148; \; D^2 = \frac{1}{.0224} = 44.64 \rightarrow D = 6.7.$$

That is, the posterior distribution's mean value is 148 (Figure 1). The Bayesian would say the population has an average I.Q. of 148 instead of 100 where a 95% probability exists that a person tested in that sample population has an I.Q. between $[148-2\sqrt{D},148+2\sqrt{D}] = [134.6, 161.4]$ where $\mathrm{Prob}\{\mu^*(\overline{x})-2\sqrt{D}\leq\mu\leq\mu^*(\overline{x})+2\sqrt{D}|\overline{x}\} = .95$ is the Bayesian analogue to a 95% confidence interval.

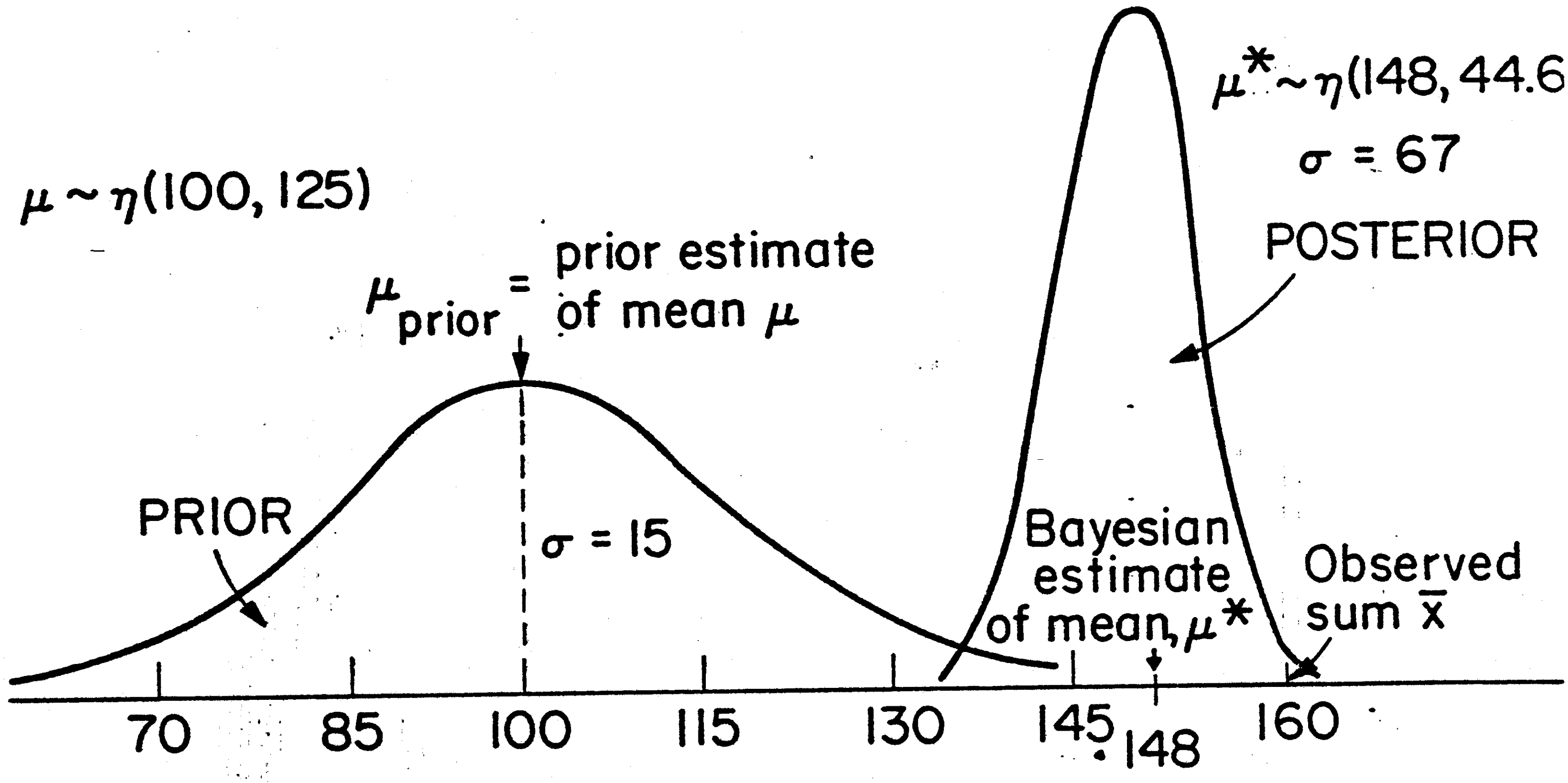
The Frequentists would observe the same example differently; assume no prior knowledge of $\mu$ and observe $\overline{x} \sim \eta(\mu,\sigma^2/n)$, $\sigma/\sqrt{n} = 7.5$ and $\overline{x} = 160$. Then $\mu = 160$ is the best Gaussian estimate of the mean and the 95% confidence limits are $\{\hat{\mu}-2\sigma/n, \hat{\mu}+2\sigma/n\} = (145,175)$. Suppose that new information is provided indicating that all scores below 100 were reported as 100, although all others were reported correctly. The Frequentist would still assume $\hat{\mu}=\overline{x}=160$ even given new information. This apparent defect in the Frequentist approach is resolved by Bayesian methods since new information can be used to update existing prior information.

If no information, or very little, is available upon which to base a prior estimate, there are two schools of Bayesian thought about how to proceed:

(1) <u>Objective Bayesians</u>:* A flat prior is assumed: $\mu \sim \eta(0,\infty)$. This represents a prior opinion that is neutral and therefore "objective". The Bayesian estimate in this case becomes $\mu^*=\hat{\mu}=\overline{x}$ and $\mu|\overline{x} \sim \eta(\overline{x},\sigma^2/n)$. The estimator is that of the Frequentists. A problem with this approach

*Bayes and Laplace both believed in this approach.

Figure 1 Bayesian Statistics: IQ Testing Example



is that though the prior is flat for $\mu$, it is not for $\mu^3$ or any other power of $\mu$, so expressing ignorance seems to depend on which function of the unknown parameter one is interested in.

2. Subjective Bayesians: The subjectivists assess a prior distribution based on "engineering judgment" otherwise referred to in the literature as "expert opinion". Probability distributions based on expert judgment and available data can be derived to represent prior estimates. This approach is not useful for scientists publishing controversial new results because of the subjectivity involved, but is of considerable benefit to risk analysts, business and R & D managers, safety assessors, and others - including nuclear engineers.

## B. Statistical Distributions/Importance to Engineering Safety Analyses

### B.1 Statistical Distributions

The engineer should become familiar with several statistical distributions which are commonly used in reliability analyses:

(i) the NORMAL distribution;

(ii) the LOG-NORMAL distribution;

(iii) the WEIBULL distribution;

(iv) the EXPONENTIAL distribution;

(v) the BINOMIAL distribution; and

(vi) the POISSON distribution.

These distributions are often used to probabilistically model the failure rate of components; for example, in WASH-1400, log-normal distributions were assumed throughout in modeling failure rates (see App. II, WASH-1400, pp. 42-43). Important properties of these functions and their behavior are shown in Figures 2 through 7.

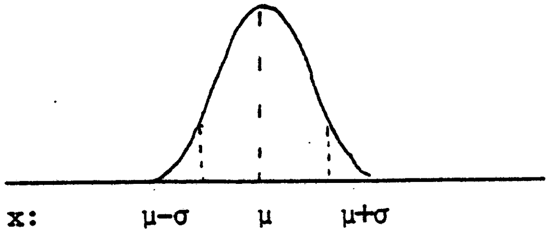
### B.2 Importance to Engineering Safety Analyses

The importance and relevance of each distribution to engineering safety analyses is dependent upon the shape of the distribution, its mathematical properties (i.e., is it part of a conjugate pair of distributions), its relative utility (i.e., how easy it is to use), and how well it fits a pattern established by a given set of data.

#### B.2.1 The Normal Distribution

The normal distribution is probably the most widely used distribution in science and engineering since it models very well the behavior of many natural systems. It is symmetric about the mean and models any process that varies by an additive or subtractive factor.

Figure 2 The Normal Distribution



Probability Density Function (PDF):

$$f(x) = \frac{1}{\sqrt{2\pi\sigma}} \exp - [\frac{(x-\mu)^2}{2\sigma^2}]; - \infty < x < + \infty$$

Mean, Median, or Mode: $\mu = \int_{-\infty}^{\infty} xf(x)dx$

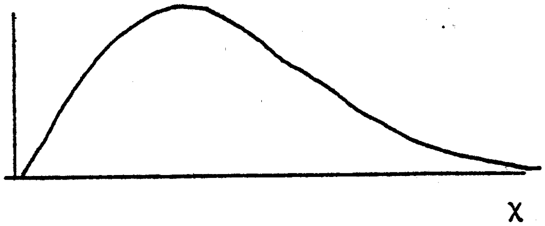
Variance: $\sigma^2 = \int_{-\infty}^{\infty} (x-\mu)^2 f(x)dx$

To evaluate these parameters tables are used referring to a factor "t" where"

$$P(t) = \int_{o}^{t} \frac{1}{\sqrt{2\pi}} \exp(-t^2/2)dt$$

where when $t = 0$ $x = \mu$; $t = 0$ to $1$ given $\mu$ to $\mu + \sigma$

Figure 3 The Log-Normal Distribution



Probability Density Function (PDF):

$$f(x) = \frac{1}{(\sqrt{2\pi})\sigma x} \exp - [\frac{\ln(x-\mu)^2}{2\sigma^2}]; x > 0$$

Mean: $\bar{x} = e^{\mu+\sigma^2/2}$

Variance: $V = e^{2\mu+\sigma^2}[e^{\sigma^2} -1 ]$

Often, models are constructed that represent combinations of normal distributions. A common use of the normal distribution in engineering calculations is in modeling the random error that exists on some uncertain parameter such as tolerances of electrical components (e.g., resistors, capacitors, etc.).

In utilizing the normal distribution, two other distributions are made use of: the "chi-squared" distribution ($\chi^2$) and the "student's t" distribution. The $\chi^2$ distribution is used to find the range on the variance $\sigma^2$ such that

$$\frac{\hat{\sigma}^2 f}{\chi_2^2} \leq \sigma^2 \leq \frac{\hat{\sigma}^2 f}{\chi_1^2}$$

where $f = n-1$. The student's t distribution is used to estimate the range on the true mean $\mu$ of the normal, and can be used to establish confidence intervals as follows:

$$\hat{\mu} - \frac{t\hat{\sigma}}{\sqrt{n}} \leq \mu \leq \hat{\mu} + \frac{t\hat{\sigma}}{\sqrt{n}}$$

(The interested reader is referred to Ref. 13 for further information on the uses of these additional distributions in sampling from a normal distribution. Statistical tables for the $\chi^2$ and t distributions are provided in the attached Appendix.)

### B.2.2 The Log-Normal Distribution

The log-normal distribution is useful because it models well the mean time to repair of a component; specifically, a component's failure rate. It is useful in reliability calculations if the x-axis is time.

Also, its asymmetry at higher values of x is useful for modeling very uncertain problems where conservatism is added on the high side to account for a lack of data or high degree of uncertainty. In WASH-1400, for example, the failure rate of a component placed on an hourly basis was generally estimated to fall between some value $10^{-x}$ to $(10^{-x}) \overset{\times}{\div} 10$. The log-normal was found applicable since it is often used when factors or percentages characterize the variation. The log-normal is a natural distribution for describing data which can vary by factors in the same way that the normal distribution is the natural choice when data can vary by additive or subtractive factors. The use of the log-normal can be interpreted as viewing the exponent as being the significant variable in the failure rate characterization problem.

Some other reasons for using log-normals were given in WASH-1400, and are quoted here as follows [15]:

"a. The two-parameter nature of the log normal family gives sufficient flexibility for describing the range variability (to define a unique log normal distribution, two parameters must be specified; e.g., the two range end points).

"b. The log normal distribution form, in particular its positive skewness, can incorporate general reliability associated behaviors of the assessed data (the positive skewness accounts for the occurrence of less likely but large deviations, such as abnormally high failure rates due to batch defects, environmental degradation, and other outlier causing effects).

"c. The assessed data comprise reliability data in the form of probabilities (for example, a failure rate is simply a conditional probability). If the probabilities are decomposed into products of probabilities representing requisites for failure, then when the central-limit theorem is applicable, the log normal is the resulting distribution. (In this characterization, a failure rate $\lambda$, for example, is decomposed into a product of probabilities $P_i$ which represent occurrences of various causal mechanisms, $\lambda = p_1p_2$. If logarithms are taken, the result follows.)

"d. Related to item b., as an a priori distribution the log normal gives coverage to errors which can be skewed toward large values. In general, the average value is greater than the median value, which, in turn, is greater than the most probable value, thus providing a protective, positive-type bias which is retained when the distributions are propagated. (The larger tails on the log normal account for failure rates, for example, which can greatly deviate from the estimate for the average component. The average and median values for the log normal are, in general, larger than the most probable value, and this behavior propagates as the distributions are propagated.)

"e. The log normal distribution, under the applicable situations, can assume a near normal-type shape or a near exponential-type shape and is thus adaptable in its description.

"f. Finally, the log normal has an established history of useful representation when relative variations (factors) characterize the random variable. Common examples include stress treatment, Arrhenius modeling, and log normal regressions, as well as general reliability-modeling applications. Its application as a general distribution for modeling physical and reliability processes is established and has often been validated.

Median: $x_{0.5} = e^{\mu} = \sqrt{x_u x_L}$; $x_u$ = upper bound

$x_L$ = lower bound

Mode (most probable value): $x_m = e^{\mu-\sigma^2}$

Example: Suppose $\mu = 3$, $\sigma = 1$:

Then, the mean $\bar{x} = e^{\mu+\sigma^2/2} = e^{3+1/2} = e^{3.5} \cong 33$

and the median $x_{0.5} = e^3 = 20$

Figure 4 The Weibull Distribution

Probability Density Function (PDF):
(three-parameter Weibull function)

$$f(x) = [\frac{C}{E-T_o} (\frac{x-T_o}{E-T_o})^{C-1}] \exp - [\frac{x-T_o}{E-T_o}^{C}]$$

where C = Weibull slope or shape parameter
E = characteristic life or scale parameter
$T_o$ = location parameter

C, E, $T_o$ are determined experimentally

$$F(x) = \int_o^x f(x)dx \text{ for } T_o = 0 \text{ where}$$

$$f(x) = \frac{C}{E}(\frac{x}{E})^{C-1} \exp[- \frac{x}{E}^{C}]$$

$$\rightarrow F(x) = 1 - \exp[\frac{x}{E}^{C}] \text{ for } x \geq 0$$

The Weibull function has been used to describe the lifetime of electronic tubes, antifriction bearings, transmission gears, and mechanical and electrical components as well as the fatigue of materials.

"The above items of course do not constitute tenets for the dogmatic justification of the log normal as the only distribution applicable, but instead serve as a priori considerations. As a complement to the agove considerations, from a pragmatic point of view, the log normal was employed because it was flexible, it was consistent with reliability and data properties, and it is a standardly employed and straightforward (null-hypothesis) distribution. Checks and tests of its applicability to the data of this study did not contradict nor refute these a priori and pragmatic justifications."

### B.2.3 The Weibull Distribution

The Weibull distribution can be used to fit a wide range of data because of the shape parameters which can be varied to fit the data at hand. Perhaps the most useful Weibull distribution is the special case where C=1, the exponential distribution.

Graphical techniques have been used to estimate the parameters of the Weibull distribution. Special graph paper known as modified Weibull probability paper is utilized to estimate these parameters graphically. A new statistical test of the goodness-of-fit for the two-parameter Weibull function has been developed. In addition, if the test data are censored or not burdened to the end of design life or to failure, techniques can be used to estimate the Weibull parameters.*

*See W. Weibull, "A Statistical Distribution Function of Wide Applicability", ASME Paper 51-A-6, presented at annual meeting of the American Society of Mechanical Engineers, Nov. 25-30, 1951; C. Lipson and N.J. Sheth, "Statistical Design and Analysis of Engineering Experiments", McGraw-Hill Book Co., Inc., New York, 1973; N.R. Mann, "Confidence and Tolerance Bounds and a New Goodness-of-Fit for Two Parameter Weibull or Extreme Value Distributions with Tables for Censored Samples of Size 3(1)25", ARL 71-0077, Aerospace Research Laboratories, May 1971; A.C. Cohen, "Maximum Likelihood Estimation in the Weibull Distribution Based on Complete and on Censored Samples, Technometrics 7, (4) 579-588, November 1965.

### B.2.4 The Exponential Distribution

The exponential distribution can be used in reliability problems where $\lambda$ is assumed the failure rate of a component to model the high failure rate behavior at the end and very beginning of component life (i.e., the famous "bathtub" curve of time (x-axis) vs failure probability (y-axis)). For example, for a large number of components, N, with probability per unit time of failure, $\theta$, then $dN = -N\theta\ dt$ is the change in the number of components so $\frac{dN}{N} = -\theta dt \rightarrow N = N_o e^{-\theta t}$. Thus, $N/N_o$ = probability of survival = $e^{-\theta t}$, or $(1-e^{-\theta t})$ = probability of failure. Thus, $f(t)dt$ = (probability of survival) x (probability of failure)$dt = e^{-\theta t}\theta dt$, where, if $\theta = 1/\lambda$ and $\lambda$ is near the failure time, $f(t)dt = 1/\lambda e^{-t/\lambda}$. This last function is the exponential distribution and finds wide application in reliability theory.

### B.2.5 The Binomial Distribution

The Binomial distribution is useful for those problems where a variable can assume only discrete values. An example would be a "throwing-of-dice" problem; i.e., estimating a probability of 1/6 of getting a "3" on a roll of a die. The formulas do not work with card problems for estimating the probability of getting four aces in a row since, for example, in these problems, the denominator would also be changing in the calculation (e.g., 4/52 x 3/51 x 2/50 x 1/49). Thus, if p and q are both changing, the binomial distribution should not be used.

### B.2.6 The Poisson Distribution

The Poisson distribution is a special case of the binomial distribution approximating a normal distribution at large values of n,

Figure 5 The Exponential Distribution

Probability Density Function (PDF):

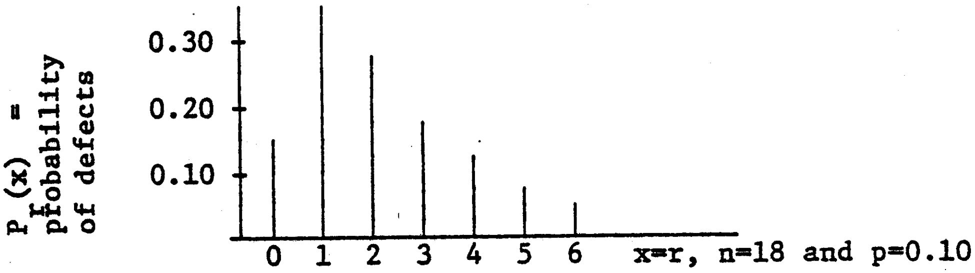
$$f(x) = \frac{1}{\lambda} e^{-(x/\lambda)}$$

(special case of Weibull distribution with C = 1)

Mean: $\bar{x} = \lambda$

Variance: $V = \lambda^2$

Figure 6 The Binomial Distribution



Probability Density Function (PDF):

$$P_r = \frac{n!}{r!(n-r)!} p^r (1-p)^{n-r}$$

where $0 < p < 1$, $n \equiv$ positive integer (binomial random variable).

For n=1, P(0)=1-p, P(1)=p and p is called a Bernouilli random variable.

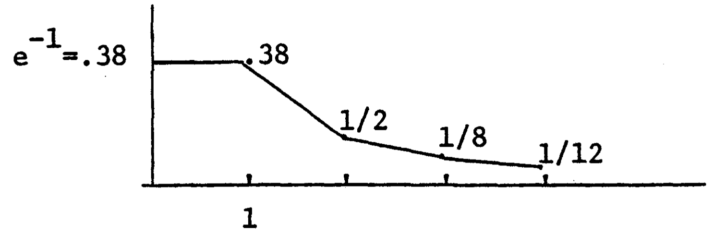
Mean: $$\bar{x} = \sum_{r=0}^{n} r \frac{n!}{r!(n-r)!} p^r (1-p)^{n-r}$$

$$= np$$

Variance: $V = np(1-p)$

where n is the number of data points taken. It can therefore often be used for problems where the phenomenon is not known to be strictly normal (e.g., counts from a scintillation counter). When there is a series of things contributing to a measurement, then the distribution derived approaches that of a Poisson, which looks normal when n is sufficiently large.

Figure 7 The Poisson Distribution



Probability Density Function (PDF):

$$P_r = \frac{n^r p^r}{r!} e^{-np}$$

and is approximation for Binomial distribution as n → ∞, p → 0:

$$n^r \cong \frac{n!}{(n-r)!} \quad ; \quad (1-p)^{n-r} \cong e^{-np}$$

## C. Fault and Event Trees/Cause-Consequence Diagrams

Three methods are available for modeling the interactions of systems and events that can lead to possible accident scenarios with consequent negative impacts:

(i) Fault trees;

(ii) Event trees; and

(iii) Cause-consequence diagrams.

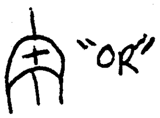
Each of these methods is now described and examples given.

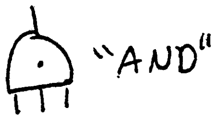
### C.I Fault Trees

Fault tree analysis (FTA) evolved in the aerospace industry in the 1960's [3]. As one of the principal methods of systems safety analysis, it is a detailed deductive analysis that requires considerable system information. Best applied during the design stages, it can identify hazardous conditions and potential accidents in a system design that can help eliminate costly design changes and retrofits that would otherwise have to be made later in the system life cycle. Undesirable consequences, such as a major release of radiation from an LWR containment, are identified by inductive analysis and/or engineering judgment-intuition. These events are usually undesired system states that can occur as a result of subsystem functional faults. These events can be broad and all encompassing or specific (e.g., failure to scram).

Fault trees describe the paths by which these undesirable events can take place. The first step is to define a top undesired event, called the TOP event. Care and understanding must be taken in this first step. A fault tree is a model that graphically and logically represents the various combinations of possible events, both fault and normal. An "event" is a dynamic state-of-change that occurs in a system or piece of equipment. There are two dynamic states for system elements; the OFF state (indicating the element is working properly) and the ON state (indicating either the element has failed or is operating inadvertantly). The time at which the element is on is referred to as the fault duration time.

The fault tree is so structured that the undesired event appears as the top event (Figure 8). The direct logical antithesis of a fault tree is known as a success tree (Figure 9). In both cases, the sequence of events that leads to the undesired event are shown below the top event and are logically linked to the undesired event by standard OR and AND gates:

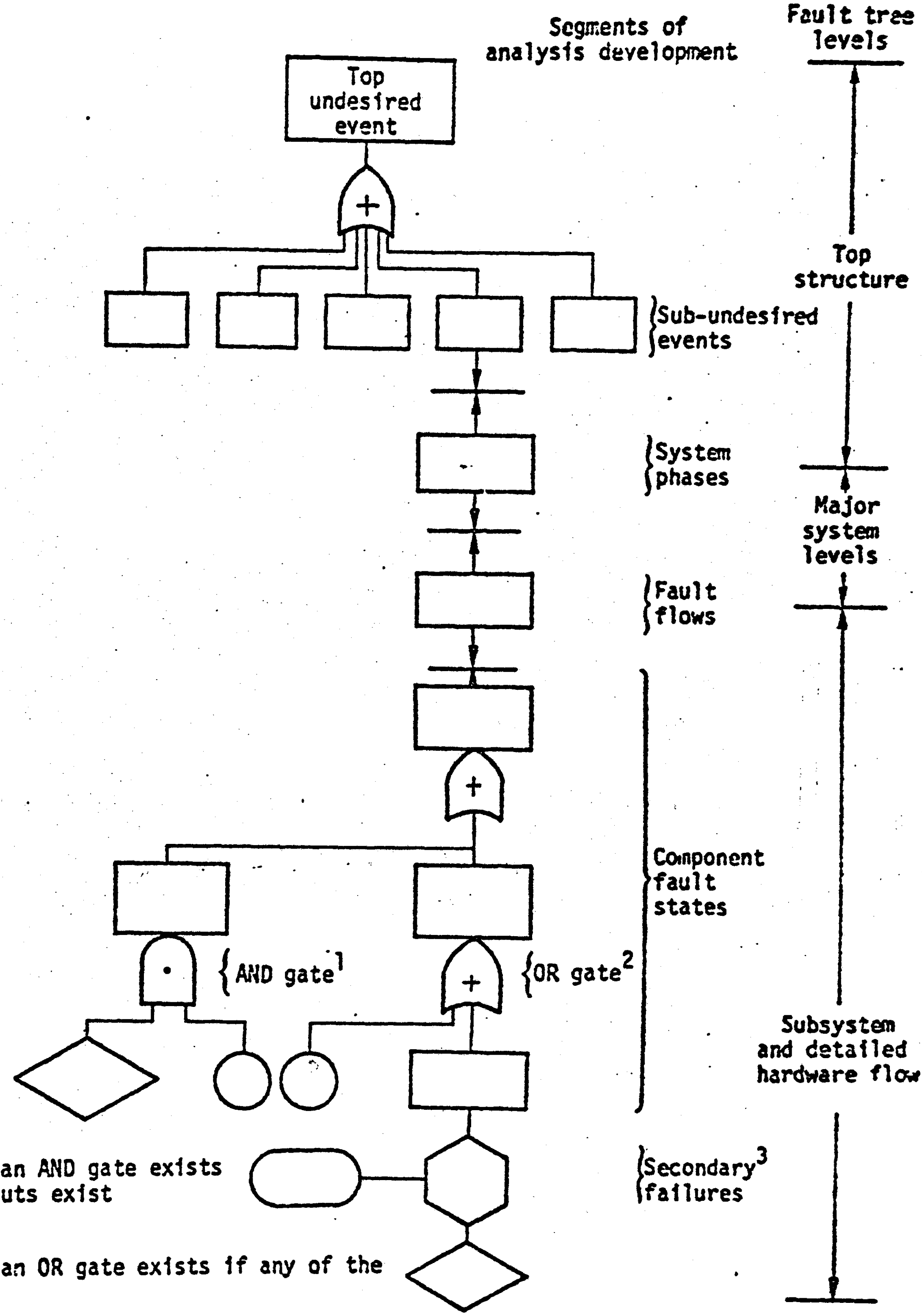




(In the success tree, AND gates replace OR gates and vice-versa.) The input events to each logic gate that are also outputs of other logic gates are shown as rectangles EVENT . These events are developed further until the sequences of events lead to basic causes. The basic events appear as circles BASIC EVENT and diamonds BASIC EVENT on the bottom of the fault tree and represent the limit of resolution. The circle represents an internal or primary failure and the diamond represents a non-primary failure that is not further developed. (For a complete definition of fault tree components, see Figure 10.)

A complete safety analysis of a nuclear plant requires normally three levels of fault tree development (Figure 8). The upper level is

Figure 8 Fault Tree Structure



[1] The output on an AND gate exists if all the inputs exist

[2] The output of an OR gate exists if any of the inputs exist

[3] A secondary failure is a out-of-tolerance failure of a system element - failure due to excessive operational or environmental stress placed on the system element

the top structure and includes the top undesired event and lesser events leading to it. The next level consists of an examination of system elements from a functional point-of-view. Fault flaws within each system lead to the third level where statistical independence of the events must be shown. Two events are statistically independent if one event in no way affects the outcome of the other event.

To perform a quantitative evaluation of the fault tree (that is, to determine the probability of occurrence of the TOP event), failure probabilities of system components must be estimated. Then, simple rules for combining probabilities in AND and OR gates are used to "fold-back" thre tree to the TOP event. Specifically, the information required to perform a quantitative analysis is: (1) a Boolean expression for the TOP event in terms of the basic events, (2) the probability of occurrence and the fault duration time for each basic event, and (3) the statistical dependence of basic events in the fault tree. In simple fault trees, the Boolean expression is easily determined; for the fault tree of Figure 9, the correct Boolean expression is $(P_{ps1} \cdot P_{ps2}) + P_B = P_A + P_B = P_{TOP}$. However, complex trees sometimes require computer codes that can solve fault trees. Also, Monte Carlo simulation can be used to find the top event. This is done by doing a random large number of direct calculations to find a range on the TOP event probability.

The general steps in constructing a fault tree are as follows [6]:

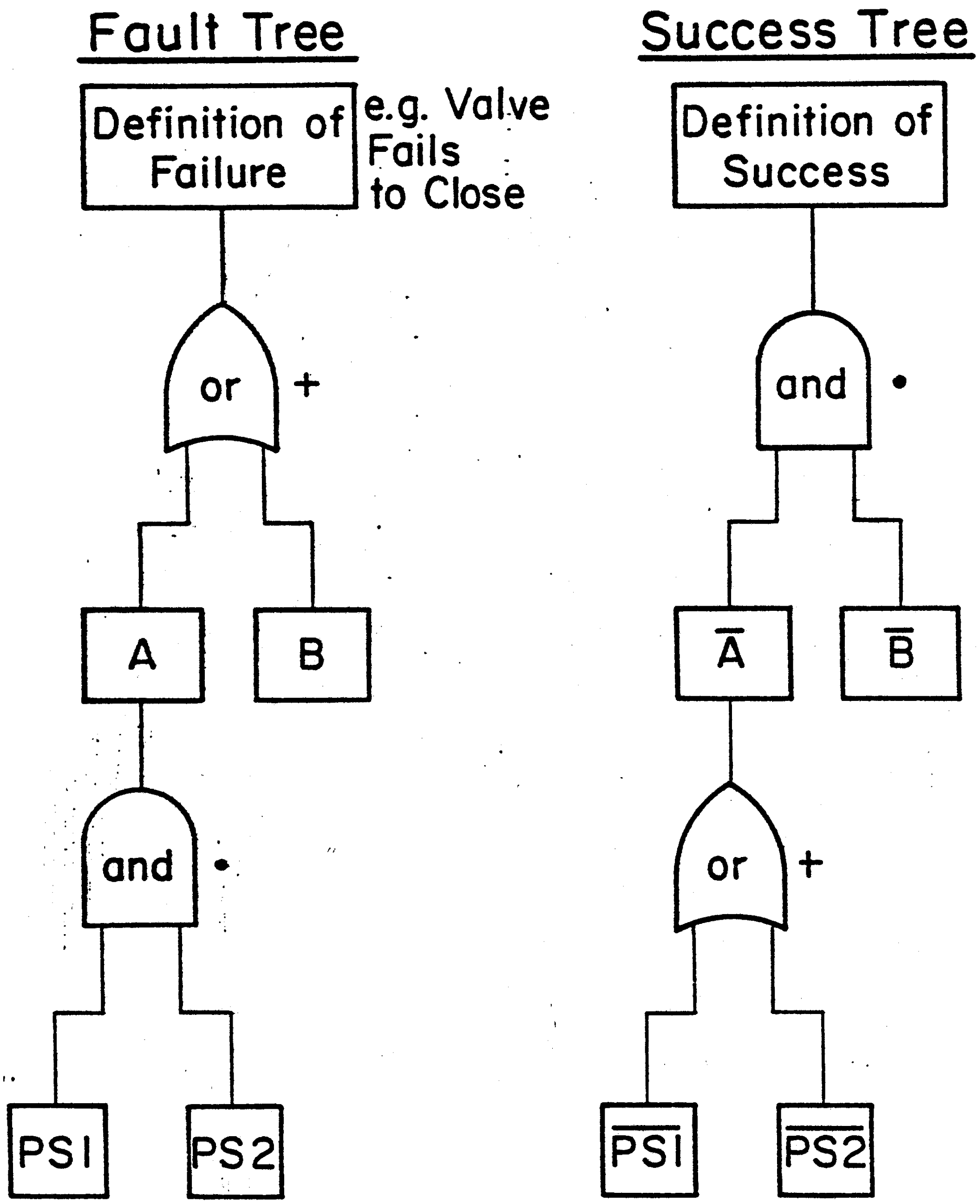
Step 1. Define the most undesired event. This event, called the "top event", is the starting point of the fault tree. It is important that this event be precisely worded so that its interpretation will not vary. For a particular fault tree there is one and only one most undesired event.

Step 2. Define for the main branches of the tree those events that lead directly to the top event and decide what logic gate should be used to relate them to the top event of the tree. These events are deduced from experience and knowledge of what can happen. They should be kept sufficiently general so that the details of the system can be developed in subsequent branches.

Step 3. Select one of the branches and deduce its next level of sub-branches. The manner of deducing these sub-branches is identical to that used in deducing main branches, and so on throughout the rest of the tree. The termination of a sub-branch of a tree occurs when the event being considered is a fundamental event (basic fault) or when a transfer gate can be used to another sub-tree already developed.

Like any technique, fault tree analysis has its good and bad points. The problem of oversight and omission is less a problem of the method than it is of the modeler - even skilled and knowledgable people make mistakes in applying the method. An increasing number of trained practitioners can insure redundancy of performed studies helping to alleviate this problem. Another problem is the modeling of components that have a multitude of possible operating modes; advanced methods are used to handle such cases. Data limitations are also a problem; the analysis is only as good as the input data and expertise. Nevertheless, quantitative evaluations are particularly valuable for comparing system designs. Despite some drawbacks, fault tree analysis provides a systematic procedure for identifying faults, forcing the analyst to understand the problem at hand. It is one of the best such tools available.

Figure 9 Fault and Success Trees



## C.2 Event Trees

An event tree is a model that expresses system reliability in terms of component reliability [4]. It is a process that examines individually the state of each component in the system and links these states to outcomes affecting the state of the system. Take, for example, a system comprised of one component (such as a pump) whose probability of successful operation is 0.98. The event tree branches at the nodal points and examines all possible states of the pump. By convention, desirable outcomes branch upward and undesirable outcomes branch downward (Figure 10). The event tree is read left to right. In the example shown (Figure 10), if the pump is operable, the system is successful and the probability that the system is working is equal to the probability that the pump is working (0.98). The process may be extended to two components in series, such as a pump and a valve having reliabilities of 0.98 and 0.95, respectively. If the pump is not working, the system has failed (even though the valve might not have). If the pump is working, the valve must then be checked (Figure 11). The system reliability is thus 0.98 x 0.95 - 0.931 and the system unreliability is 0.98 x 0.05 + 0.02 = 0.069. In these calculations, the pump and valve reliabilities are statistically independent (the operation of the pump in no way affects the operation of the valve and vice versa).

## C.3 Cause-Consequence Diagrams*

Cause-consequence analysis (CCA) is a method of system reliability and risk analysis and is a combination of both fault and event tree

*Cause-consequence analysis has been used as an aid in nuclear power plant reliability and risk assessment in Scandinavian countries since its inception in 1971. The material presented here has been derived in large part from Ref. [2].

Figure 10 Event Tree Example

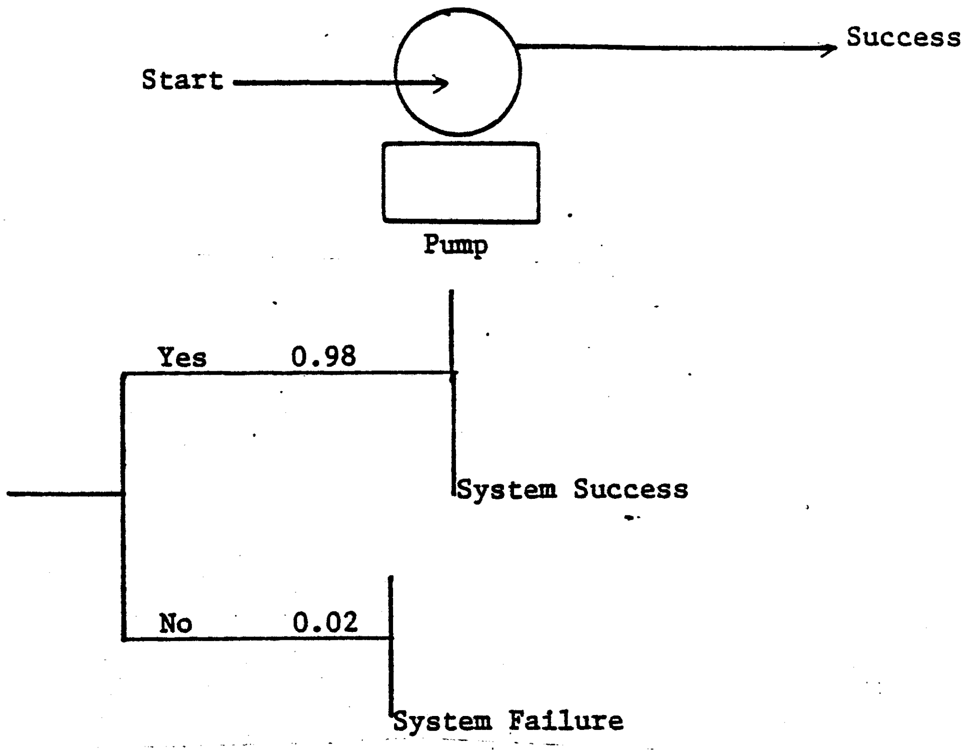
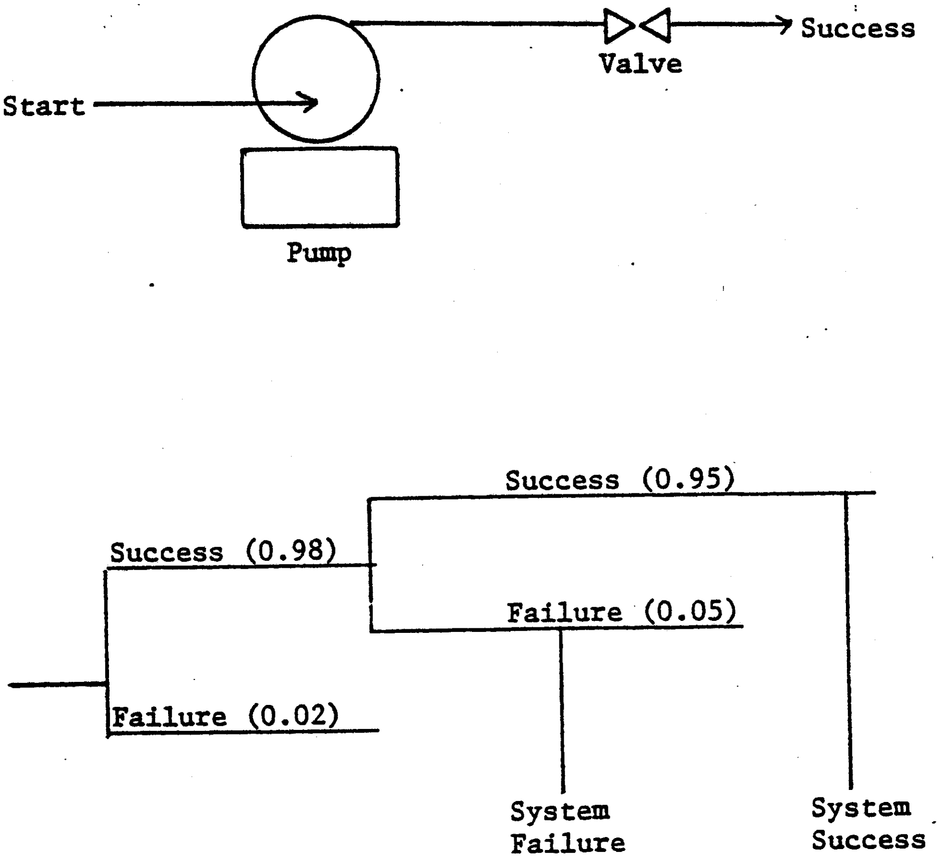


Figure 11 Extended Event Tree Example



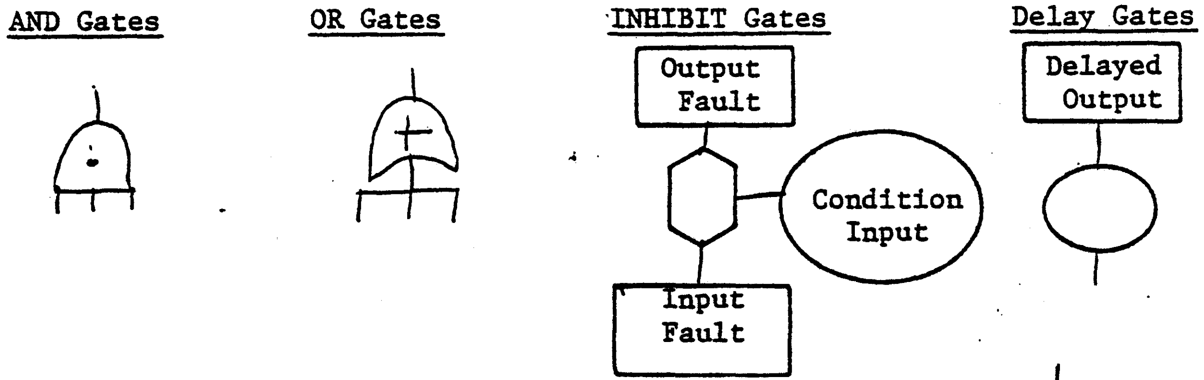
analysis. Its advantages include providing the analyst a means for displaying the complex relations between consequences and their causes. The "cause" portions of the cause-consequence diagram are fault trees with the TOP events being component or system failures that can lead to various levels of undesired consequence depending on the degree of mitigation imposed by standby systems. The "consequence" portion of the diagram illustrates the array of consequences as a function of the standby system state (failed or unfailed). The diagram illustrates the relations that preclude or contribute to the probabilities of occurrence of the possible consequences that can arise from a particular TOP event. Symbols used in the CCA are shown in Figure. 12. A sample cause-consequence diagram is shown in Figure 13.

Using the rules applicable to fault trees, calculation of consequence probabilities and risk assessment of consequences can be done in the cause-consequence diagram. Knowing the probability of occurrence of the basic events in each fault tree, it is possible to calculate the probability of occurrence of each fault tree TOP event in the cause-consequence diagram. If the branching operators are statistically independent, then by multiplying probabilities at each branching operator corresponding to event occurrence (yes) or nonoccurrence (no), an estimate of the occurrence probability estimate can be obtained. (An example of such a calculation in a sample cause-consequence analysis is given in section E.)

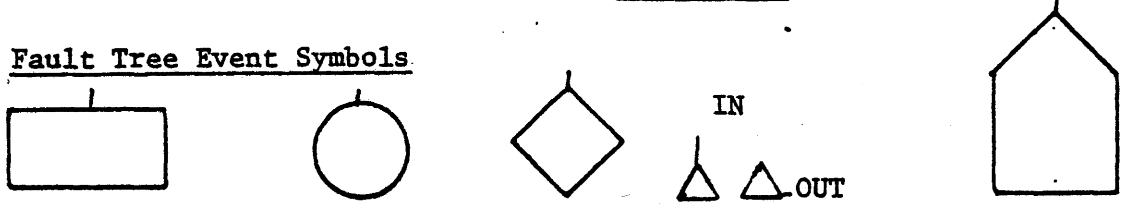
The cause-consequence diagram is a more detailed representation of the relationships between system failures and consequences, and can in any case be reduced to an event tree. In fact, an event tree is a

Figure 12 Symbols Used in Cause-Consequence Analysis

A. Fault Tree Logic Symbols



B. Fault Tree Event Symbols



Rectangle

A fault event resulting from the combination of more basic faults acting through LOGIC gates.

Circle

A basic component fault-an independent event.

Diamond

A fault event not developed to its cause.

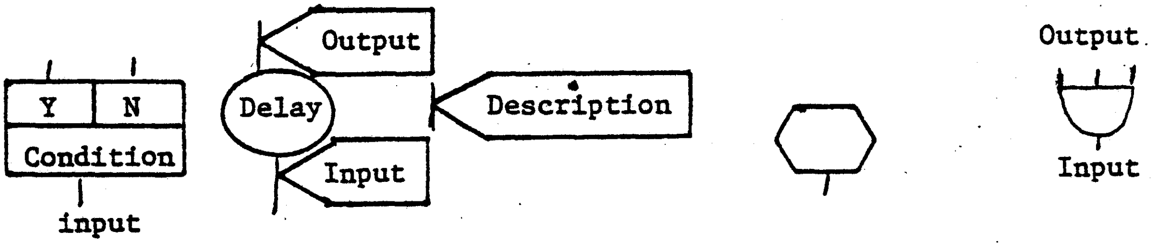
Triangle

A connecting or transfer symbol.

House

An event that is normally expected to occur or to never occur.

C. Consequence Diagram Symbols



Branching Operator

Output is "yes" if condition is met; "no" otherwise.

Delay Operator

Indicates the amount of time delay required for output event to result from the input event.

Event Description

Describes the event present at specified position.

Consequence Description

Describes the consequence. A terminal symbol.

Inverse AND Gate

All outputs occur if the input occurs.

cause-consequence diagram with all fault trees, gates, descriptions, and delay operators removed. The branching operators are replaced by the branch points in the event tree. The event tree is more streamlined than the cause-consequence diagram serving the purpose of brevity. However, the cause-consequence diagram contains more detailed information and is therefore more useful to a systems analyst or design engineer.

Cause-consequence analysis is of major value in that it allows the analyst to work an otherwise unmanageable problem in in segments. A standard approach to a typical problem is to determine inductively the possible consequences and use these as TOP events for an array of fault tree analyses. One advantage that CCA has is that it provides a better method for depicting the many logical combinations of events that contribute to a particular consequence or group of consequences. It helps the engineer or analyst to better understand the system by providing a means by which knowledge can be organized. It further provides a model from which probabilities of occurrence of various consequences can be estimated and from which risk numbers may be obtained for the consequences without loss of causal information as with event trees. Also, in constructing the cause-consequence diagram, the analyst is given the option of working forward from an event or backward from a consequence.

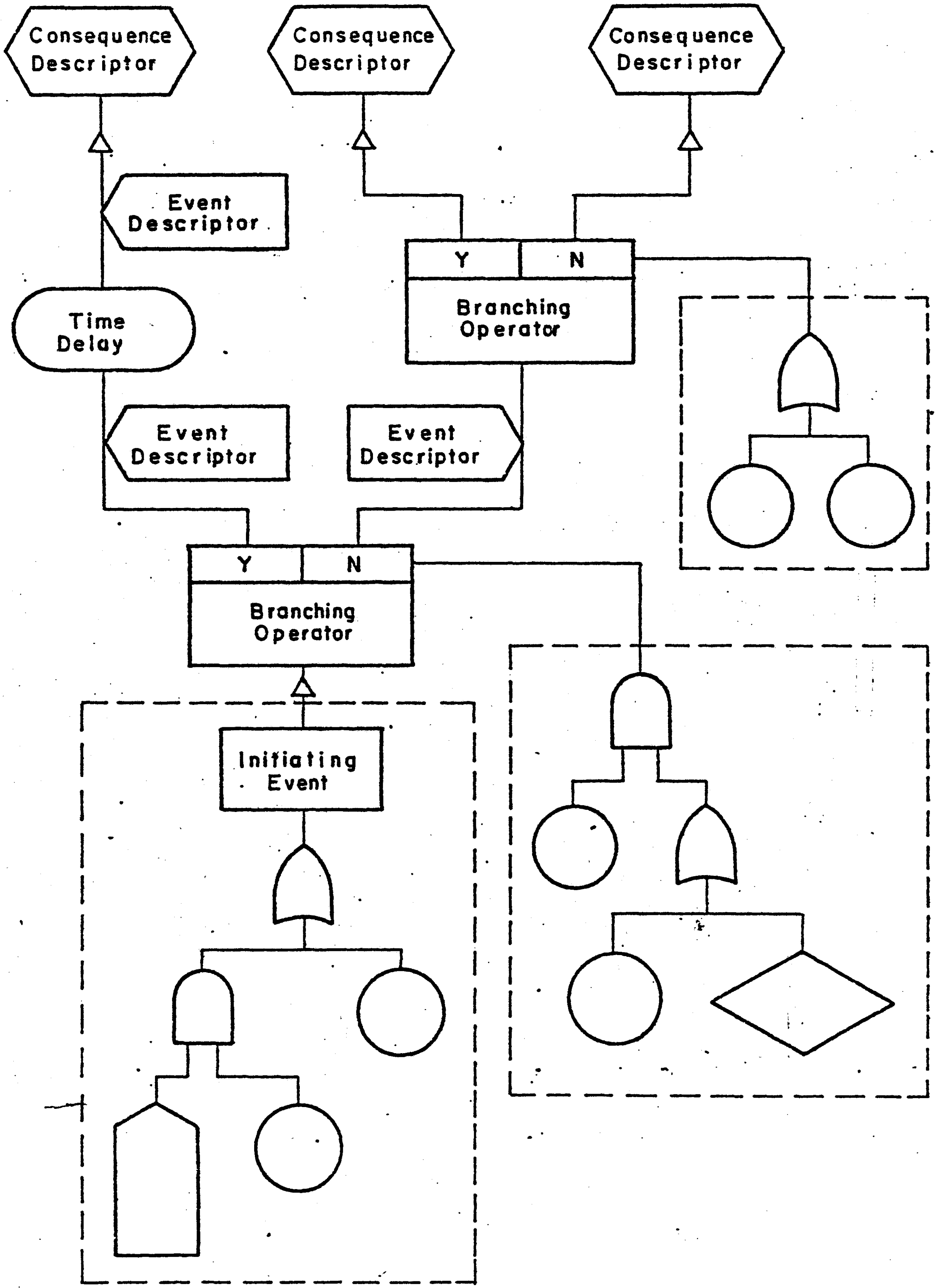


Figure 13 Sample Cause Consequence Diagram

## D. Decision Analysis/Risk Analysis and Risk Assessment Methods

The following sections discuss decision analysis (D.1) and other risk analysis and assessment methods (D.2). Examples of application are also included.

### D.1 Decision Analysis

#### (i) The Decision Problem: The Problem Space

Any decision problem can be described in terms of whether it is deterministic or probabilistic, involves many variables (complex) or only a few (simple), and is either dependent on time or is static (deterministic). The problems that are most difficult to analyze are those that are simultaneously complex, dynamic and probabilistic. Most problems in the safety-licensing area fall into this latter category. A mathematical theory that can handle such problems is Bayesian decision analysis. The problem space, shown in Figure 14 indicates the relationship of such problems with regard to similar problems handled by other scientific disciplines.

#### (ii) The Decision Analysis Cycle: Role of R&D in Information Gathering

A decision problem can be analyzed by following the cycle shown in Figure 15. First, decision alternatives must be defined; for example, a problem in reactor safety might decide between two or more available containment designs. Prior information available on a problem is used in the deterministic phase to identify which variables most affect or influence the decision problem when expressed in deterministic terms. For example, in a reactor safety problem the analyst would like to know how to bound his problem - if he goes into too great detail, his problem will quickly be too large to handle even on

Figure 14 The Problem Space

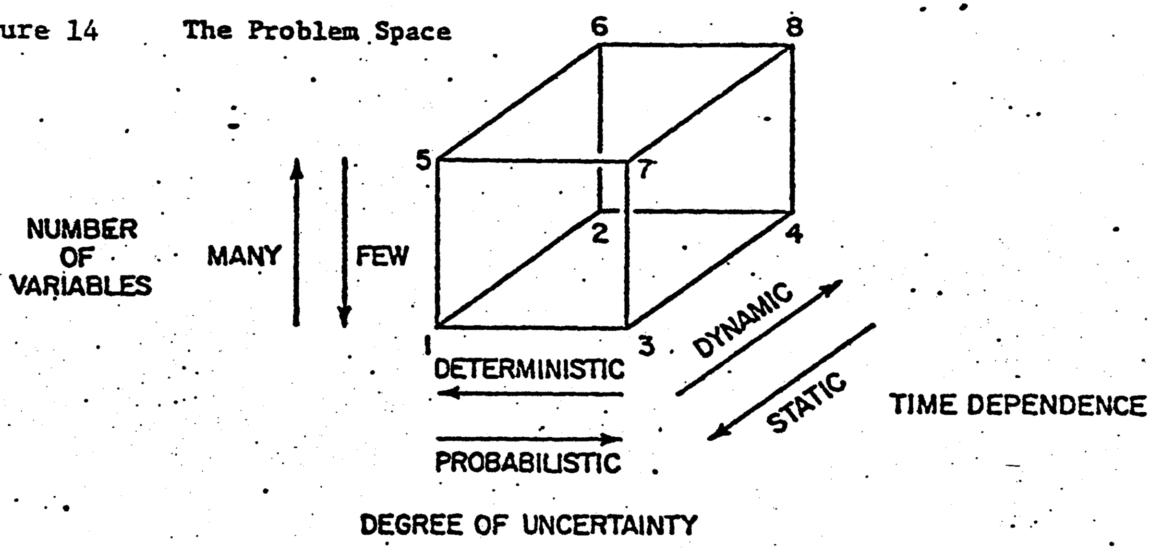
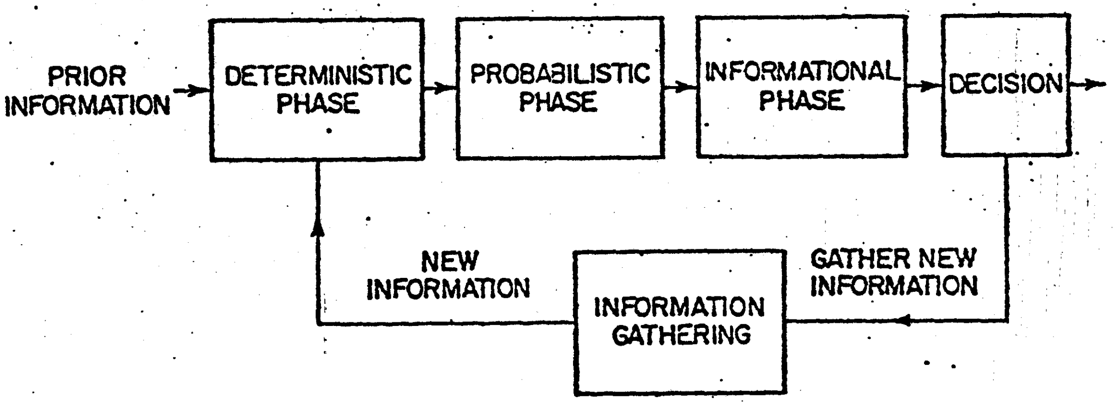


Figure 15 The Decision Analysis Cycle



the largest of computers. The deterministic phase involves constructing a model, running a few calculations using "best estimates" on inherently uncertain parameters to get a feeling for which variables are most important. It provides a way to limit the size of the final model.

After the important variables and system relations have been determined, a full-blown probabilistic analysis is conducted using decision-event trees, fault-trees, statistics, and other methods. In the informational phase, sensitivity analysis determines whether one decision alternative stochastically dominates another. If this is the case, the decision is clear cut. However, in many cases, the results of the analysis do not give clear cut results because the prior information available may not be sufficient to adequately distinguish between alternatives. The box labeled "decision" also includes the alternative to delay the decision until further information can be provided.* Sometimes, decision must be made immediately, and further information gathering is not possible; other times, the delay that would be required to update the prior information would be so long (10-50 years) that the information gathering approach is not practical. The role of research and development in the decision making process occurs in the information gathering state; new information from this stage is then used to repeat the decision analysis. Sometimes, the information gathering stage must be repeated many times before a decision can be

*The NRC as does any decision-making organization often must decide between setting a regulation immediately based upon existing information or delaying the decision until further information can be gathered to help clarify matters.

made; however, at some point delay becomes too costly or impractical such that the decision has to be made irregardless of the existing uncertainty.

(iii) Decision Models: Definitions of Event Tree and Outcome Values: The Axioms of Decision Analysis

The basic construction of a decision model involves construction of an event tree where the symbol "□" signifies a decision node; the symbol "○" an event node. Branches are used to signify various decision alternatives and possible event outcomes (Figure 16). In a decision-event tree, the branches represent the process of discretization necessary for analytic simplicity and practicality. Most uncertain events can assume a continuum of final outcomes expressed by their continuous probability density functions (p.d.f.). Discretization is a process by which such p.d.f.'s can be approximated for use in an event-decision tree.

The axioms of decision analysis are given in Figure 17, and indicate the relations which must hold given the trees are to be analyzed logically: an example of a decision-event tree is shown at the top as a lottery involving three alternatives with probability $P_A$, $P_B$, $P_C$ of getting prize A, B, or C as an outcome. These axioms make up the foundations of decision analysis.

(iv) Probability Encoding

The process of probability assessment is used by the analyst to encode quantitatively expert opinion (engineering judgment) on various uncertain parameters. Usually, this process involves questionnaires or personal interviews of experts. Techniques for probability encoding are well established and continually being up-dated [14]. The

Figure 16 Decision Tree Construction

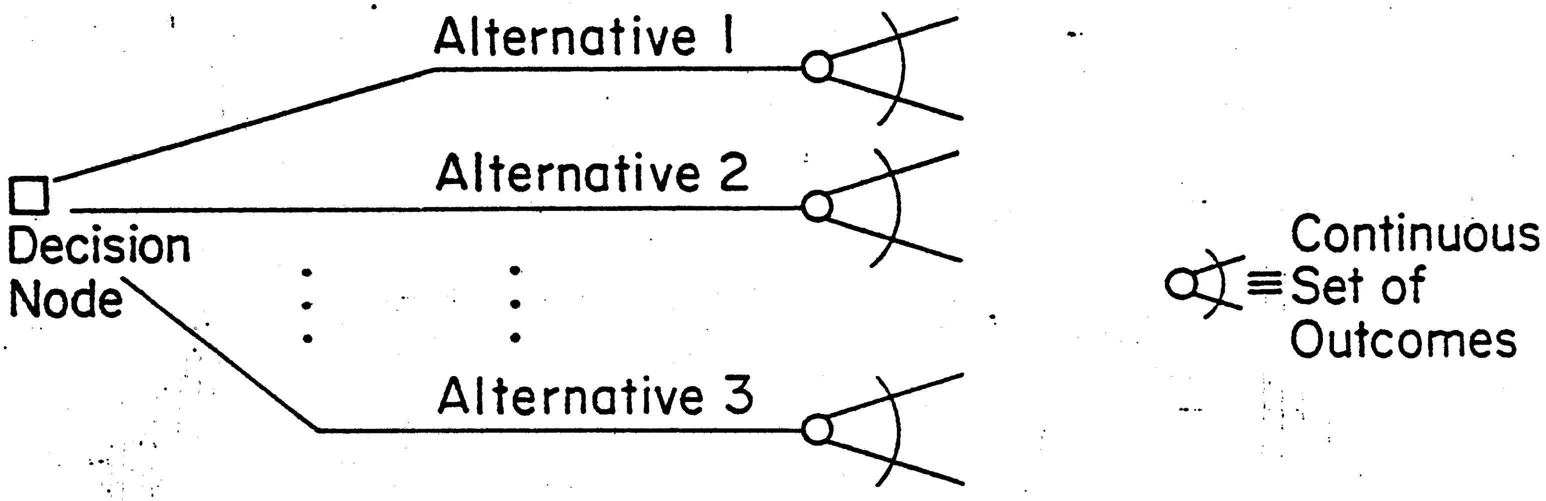
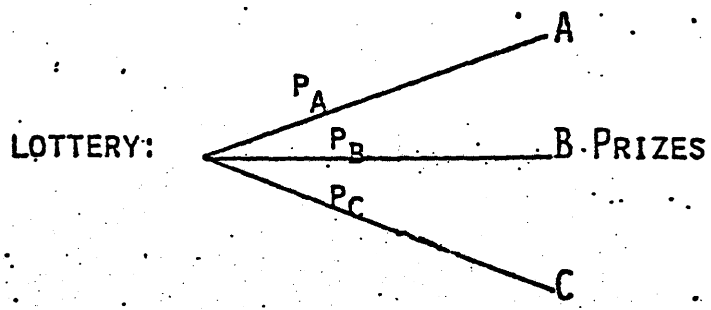


Figure 17 Axioms of Decision Analysis



AXIOMS

1) ORDERABILITY OF PRIZES

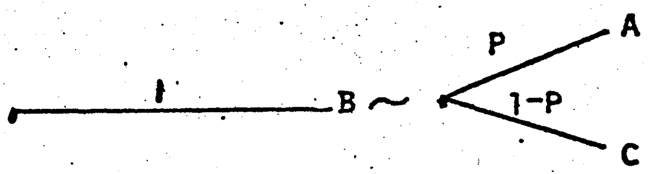
$A > B$, $A \gtrsim B$, $A \sim B$, $A \lesssim B$, $A < B$

TRANSITIVITY IF $A > B$, $B > C$ THEN $A > C$

2) CONTINUITY

IF $A > B > C$

THEN FOR SOME P



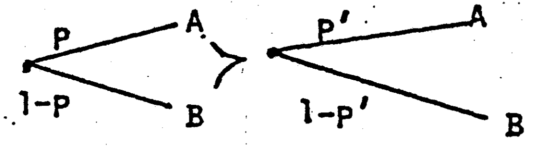
B IS THEN CALLED THE CERTAIN EQUIVALENT OF THE LOTTERY

3) SUBSTITUTABILITY

A LOTTERY AND ITS CERTAIN EQUIVALENT ARE INTERCHANGEABLE WITHOUT AFFECTING PREFERENCES

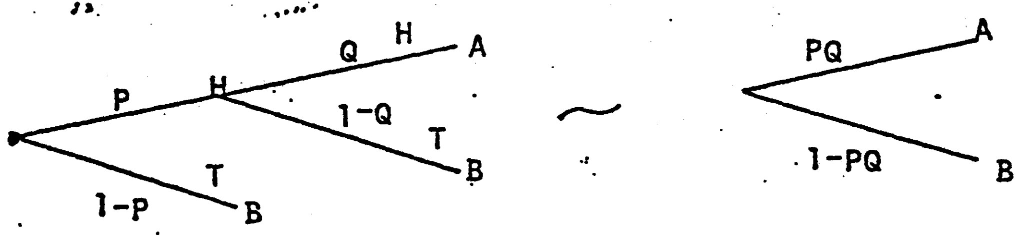
4) MONOTONICITY

IF $A > B$, THEN



IF AND ONLY IF $P > P'$

5) DECOMPOSABILITY



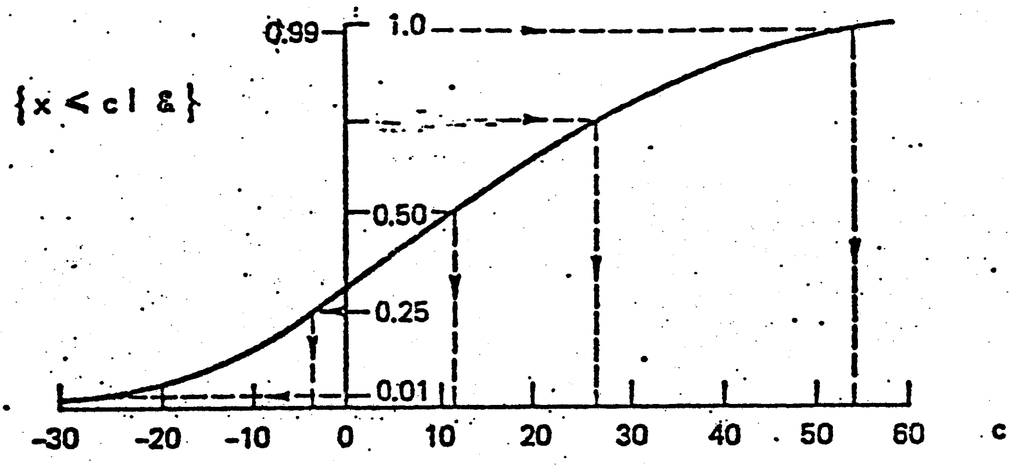
experts' opinion is usually encoded as a cumulative probability distribution indicating, on the y-axis, the probability that the variable will assume a value greater than or equal to x, expressed on the x-axis. The process is shown in Figure 18 with an example (Figure 19) of three experts' opinions on the probability of a particular material having a lifetime greater than or equal to t years. (Sometimes, concensus between experts is not as evident as in the case shown in the example of Figure 19.) Finally, a probability encoding form used in such assessments is shown in Figure 20. The process of probability encoding is routine in some industries such as in the oil industry that employ large staffs of operations researchers. Often, however, consultants are called in to perform a company's decision analysis, and several consulting firms which specialize exclusively in decision analysis have been formed in recent years to meet the growing industrial and government demand for such services (e.g., Applied Decision Analysis, Decision Focus, etc.).

## D.2 Risk Analysis and Risk Assessment Methods

Risk is mathematically defined as a function of probability and consequence of an event occurrence: $R = f(p,q)$ where $R$ = risk, $p$ = probability, $q$ = consequence, and $f(p,q)$ is some mathematically defined function of $p$ and $q$. In most treatments of risk, the mathematical relation for risk is expressed as a multiplicative linear relationship between $p$ and $q$: $R = p \cdot q$ which can be expressed conceptually as follows:

$$\begin{array}{ccccc} \text{Risk}(r) & = & \text{Frequency}(p) & \text{x} & \text{Magnitude}(q) \\ \left(\dfrac{\text{Consequences}}{\text{Unit Time}}\right) & = & \left(\dfrac{\text{Events}}{\text{Unit Time}}\right) & \text{x} & \left(\dfrac{\text{Consequences}}{\text{Event}}\right) \end{array}$$

Figure 18 Probability Assessment



DEFINE FRACTILE ${}^{<}x(f)$

$$\{x < {}^{<}x(f) \mid \&\} = f$$

| f | ${}^{<}x(f)$ |
|---|---|
| 0.01 | -26 |
| 0.25 | - 4 |
| 0.50 | 11 |
| 0.75 | 27 |
| 0.99 | 54 |

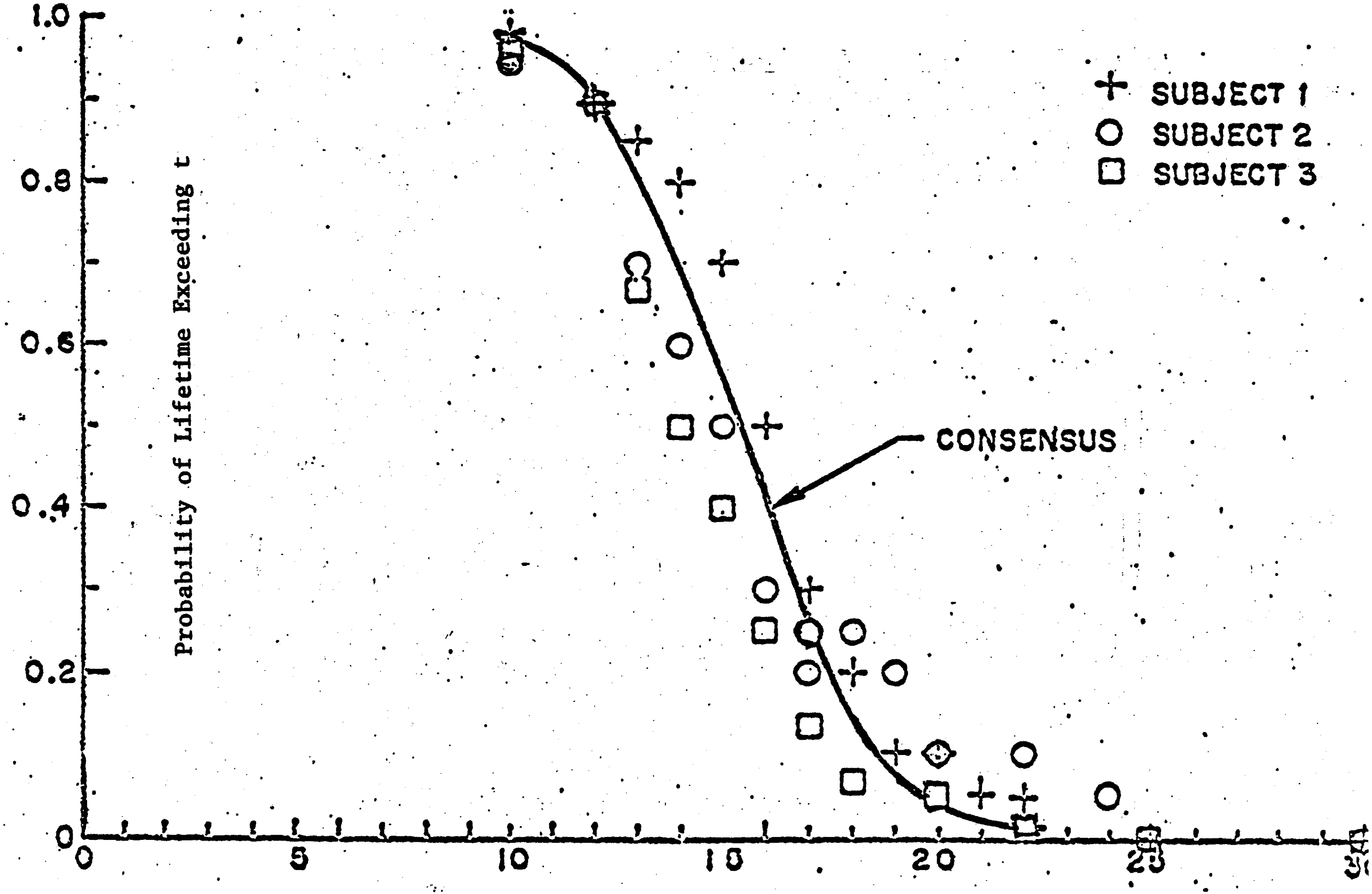
$$\{{}^{<}x(0.25) < x < {}^{<}x(0.75) \mid \&\} = \{x < {}^{<}x(0.75) \mid \&\} - \{x < {}^{<}x(0.25) \mid \&\}$$

$$= 0.75 - 0.25 = \underline{\underline{0.50}}$$

INTERVAL $({}^{<}x(0.25), {}^{<}x(0.75))$ IS CALLED INTERQUARTILE INTERVAL.

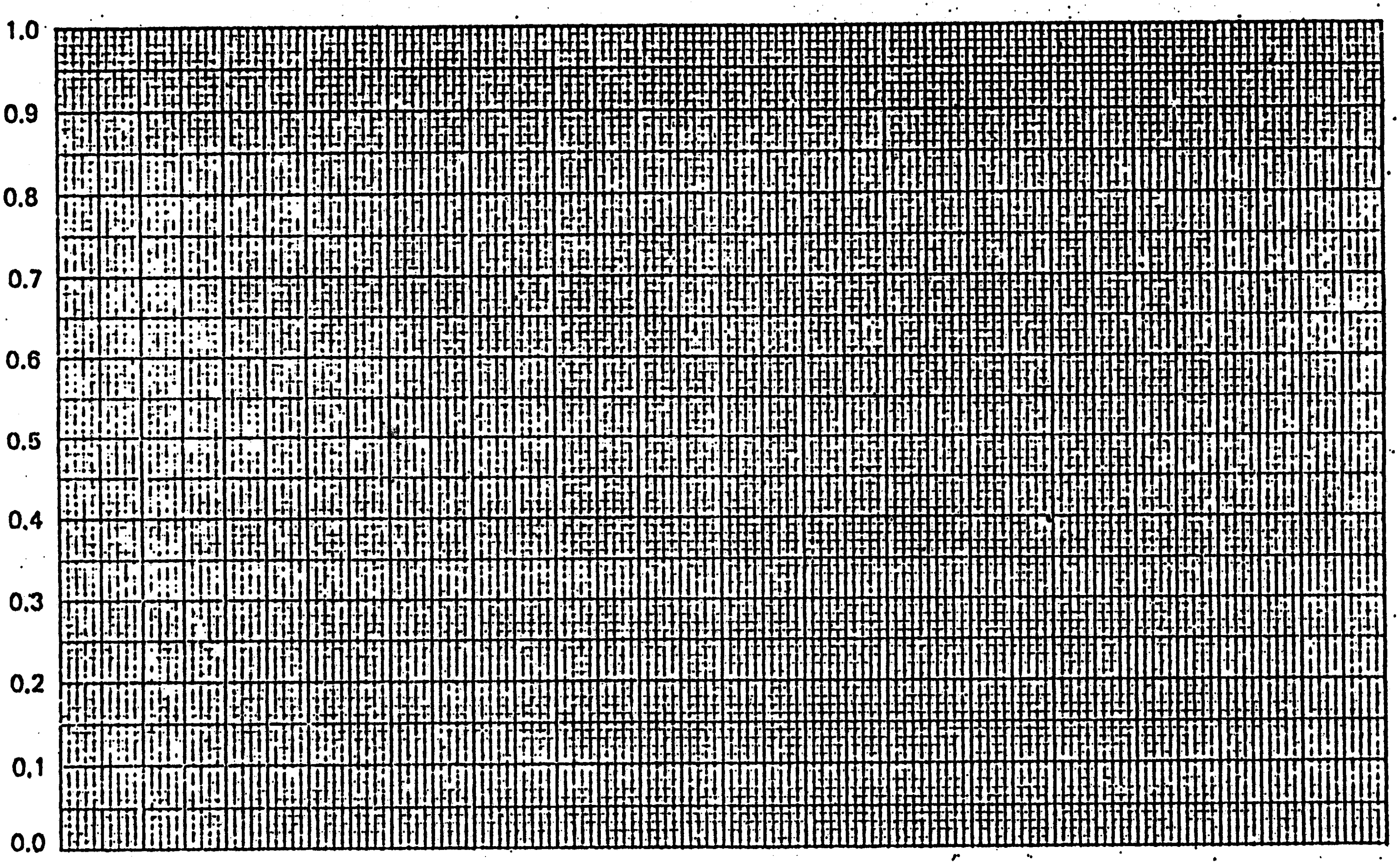
$\{x$ IN INTERQUARTILE INTERVAL $\mid \&\} = 0.50$.

Figure 19 Priors on Material Lifetime



Lifetime t (years)

SUBJECT ______________________ DATE ______________________



VARIABLE ______________________________

SRI—PROBABILITY ENCODING FORM—MAY 1969

Figure 20 Probability Encoding Form

From utility theory [12], the consequence q can be expressed as a utility function u(q) which can be a nonlinear function of q. This function measures the risk preference of an individual or society as a whole to a wide range of consequence magnitudes. Most utility functions are concave and represent a risk adverse attitude toward large consequences; i.e., high consequence-low probability accidents are less acceptable than low consequence-high probability accidents.

A recent Ph.D. thesis at MIT by D. Litai [7] reviews the various risk analysis and risk assessment methods available, and develops a new approach to this problem. The various risk analysis methods available are reviewed in Table I. These include methods that fall under the broad category of <u>economic risk theory</u>:

(i) risk-benefit analysis;

(ii) cost-effectiveness analysis; and

(iii) method of revealed preferences.

A second broad category of methods includes those that fall under <u>demographic risk theory</u>:

(i) expressed preference analysis;

(ii) life-expectancy analysis;

(iii) risk-comparison; and

(iv) natural hazards approach.

The characteristics of each of these methods are described in Table I, including the main features of each, the basic assumptions utilized, the main advantages and drawbacks followed by examples of successful or reasonable use of each method and the principle references for each method.

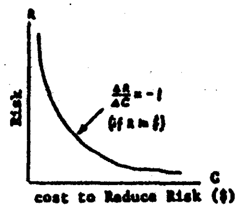
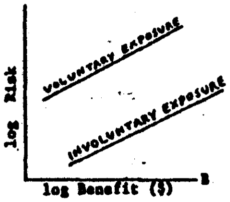
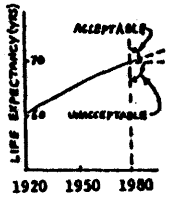
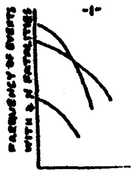
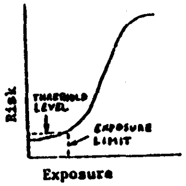
| METHOD | RISK-BENEFIT | COST-EFFECTIVENESS | REVEALED PREFERENCES | EXPRESSED PREFERENCES | LIFE EXPECTANCY | RISK COMPARISON | NATURAL HAZARDS |
|---|---|---|---|---|---|---|---|
| CHARACTERISTIC | | | | | | | |
| Main features, or schematic description | o Benefit>Risk is condition for acceptance<br>o Utility functions can be helpful in quantification process |  |  | o Polls used to assert public opinion on risk issues |  |  |  |
| Basic assumptions | o Risk and Benefit may be quantified in same units ($) | o Expenditure in life saving operations indicates that residual risk is acceptable | o society has arrived at a balance between an activities risk and benefit; observed B-R ratio reveals preferences<br>o Different correlations obtained for different risks | o People understand issues, know what they want | o Only activities that have a net positive effect on life expectancy, or do not compromise life expectancy perceptibly are acceptable | o New risks may be compared to accepted ones of similar nature | o Risk must be reduced to zero tolerance level, i.e., to near natural background levels, or such levels that would make the risk barely perceptible |
| Main Advantages | o Simple convincing analysis if R-B data are given | o Risk need not be expressed in terms of money | o Risk need not be expressed in terms of money<br>o Acceptable risk asserted on graph from known or predicted benefit | o Direct information from public<br>o Public is decision maker<br>o Current ideas prevail, not yesterday's | o Simple and convincing when such balance is possible, and directly appealing | o Easiest method to apply<br>o Simple to understand | |
| Main drawbacks | o Difficult to quantify risk<br>o Judgment of risk and benefits is subjective | o If risk is express in $, same as for risk-benefit method, if not, decision is not clear | o Results depend on numeraire used to measure R and B and on examples used<br>o Too many risk types scatter data points to confound unique correlations<br>o Assumes yesterday's ideas are valid today<br>o Assumes people have freedom of choice and full information<br>o Quantification problems | o People subject to influence, inconsistency, misinterpreation<br>o Actual behavior often not according to expressed opinions<br>o Usual polling problems | o Net effects often very difficult to quantify<br>o Does not explain many human activities (smoking) | o Society may choose not to accept risks, even if similar ones have been accepted before<br>o Due to variety of factors involved in judgment of risks, only risks of the same type may possibly be comparable | o Man is not as risk aversive as assumed by this approach<br>o Many human risks have no corresponding natural background or S shaped risk-exposure relationship (e.g., cars) |
| Examples of successful or reasonable use | o Risk to property or in cases of simple injury | o In industry, to compare various alternatives to reduce risk | o Project management | | o Medical treatment: x-rays, radiation therapy, surgery | o Comparing natural or man-made catastrophical risks<br>o Comparing occupational risks | o Radiation exposure standards |
| References | o Mishan (1971) | --- | o Starr (1969) | o Otway (1977)<br>o Fischhoff et al. (1978) | o Bowen (1976)<br>o Thompson (1979) | o Farmer (1967)<br>o Reactor Safety Study (1975)<br>o Statistical Year Books<br>o Accident Facts | --- |

Table I REVIEW OF RISK ASSESSMENT METHODS [7]

D.2.1 Economic Risk Theory

Methods included in this group are: "risk-benefit", "cost-effectiveness" and the "method of revealed preferences".

Risk-Benefit Analysis

The basic assumption of this approach is that risk and benefit may be expressed and quantified in the same units (same numeraire), usually taken as dollars. Since a risk may involve various consequences, it is necessary to price each one of these before they can be summed. Unit prices must be assigned to fatalities, injuries, and other consequences as well as to the various benefits that may be associated with the risk. Since benefits may also be subject to probabilistic effects, it follows that the expected gain is the net positive outcome, and the expected loss is the net negative outcome. For the project to be worthwhile the first must be higher than the latter. The expected gain is obtained by multiplying all the possible benefits by their corresponding likelihoods and summing their products up. Likewise, the expected loss is the sum of the products of all possible deleterious consequences and their corresponding likelihoods.

Difficulties arise in the quantification process of assigning a dollar value to fatalities and suffering, among other deleterious consequences. Several utility functions* have been proposed to help in evaluating human life. They may be purely economic in their approach,

*A "utility function" is a mathematical descriptor of the way in which a person (or society) values a particular benefit or cost. A linear utility function indicates that the preference toward a given cost or benefit is independent of its absolute magnitude, while non-linear utility functions reveal either a risk preferring or adverse attitude.

or involve psychological factors as well. However, no generally accepted utility function and no generally accepted parameters for any utility function have yet been found. Placing a dollar value on human life is still very controversial.

## Cost Effectiveness Analysis

Cost effectiveness is a special case of cost-benefit analysis. Here, the benefit considered is that of risk reduction. For any project which involves some risk, it is possible to reduce the risk to almost any desirable level, but the effort costs money. The question of how much risk is acceptable has been replaced here by how much society is willing to pay to avoid a risk. The trade-off point is defined to be where $\frac{\Delta R}{\Delta C} = -1$, but to find this point it is necessary to measure risk and cost in the same units (i.e., dollars). If risk is measured in some other way, then the question how much to invest is open again.

Experience shows that public expenditures for risk aversion varies from \$100 for automobile seat belts to \$10 million for removing $^{90}$Sr from milk for averting one death [7]. No consistent reasoning behind this practice has been found that could explain these tremendous variations. So the question of how much to spend remains open.

## Revealed Preferences

This method suggests that society has revealed its preferences toward risk-taking in its present and past behavior. The method is based upon taking present and past data on the level of risk faced in various human activities (e.g., work, travel and leisure activities) and comparing the implied risk preference level between the activities. Starr suggested such a method in 1968, and this method is expanded upon by Litai [7]. Fischoff et al., identified several drawbacks in the method: "the method assumes that past behavior is a valid predictor of present preferences, which may not always be true". Even in spite of the method's drawbacks, the approach suggested by Starr may not be invalid. As Starr notes: "by trial and error, society has arrived at an essentially optimum balance between the risk and benefits of any activity", which may be a valid statement. While it is quite conceivable that this state of balance, or equilibrium, is not a static but dynamic one, which changes with time as new perceptions of risk and benefit develop, this shift is quite slow. Many examples abound which show that in spite of abundant information and freedom of choice, societal attitudes have changed very little if any (smoking, contraceptives, alcohol). Thus, it may be that basic relationships should be updated from time to time, say, every five years, yet they do represent a certain societal "equilibrium" even if only a temporary one. It may well be that this equilibrium is not the optimal one, and that choice is not always rational (smoking provides again a good example), yet equilibrium it is, and thus, indicates societal preferences.

### D.2.2 Demographic Risk Theory

Demographic risk theory refers to methods that do not actually attempt to quantify and balance risk against benefit, but seek to find other ways to determine what level of risk might be acceptable for a given activity. In particular, risks that have a potential for fatalities are of concern here, since these are more easily conceptualized, and, therefore, easier to compare. It should be remarked, at this point, that perhaps all methods for assessing risk acceptability are basically risk-benefit analysis. But in demographic risk theory, the analysis is not carried out explicitly - certainly not in terms of money - and is hidden in most cases in the subtle comparisons or distinctions that are made.

## Expressed Preferences

This method attempts to avoid the difficulties associated with the method of revealed preferences, or risk-benefit methods in general, by asking people directly what levels of safety they deem acceptable. This method has been advocated by Otway (1977), and by Fischhoff et al., (1978) and (1979), although it was recognized by them that people may be baffled by such problems, influenced by the selection and enunciation of the problems laid before them, prone to change their mind, and generally inconsistent in their responses. Other deficiencies of public-poll techniques tend to bias the results of this kind of analysis.

## Life Expectancy Formulations

Bowen (1976), and Thompson (1979) among others have advocated the use of the life expectancy method which presumably simplifies decision-making by putting the evaluated risk in the perspective of its potential influence of the total expected span of man's life. It is possible by using statistical methods to calculate the effect on life expectancy of eliminating, or adding a given risk. Thus, eliminating the risk of motor vehicle accidents, life expectancy would rise by 0.8 years, and adding the risk of nuclear energy life would be shortened by 18 seconds (Thompson, 1979). Even if we assume that the risk of nuclear energy was 10,000 times higher than the value used in the previous calculation (taken from the Reactor Safety Study (WASH-1400, 1975), the effect would still be of the order of one day or so, still a far cry from the penalty we pay for the use of motor vehicles. All this would be quite clear from the mortality rates themselves, but this method of representation adds another perspective which may be of help sometimes in deciding the question.

Perhaps every technology has had some influence on human life expectancy, but its assessment is very often intractable. The total contribution of all human undertakings has obviously so far been positive, since we now live longer than previous generations did. In general, then, a project may be deemed acceptable if it contributes a net positive increment to life expectancy, or at least does not compromise it too highly (Figure 2.4). In Figure 2.4 a horizontal extrapolation is used as the limit of acceptability, but this is not necessarily so.

## Risk Comparison

This is the most commonly practiced method of risk assessment. Frequencies of mortality, morbidity, and other damage are compared directly between various activities, between one year and another, between countries, cities, and the like "in order to encourage some desired action or reveal some inconsistency". The method assumes that risks that have been accepted in the past will also be accepted in the future. (A similar argument has been raised and discussed in connection with the method of revealed preferences.) The method is often used without due attention to the various factors which govern human perceptions of risk, thus comparing, for example, voluntary and involuntary, immediate and delayed, ordinary and catastrophic, etc., risks without discrimination. It may be reasonably thought that only risks that invoke the same perceptions, which we shall call henceforward risks of the same type or category, may be comparable in this way. (Litai deals directly with this problem in his methodology formulation.)

Natural Hazard

This is a risk averse approach based on the assumption that all risks are unacceptable unless they are barely perceptible. This may happen when the risk in question is small compared to a naturally existing background (cancer), or if the risk-exposure relationship shows a low threshold level. Examples where such an approach may seem appropriate do exist (radiation exposure risks) but in general, human behavior again indicates that much higher risks than would be admissible by this approach are readily acceptable.

### D.2.3 An Expanded Revealed Preference Method (Litai [7])

The work of Litai is based upon the method of revealed preferences and defines nine risk conversion factors that affect a risk comparison assessment. These are:

(i) natural vs manmade risk;

(ii) voluntary vs involuntary risk;

(iii) ordinary vs catastrophic risk;

(iv) delayed vs immediate risk;

(v) necessary vs luxury risk;

(vi) old vs new risk;

(vii) regular vs occasional risk;

(viii) controllable vs uncontrollable risk; and

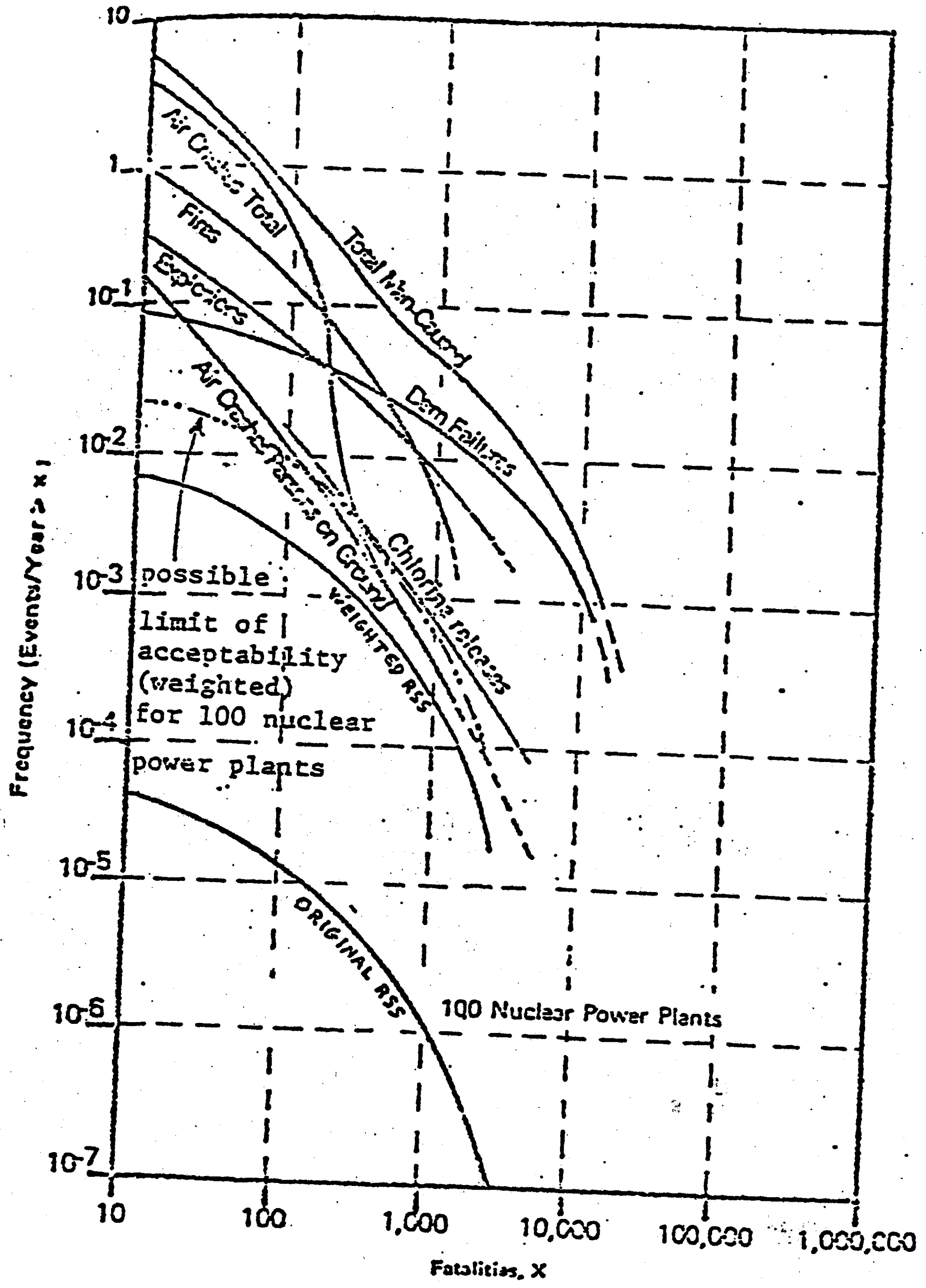
(ix) direct vs indirect risk.

These factors influence, for example, a comparison of nuclear with coal-fired electrical generating technology risks (i.e., nuclear is a man-made involuntary catastrophic risk, while coal is a man-made involuntary ordinary risk). The method provides a way for combining delayed with immediate fatalities (e.g., WASH-1400 results have been combined together in this way by Litai; see Figure 21). Litai examined past data on various types of risks (data from insurance company records) and established risk profile histograms that, when divided into each other for each of the nine dichotomous pairs above, rendered integral risk conversion factors that can be used to multiply (or divide) risk numbers so that each cateogry may be compared with the others.

Litai's work deals with the problem of acceptable risk. Six such factors were found to be of major importance in risk evaluations and value judgments: volition, severity, manifestation of effort, familiarity, controllability, and origin. Three other factors were also found interesting but less important: necessity, exposure pattern and benefit factor. Risk distributions for four different risk categories were developed: immediate and delayed occupational risks, smoking and homicide, ill-based or historical data available from insurance companies.

Based on this work for the spectrum of human physical-mortality risks examined, mortality risks between $4x10^{-3}$/person-yr to $\sim 10^{-9}$/person-year were encountered. The former value relates to the highest

Figure 21 Litai's Combination Delayed with Immediate Fatalitics in WASH-1400.



tolerated human risk, the latter to the lowest magnitude that is, perhaps, physically possible.

Risk conversion factors based on this work are given in Table II, where they are compared with results from earlier studies. Litai suggests that risk design criteria could be derived from the methods of his study which would be compatible with historical U.S. societal perceptions of the involved risk types. The risk conversion factors and distributions seem to indicate why society seems to spend "unreasonable" sums to avert death in some cases while spending much less in other cases. These observations and the basic consistency of the derived vales are believed to demonstrate the validity of the model results. However, an accuracy to no better than a factor of two to three can be claimed for the derived values, and is limited to comparison of mortality risk only; further work would be required to extend the results to other forms of risk (e.g., injuries, plant damage and equipment loss, lost work days, indices of harm, etc.). Further work could also be done to investigate the relative importance and globality of the risk factor categories; others may need to be added (or deleted). Continued work in these directions may lead to other areas helping to shed more light on the question of how safe is "safe enough".

## Table II

## RISK CONVERSION FACTORS FOR RISK PAIRS (Litai [7])

| Characteristic Risk Pairs | | Risk Conversion Factors | | | | |
|---|---|---|---|---|---|---|
| | | Litai (1980) | Rowe (1977) | Starr (1969) | Kinchin (1978) | Otway/ Cohen (1975) |
| Origin | Natural/Man-Made | 20 | 10 | | | |
| Severity | Ordinary/Catastrophic | 30 | 50 | | | |
| Volition | Voluntary/Involuntary | 100 | 100 | ∿1000 | | 1-1000 |
| Effect | Delayed/Immediate | 30 | 20%/yr | | 30 | |
| Controllability | Controllable/Uncontrollable | 5-10 | 100 | | | |
| Familiarity | Old/New | 10 | | | | |
| Necessity | Necessary/Luxury | 1 | | | | |
| Exposure | Continuous/Occasional | 1 | | | | |
| Benefit | Clear/Unclear | n/a* | | | | |

*n/a = not applicable

## E. Examples of Aoplication to Sample Problems

### E.1 Fault and Event Trees

### Fault Tree Example

Fault trees are used to calculate the failure probabilities of engineering systems. An example of such an application is in calculating the probability that a warehouse fire protection system would fail to put out a fire on demand. The protection system consists of pumps, motors, and valves that pump water out of a nearby river. During a fire, the protection system is designed to quench the flames by spraying water through a nozzle installed on the warehouse ceiling. A system diagram is shown in Figure 22.

Question: The task is to construct a fault tree to calculate the failure probability on demand.

Answer: The solution to this problem is to begin by following the steps for fault tree construction. The first step is to define a TOP event.

Examples of a correct description of the TOP event include "Fail to Put Out Fire on Demand", or "System Fails to Put Out Fire". (Incomplete descriptions would be "No Sufficient $H_20$ Out of Nozzle", or "Fire Not Put Out", or "System Works But No Fire".)

Next, define events that lead to the TOP event. These include

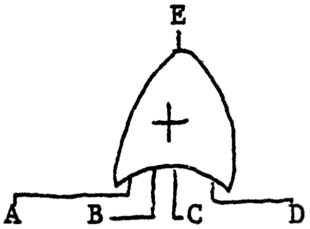
1. Fire Fails to Trip Detectors (No Signal Out of Detectors);
2. Detector Signals But Motor Fails to Operate;
3. Pump Motor Operates But Fails to Deliver Water Out of Nozzle; and
4. Water Out of Nozzle But Fails to Put Out Fire.

Then, these events must be broken down into basic events where probabilities can be meaningfully assigned. Events (1) and (4) are broken down further for purposes of example (Figure 23). This procedure would be followed until all four major events were broken down into basic events; then, the tree would provide the vehicle by which the probabilities would be combined together mathematically to arrive at the failure probability corresponding to the TOP event. (An example of a simple calculation is gfven below.)

Example of Probability Calculations in Fault Trees

(i) "OR" Gate

Question: Event E is related to Events A, B, C, and D as shown:



"OR"

What is the probability of E if:

(a) $P_A = 0.1$ $P_B = 0.2$ $P_C = 0.4$ $P_D = 0.5$

(b) $P_A = 0.01$ $P_B = 0.02$ $P_C = 0.04$ $P_D = 0.05$

(c) Derive an expression for the error if the approximation $P_E \overset{\sim}{=} P_A + P_B + P_C + P_D$ is used (instead of the exact expression) in terms of $P_A$, $P_B$, $P_C$, and $P_D$.

Solution:

$$E = A + B + C + D$$

$$P_E = 1 - \overline{P}_A\overline{P}_B\overline{P}_C\overline{P}_D$$

$$= 1 - (1-P_A)(1-P_B)(1-P_C)(1-P_D)$$

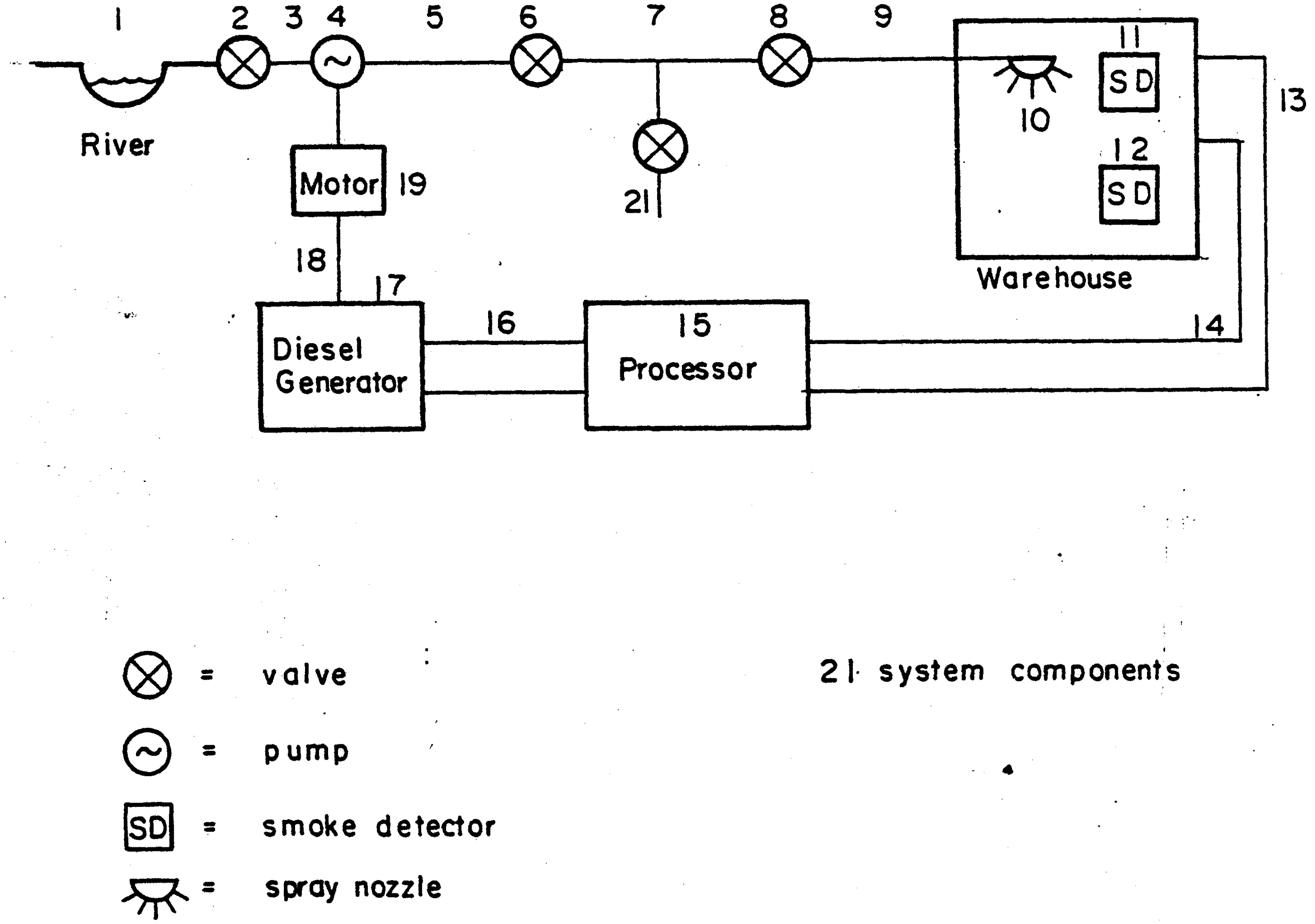


Figure 22 Fire Protection System for Warehouse

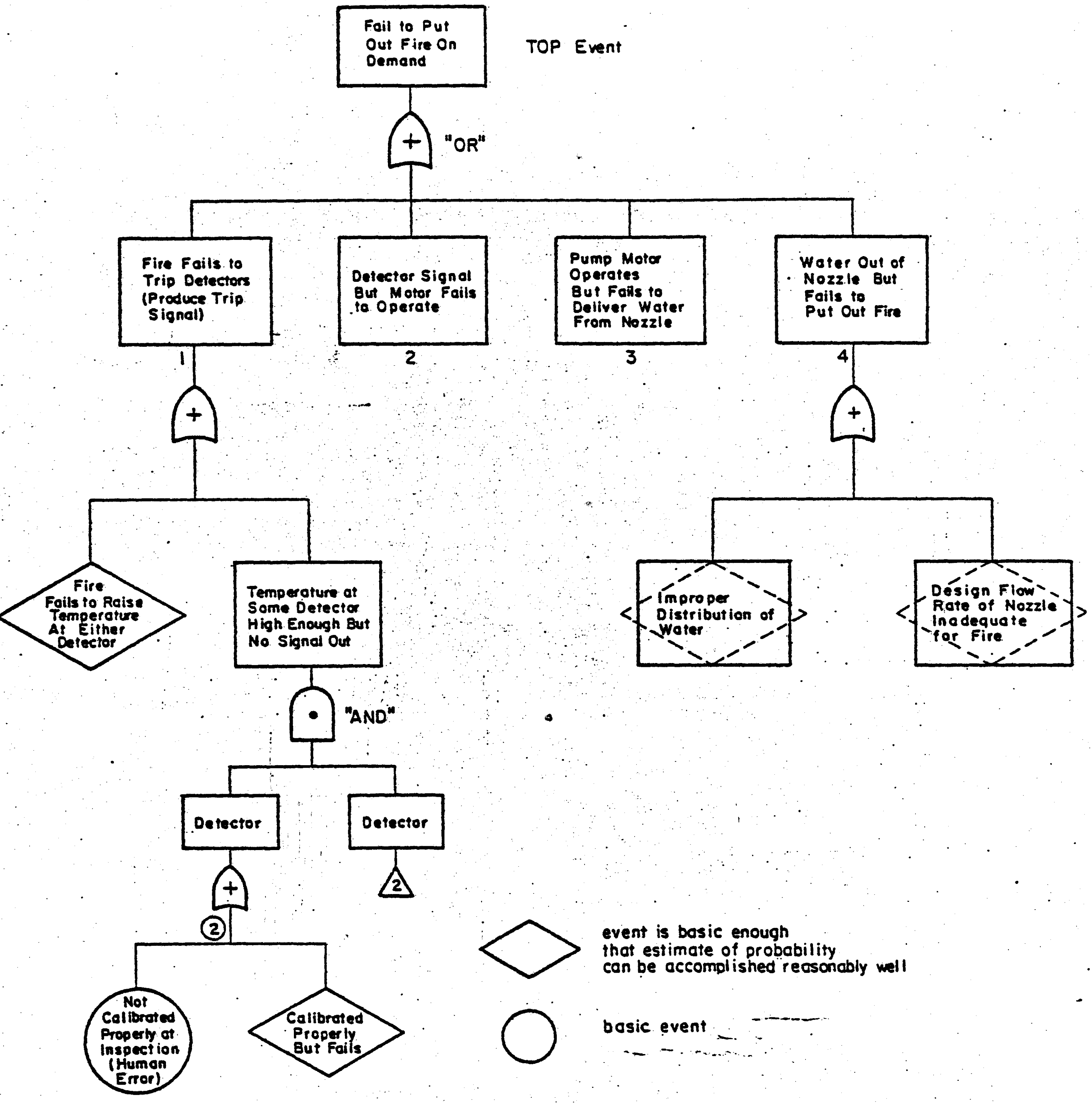

Fail to Put Out Fire On Demand
TOP Event
+
"OR"
Fire Fails to Trip Detectors (Produce Trip Signal)
1
Detector Signal But Motor Fails to Operate
2
Pump Motor Operates But Fails to Deliver Water From Nozzle
3
Water Out of Nozzle But Fails to Put Out Fire
4
+
+
Fire Fails to Raise Temperature At Either Detector
Temperature at Some Detector High Enough But No Signal Out
•
"AND"
Improper Distribution of Water
Design Flow Rate of Nozzle Inadequate for Fire
Detector
Detector
+
2
2
Not Calibrated Properly at Inspection (Human Error)
Calibrated Properly But Fails
event is basic enough that estimate of probability can be accomplished reasonably well
basic event

Figure 23 Abbreviated Fault Tree for Warehouse Example (with Development of Events # 1, 4)

$$
\begin{aligned}
\text{(a)}\quad P_E &= 1 - (1-0.1)(1-0.2)(1-0.4)(1-0.5)\\
&= 1 - (0.9)(0.8)(0.6)(0.5)\\
&= 1 - 0.216\\
&= 0.784
\end{aligned}
$$

$$
\begin{aligned}
\text{(b)}\quad P_E &= 1 - (1-0.01)(1-0.02)(1-0.04)(1-0.05)\\
&= 1 - (0.99)(0.98)(0.96)(0.95)\\
&= 1 - 0.8848\\
&= 0.1152
\end{aligned}
$$

$$
\begin{aligned}
\text{(c)}\quad P_E &= 1 - (1-P_A)(1-P_B)(1-P_C)(1-P_D)\\
&= 1 - (1-P_A-P_B+P_AP_B)(1-P_C-P_D+P_CP_D)\\
&= 1 - (1-P_A-P_B-P_C-P_D+P_AP_B+P_AP_C+P_AP_D\\
&\qquad + P_BP_C+P_BP_D+P_CP_D-P_AP_BP_C-P_AP_BP_D\\
&\qquad - P_AP_CP_D-P_BP_CP_D+P_AP_BP_CP_D)\\
&= (P_A+P_B+P_C+P_D) + [-P_AP_B-P_AP_C-P_AP_D\\
&\qquad\qquad -P_BP_C-P_BP_D-P_CP_D\\
&\qquad\qquad +P_AP_BP_C+P_AP_BP_D\\
&\qquad\qquad +P_AP_CP_D+P_BP_CP_D\\
&\qquad\qquad -P_AP_BP_CP_D]
\end{aligned}
$$

when $P_E$ is approximated by

$$P_E \simeq P_A+P_B+P_C+P_D$$

the error is the square bracket terms.

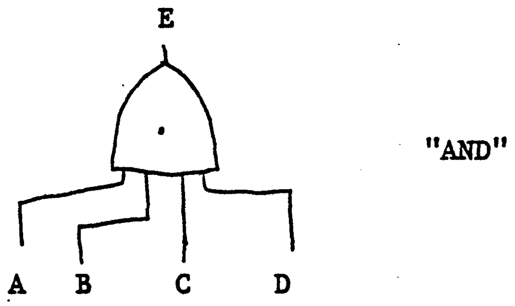
Example: (a) $P_E \simeq 0.1 + 0.2 + 0.4 + 0.5 = 1.2$

(b) $P_E \simeq 0.01 + 0.02 + 0.04 + 0.05 = 0.12$

when Pi have the same order of magnitude, the error $\simeq 0(P_i^{\,2})$.

(ii) "AND" Gate

Question: Event E is related to Events A, B, C, and D as shown: (assume A, B, C, and D independent events)



What is the probability of E if:

(a) $P_A = 0.1$, $P_B = 0.2$, $P_C = 0.4$, $P_D = 0.5$

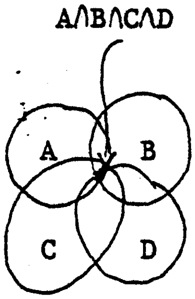
(b) $P_A = 0.01$, $P_B = 0.02$, $P_C = 0.04$, $P_D = 0.05$

(c) Suppose A, B, C, and D were dependent events. Then what would the expression for $P_E$ be:

Solution:

$$E = A \cdot B \cdot C \cdot D$$

$$P_E = P_A \cdot P_B \cdot P_C \cdot P_D$$



(a) $P_E = (0.1)(0.2)(0.4)(0.5) = 4 \times 10^{-3}$

(b) $P_E = (0.01)(0.02)(0.04)(0.05) = 4 \times 10^{-7}$

(c) $P(E|A,B,C,D) = P(A|BCD)\,P(B|ACD)\,P(C|ABD)\,P(D|ABC)$

$$= \frac{P(A)P(BCD|A)}{P(BCD)} \cdot \frac{P(B)P(ACD|B)}{P(ACD)}$$

$$\cdot \frac{P(C)P(ABD|C)}{P(ABD)} \cdot \frac{P(D)\ (ABC|D)}{P(ABC)}$$

$$= P(A)(B)P(C)P(D) \quad \frac{P(BCD|A)P(ACD|B)P(ABD|C)P(ABC|D)}{P(BCD) \quad P(ACD) \quad P(ABD) \quad P(ABC)}$$

(Note that given A was independent from B, C and D, then

$$P(BCD|A) = P(BCD) \text{ by definition.}$$

Then the expression for P(E) reduces to $P(E) = P(A)P(B)P(C)P(D)$.

Event Tree Example

Question: Construct an event tree that correctly relates the functions of each of the following engineered safety features (ESF) to determine possible event sequences that could lead to negative consequences.

Begin the tree with the initiating event being a pipe break (PB). The systems are:

(a) Reactor shutdown or "trip" (RT) to stop significant power generation due to the fission process during the LOCA.

(b) Emergency core cooling (ECC) to cool the core to keep the release of radioactivity from the fuel into the containment at low levels.

(c) Post accident radioactivity removal (PARR) to remove from the containment atmosphere the radioactivity that could be released from the core.

(d) Post accident heat removal (PAHR) to remove the core decay heat from the containment to prevent its overpressure.

(e) Containment integrity (CI) to prevent the radioactivity not removed by PARR from being dispersed into the environment.

Solution: (from Ref. [15]).

In considering the events involved in a LOCA after the pipe break that is the initiating event, one must consider the functions that the ESFs are required to perform. Regardless of the design details of a particular reactor, the ESFs perform a uniform set of functions.

The event tree is started by indicating these functions, i,e., RT, ECC, PARR, PAHR, and CI, together with the initiating event, pipe break (PB), as event tree headings, in roughly chronological order. It proceeds from left to right by the addition under each heading of branches corresponding to two alternatives: successful performance of function (upper branch) and failure (lower branch). After the tree is drawn, paths across it can be traced by choosing a branch under each successive heading. Each path corresponds to an accident sequence. Six headings, five of which have two alternatives, result in a $2^{n-1}$ (where n = 6) event tree representing 32 accident sequences, designated S1 to S32. Figure 25 illustrates the design basis LOCA defined in the regulatory process.

When more headings are used because ESF systems replace the functional headings, the number of sequences can be quite large. Analysis of individual sequences indicates that many of them are illogical or meaningless and can be eliminated. In the process of increasing the detail in the headings and eliminating the unneeded sequences, continuing attention must be given to the order of the headings. Tree development is facilitated when the order corresponds generally to the logic of the accident process, i.e., when the headings

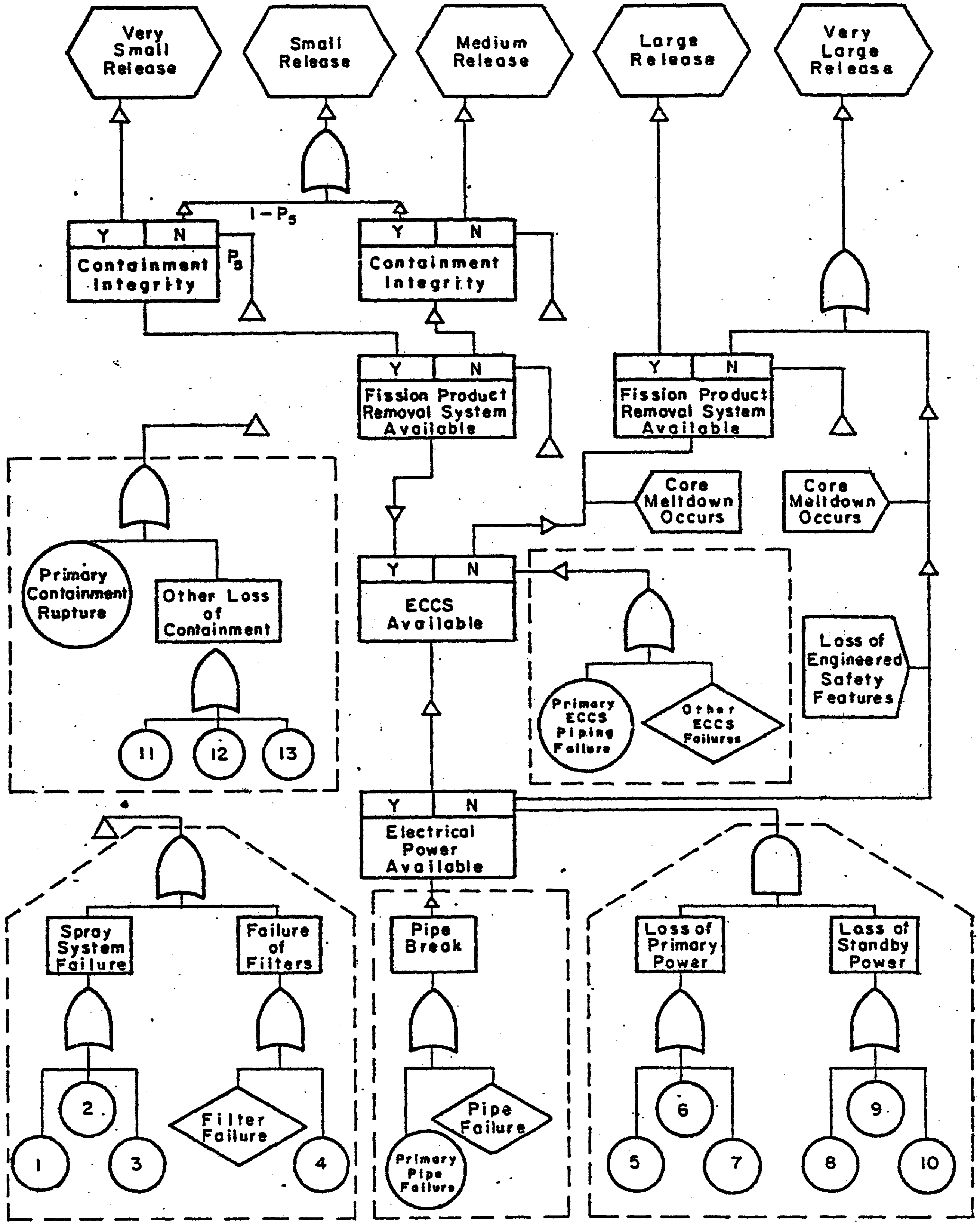


Figure 24 Cause-Consequence Diagram for Hypothetical LOCA

whose failure affects the failure of others are located early in the tree. The rationale for the order in Fig. 25 is as follows:

(a) RT is listed first because failure to shut down the fission process during a LOCA could result in high core temperatures and thus nullify the effectiveness of ECC even if cooling water were provided.

(b) ECC is listed next because cooling determines whether or not the core will melt. If it does not, the consequences of pipe break will be very small; but if the core does melt, the potential consequences can be large and are strongly affected by PARR, PAHR, and CI.

(c) PARR comes after ECC because its function is to remove any radioactivity released from the fuel into the containment.

(d) PAHR is put just before CI because the containment has failure modes that depend on the performance of PAHR (as well as on ECC).

The form of the tree does not imply independence among failure events. Dependent as well as independent events can be handled provided the dependencies are appropriately defined.

Further development of the event tree requires analysis of the physical processes, such as core melting or overpressurization of the containment, that could occur when one (or more) of the functions is not performed. The analysis must include consideration not only of functional interrelationships but also of the interrelated operational factors involved with the physical systems provided to perform the functions. Such analyses are important also in the study of common mode failures because they define, if properly done, the only significant logically permissible sequences (i.e., those that appear in the event trees) and eliminate all others. Common mode failures need be considered only for the sequences remaining in the completed event tree.

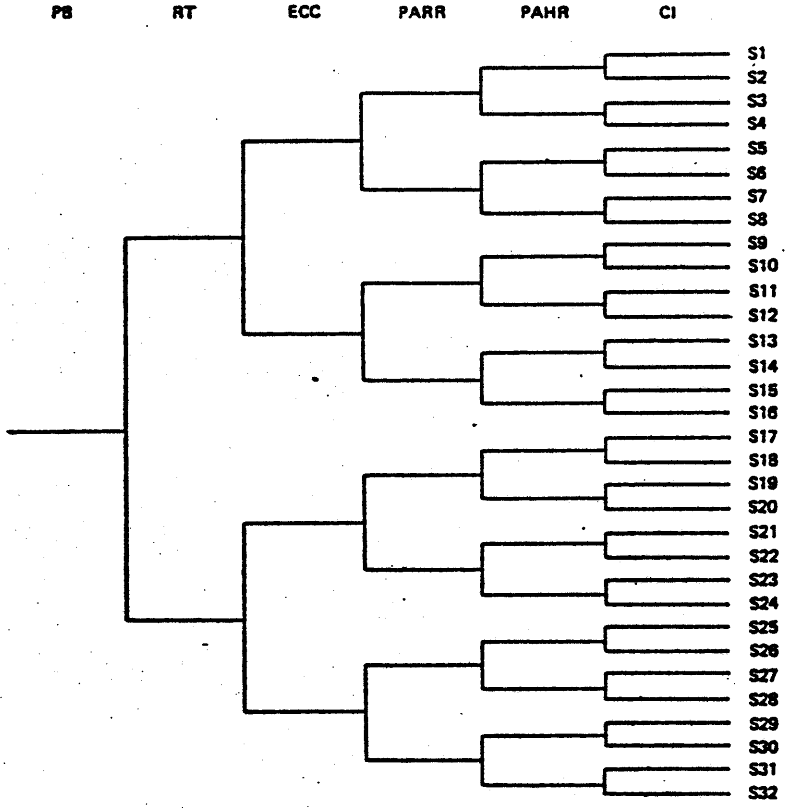


Figure 25 Simplified Event Tree for a LOCA in Typical PWR [15]

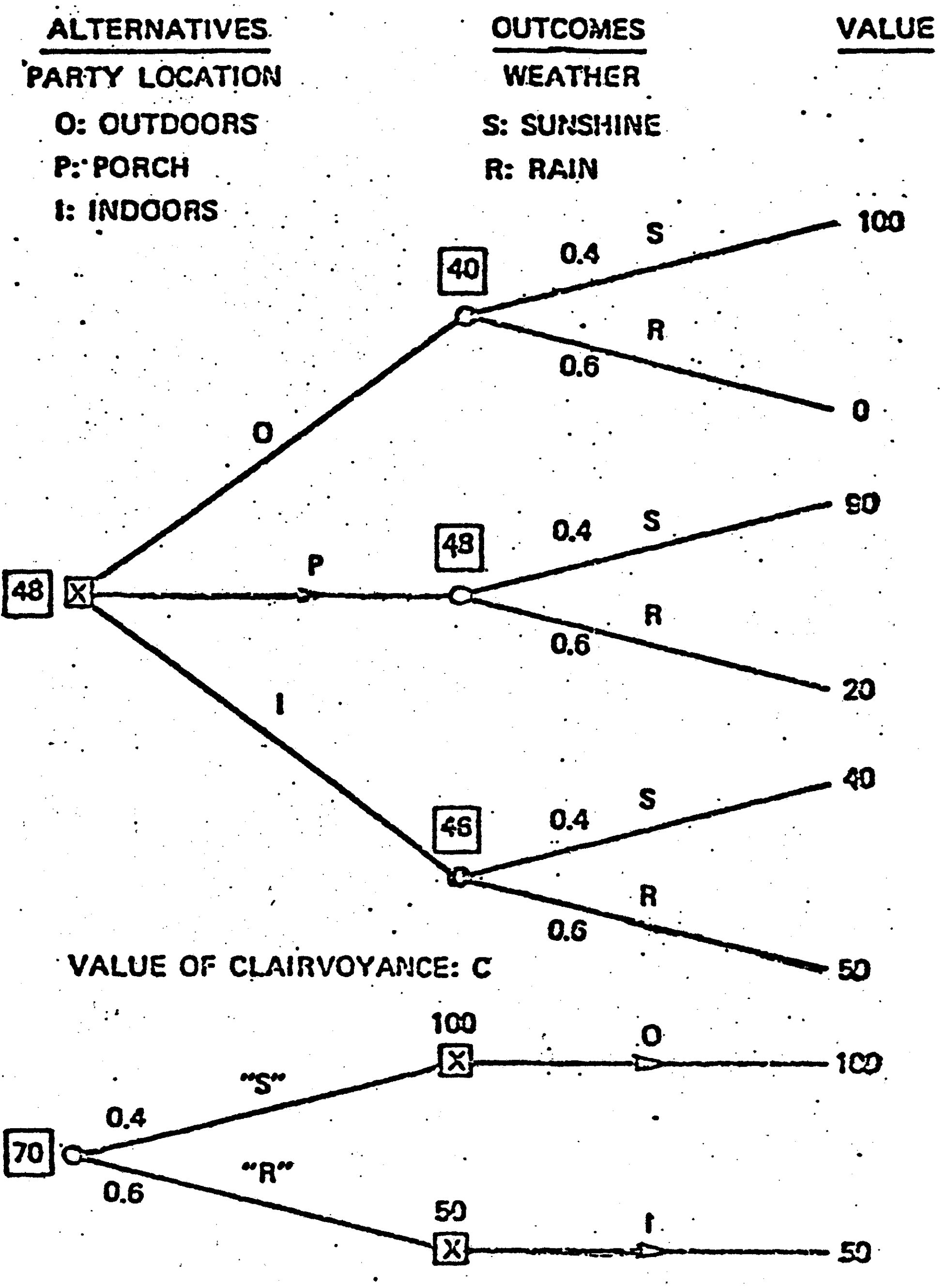
E.2 Cause-Consequence Diagrams

A typical example of the use of cause-consequence analysis is in modeling a loss-of-coolant accident (LOCA) in a typical nuclear power plant. The cause-consequence diagram for this case is given in Figure 24 where the initiating event is a pipe break in the main coolant system of a PWR. The corresponding event tree is shown in Figure 25.

E.3 Decision Tree Example: The Weather Prediction Problem

As an example of a decision problem, consider the case where a person is deciding between locations for a party to be given the next day. The alternatives are outdoors (O), the porch (P), and indoors (I). We model this decision as a decision tree with three branches, one for each alternative location (Figure 26). The possible outcomes of each decision alternative refer to the weather and are discretized into two possibilities: sunshine (S) or rain (R). These two weather conditions are considered mutually exclusive events, so $P_R = 1-P_S$ and vice versa. The probabilities of these events are independent of the decision alternative, but the values placed on them are dependent on the alternative. For example, if the party takes place outdoors and it rains, the value to the decision maker is 0 (units of happiness, dollars, or imagine what you will). However, if it's sunny, the party will be a tremendous success and the value to the decision maker is 100 units, the maximum he can assign. (Likewise, values are assigned to the other alternative outcomes.) To analyze which alternative is "best" (optimal), the expected value of the lottery is calculated by multiplying the value placed on the outcome by the probability of

Figure 26 A Party Problem



EXPECTED VALUE WITH CLAIRVOYANCE = 70

EXPECTED VALUE WITHOUT CLAIRVOYANCE = 48

EXPECTED VALUE OF CLAIRVOYANCE = 22

the outcome and summing it together at the event node. For $P_S = 0.4$ and $P_R = 0.6$, the alternative with the highest expected value is P (porch), with an expected value of 48 units (compared with 40 for "O" and 46 for "I") since (0.4) (90) + (0.6) (20) = 36 + 12 = 48.

The question is now asked: "What is the value of knowing <u>for certain</u> what the weather will be?" In other words, suppose an experiment could be run that guarantees perfect information, what would the decision-maker be willing to pay to run the experiment? This amount is called the value of clairvoyance (C in this example). It is calculated by reversing the event/decision tree around so that the outcomes to the left-hand side first, and then the optimal alternative that corresponds to each outcome is chosen representing a kind of "decision in retrospect". The value at each decision node is thus equal to one times the value of each alternative, and the expected value of the decision with clairvoyance equals the probability of each outcome times the value at each decision node. In this example, $EV_C = (0.4) (100) + (0.6) (50) = 70$. Then, C is calculated by subtracting the expected value of the lottery without clairvoyance ($EV_{NC} = 48$), from the expected value with clairvoyance: $C = EV_C - EV_{NC} = 70 - 48 = 22$. If the units are dollars, this says the decision maker is willing to spend 22 dollars to run the perfect experiment.

<u>Probability Assessment: Coin Tossing</u>

Consider repeated tossing of a fair coin where H = head, T = tail. Let n = number of tosses required to complete the first H H H sequence. For example, consider the sequence H T T H H H T H ... which implies n = 6 tosses. Suppose we want to subjectively assess the

Figure 27 Probability Assessment: Coin-Tossing

| f | 0.01 | 0.25 | 0.50 | 0.75 | 0.99 |
|---|---|---|---|---|---|
| ≤n(f) | | | | | |

Subjectively assess what the values n will be for each value of f and for each of the following sequences:

| f | 0.01 | 0.25 | 0.50 | 0.75 | 0.99 |
|---|---|---|---|---|---|
| HHH | | | | | |
| HTH | | | | | |

Note:

The actual values of the discretized distributions $\phi$ are:

| | | | | | |
|---|---|---|---|---|---|
| HHH | 3 | 5 | 10 | 19 | 57 |
| HTH | 3 | 4 | 7 | 13 | 38 |

Compare your own values with the actual values.

probability distribution function $\phi$ where: $\phi = \{n \leq n(f)|\varepsilon\} = f$, $f = 0\text{-}1$ and $n(f)$ is the value assumed for $n$ as a function of the frequency value $f$. We will assess $\phi$ at five values of f: 0.01, 0.25, 0.50, 0.75 and 0.99 as follows. Draw a box for each value of f that we will fill in for n, the number of tosses (Figure 27).

## E.4 Risk Analysis and Assessment Methods

An example of the use of risk analysis and assessment methods is provided here making use of the method of Litai described earlier in section D.2. (The examples taken here are derived directly from Litai's thesis [7].)

### E.4.1 Nuclear Energy

Nuclear energy, because of the radiation sickness and contamination problems involved in a major accident, is considered a new type of risk. Also, it has both immediate and delayed effects. An "equivalent" one-category representation may be employed by multiplying the immediate risk by 30, the risk conversion factor in this case, and adding it to the delayed risk (or dividing the delayed risk by 30 and adding it to the immediate risk). The sum total must be within the limits of the respective distribution corresponding to the size of population at risk (∿15,000,000 for 100 reactors, from the Reactor Safety Study).

WASH-1400 predicted 2 latent fatalities per year among the 15,000,000 exposed population, and one immediate fatality in 20,000 years per reactor, or 1 in 200 years per 100 reactors. The immediate risk is, therefore, $\frac{1}{200\text{x}15\text{x}10^6} = 3\text{x}10^{-10}$ per person and year, and the delayed risk is $\frac{2}{15\text{x}10^6} = 1.4\text{x}10^{-7}$ per person and year. The total weighted delayed risk is $3x10^{-10} + 1.4x10^{-7} = 1.5x10^{-7}$, and the weighted immediate risk is $3x10^{-10} + \frac{1.4x10^{-7}}{30} = 5.3x10^{-9}$ (Figure 21).

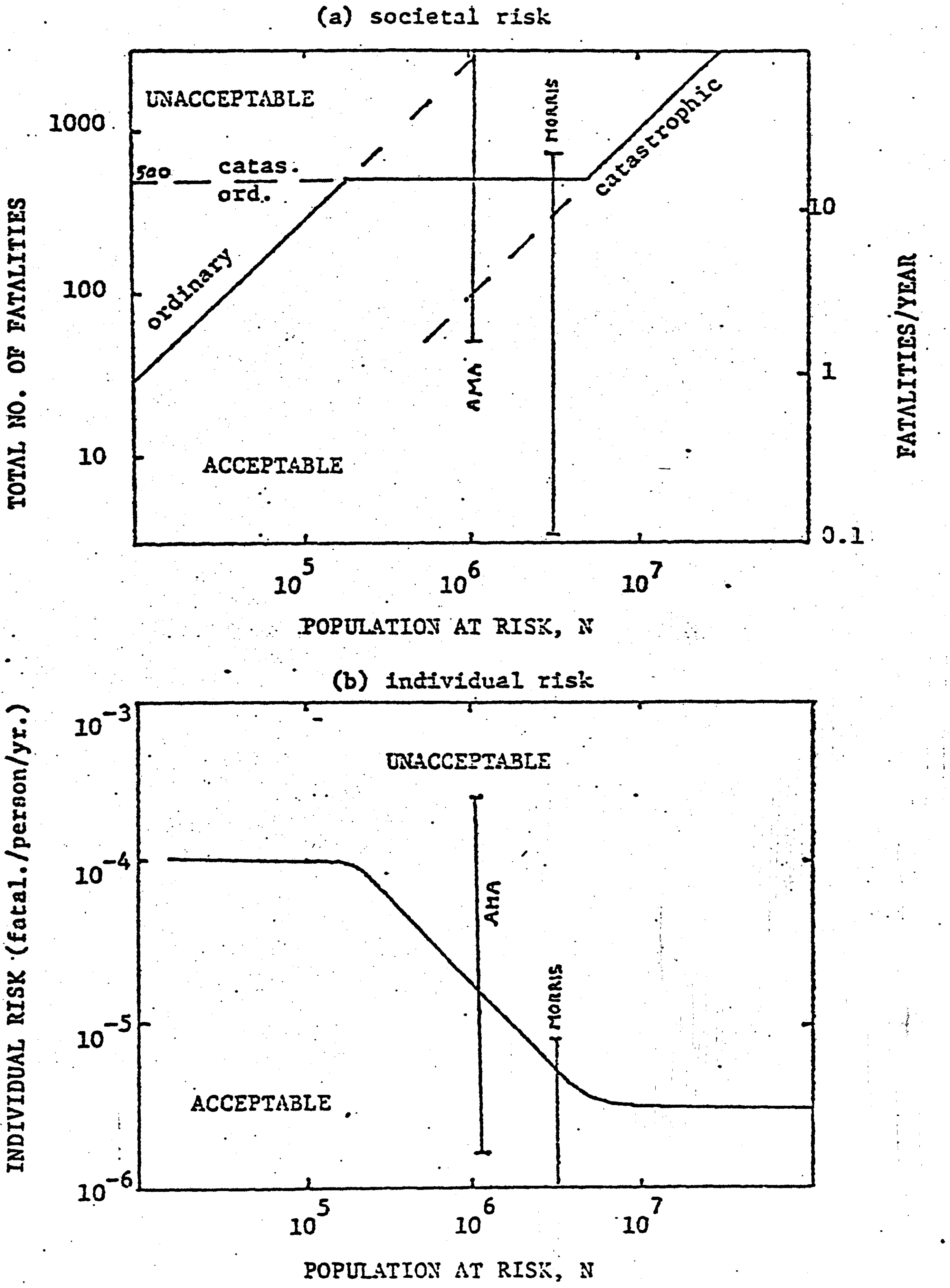
Another important conclusion may be drawn from the foregoing calculation: it seems that the delayed risks are much more important than the immediate ones. Even after dividing by 30, the delayed risk is still 15 times higher than the immediate risk. In order to adjust the curve for the immediate and delayed fatalities related to the 100 nuclear power plants, it must be raised by a factor of ∿15. Moreover, in order to convert it from "new" to "old" (assuming that today it is still an unfamiliar risk) for direct comparison with the other curves in Figure 21, it must be weighted by another factor of ∿10. Hence, a total weighting factor of ∿150 must be applied. This brings the original curve much closer to the crowded region in the figure where most other industrial catastrophes are located.

### E.4.2 Coal Energy

Coal fueled power plants are an important and growing part of our electricity production, but these plants can also pollute the air and water which can kill people.

Pollution is the combined effect of many industrial and domestic emissions. But when a single source can be identified and blamed for a large number of fatalities, its risk may be considered catastrophic. The uncertainty in estimating the effects of a coal power plant on the surrounding population is large.

Studies indicate that the annual individual mortality risk to persons living in the vicinity of a 1000 MWe coal power plant may be anywhere between $10^{-6}$ and $3x10^{-4}$. For an exposed population of size N,



(a) societal risk

(b) individual risk

FIGURE 28 ACCEPTABLE RISK FROM COAL FIRED POWER PLANTS FOR VARIOUS URBAN SITES

and for the total number of fatalities due to the plant accumulated over 30 years (n), the annual risk will be (assuming delayed effects, and "old" risk, and applying a factor of 2 as in the preceding example)

$$\frac{n}{30xn} < \begin{matrix} 3x10^{-6} & \text{for } n > 500 \text{ (catastrophic)} \\ 10^{-4} & \text{for } n < 500 \text{ (ordinary)} \end{matrix}.$$

This requirement is illustrated in Figure 26 which indicates the acceptable number of fatalities for various urban sites. This number is about 20 for most urban sites and may rise to about 30 for very populated areas such as New York City. Estimates are shown in the figure with their uncertainty bounds. Unless the optimistic estimates "prevail" by use of modern effluent scrubbing systems, coal power may well be up to an order of magnitude too risky according to the present model. It should be noted that the horizontal limit line drawn in Figure 28a at n = 500 may be moved upward or downward - probably by as much as a factor of 2 - depending on the definition we choose for a delayed catastrophe. Figure 28b shows the acceptable individual risk corresponding to the limit line of Figure 28a. Finally, it should be noted that the use of Figure 28 is not limited only to coal power plants, but could apply to other sources of similar risks.

# Appendix

## Statistical Tables

(i) Cumulative $\chi^2$ Distribution

(ii) Cumulative Normal Distribution

(iii) Cumulative t Distribution

# TABLE I

## CUMULATIVE $\chi^2$ DISTRIBUTION
(ρ in %)

| $f$ \ $P$ | 0.5 | 1.0 | 2.5 | 5.0 | 10 | 20 | 25 | 30 | 50 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000 | 0.000 | 0.001 | 0.004 | 0.016 | 0.064 | 0.102 | 0.148 | 0.455 |
| 2 | 0.010 | 0.020 | 0.051 | 0.103 | 0.211 | 0.446 | 0.575 | 0.713 | 1.386 |
| 3 | 0.072 | 0.115 | 0.216 | 0.352 | 0.584 | 1.005 | 1.213 | 1.424 | 2.366 |
| 4 | 0.207 | 0.297 | 0.484 | 0.711 | 1.064 | 1.649 | 1.923 | 2.195 | 3.357 |
| 5 | 0.412 | 0.554 | 0.831 | 1.145 | 1.610 | 2.343 | 2.675 | 3.000 | 4.351 |
| 6 | 0.676 | 0.872 | 1.237 | 1.635 | 2.204 | 3.070 | 3.455 | 3.828 | 5.348 |
| 7 | 0.989 | 1.239 | 1.690 | 2.167 | 2.833 | 3.822 | 4.255 | 4.671 | 6.346 |
| 8 | 1.344 | 1.646 | 2.180 | 2.733 | 3.490 | 4.594 | 5.071 | 5.527 | 7.344 |
| 9 | 1.735 | 2.088 | 2.700 | 3.325 | 4.168 | 5.380 | 5.899 | 6.393 | 8.343 |
| 10 | 2.156 | 2.558 | 3.247 | 3.940 | 4.865 | 6.179 | 6.737 | 7.267 | 9.342 |
| 11 | 2.603 | 3.053 | 3.816 | 4.575 | 5.578 | 6.989 | 7.584 | 8.148 | 10.341 |
| 12 | 3.074 | 3.571 | 4.404 | 5.226 | 6.304 | 7.807 | 8.438 | 9.034 | 11.340 |
| 13 | 3.565 | 4.107 | 5.009 | 5.892 | 7.042 | 8.634 | 9.299 | 9.926 | 12.340 |
| 14 | 4.075 | 4.660 | 5.629 | 6.571 | 7.790 | 9.467 | 10.165 | 10.821 | 13.339 |
| 15 | 4.601 | 5.229 | 6.262 | 7.261 | 8.547 | 10.307 | 11.036 | 11.721 | 14.339 |
| 16 | 5.142 | 5.812 | 6.908 | 7.962 | 9.312 | 11.152 | 11.912 | 12.624 | 15.338 |
| 17 | 5.697 | 6.408 | 7.564 | 8.672 | 10.085 | 12.002 | 12.792 | 13.531 | 16.338 |
| 18 | 6.265 | 7.015 | 8.231 | 9.390 | 10.865 | 12.857 | 13.675 | 14.440 | 17.338 |
| 19 | 6.844 | 7.633 | 8.907 | 10.117 | 11.651 | 13.716 | 14.562 | 15.352 | 18.338 |
| 20 | 7.434 | 8.260 | 9.591 | 10.851 | 12.443 | 14.578 | 15.452 | 16.266 | 19.337 |
| 21 | 8.034 | 8.897 | 10.283 | 11.591 | 13.240 | 15.445 | 16.344 | 17.182 | 20.337 |
| 22 | 8.643 | 9.542 | 10.982 | 12.338 | 14.041 | 16.314 | 17.240 | 18.101 | 21.337 |
| 23 | 9.260 | 10.196 | 11.688 | 13.091 | 14.848 | 17.187 | 18.137 | 19.021 | 22.337 |
| 24 | 9.886 | 10.856 | 12.401 | 13.848 | 15.659 | 18.062 | 19.037 | 19.943 | 23.337 |
| 25 | 10.520 | 11.524 | 13.120 | 14.611 | 16.473 | 18.940 | 19.939 | 20.867 | 24.337 |
| 26 | 11.160 | 12.198 | 13.844 | 15.379 | 17.292 | 19.820 | 20.843 | 21.792 | 25.336 |
| 27 | 11.808 | 12.879 | 14.573 | 16.151 | 18.114 | 20.703 | 21.749 | 22.719 | 26.336 |
| 28 | 12.461 | 13.565 | 15.308 | 16.928 | 18.939 | 21.588 | 22.657 | 23.647 | 27.336 |
| 29 | 13.121 | 14.256 | 16.047 | 17.708 | 19.768 | 22.475 | 23.567 | 24.577 | 28.336 |
| 30 | 13.787 | 14.953 | 16.791 | 18.493 | 20.599 | 23.364 | 24.478 | 25.508 | 29.336 |

| $f$ \ $P$ | 70 | 75 | 80 | 90 | 95 | 97.5 | 99 | 99.5 | 99.9 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1.074 | 1.323 | 1.642 | 2.706 | 3.841 | 5.024 | 6.635 | 7.879 | 10.827 |
| 2 | 2.408 | 2.773 | 3.219 | 4.605 | 5.991 | 7.378 | 9.210 | 10.597 | 13.815 |
| 3 | 3.665 | 4.108 | 4.642 | 6.251 | 7.815 | 9.348 | 11.345 | 12.838 | 16.268 |
| 4 | 4.878 | 5.385 | 5.989 | 7.779 | 9.488 | 11.143 | 13.277 | 14.860 | 18.465 |
| 5 | 6.064 | 6.626 | 7.289 | 9.236 | 11.070 | 12.832 | 15.086 | 16.750 | 20.517 |
| 6 | 7.231 | 7.841 | 8.558 | 10.645 | 12.592 | 14.449 | 16.812 | 18.548 | 22.457 |
| 7 | 8.383 | 9.037 | 9.803 | 12.017 | 14.067 | 16.013 | 18.475 | 20.278 | 24.322 |
| 8 | 9.524 | 10.219 | 11.030 | 13.362 | 15.507 | 17.535 | 20.090 | 21.955 | 26.125 |
| 9 | 10.656 | 11.389 | 12.242 | 14.684 | 16.919 | 19.023 | 21.666 | 23.589 | 27.877 |
| 10 | 11.781 | 12.549 | 13.442 | 15.987 | 18.307 | 20.483 | 23.209 | 25.188 | 29.588 |
| 11 | 12.899 | 13.701 | 14.631 | 17.275 | 19.675 | 21.920 | 24.725 | 26.757 | 31.264 |
| 12 | 14.011 | 14.845 | 15.812 | 18.549 | 21.026 | 23.337 | 26.217 | 28.300 | 32.909 |
| 13 | 15.119 | 15.984 | 16.985 | 19.812 | 22.362 | 24.736 | 27.688 | 29.819 | 34.528 |
| 14 | 16.222 | 17.117 | 18.151 | 21.064 | 23.685 | 26.119 | 29.141 | 31.319 | 36.123 |
| 15 | 17.322 | 18.245 | 19.311 | 22.307 | 24.996 | 27.488 | 30.578 | 32.801 | 37.697 |
| 16 | 18.418 | 19.369 | 20.465 | 23.542 | 26.296 | 28.845 | 32.000 | 34.267 | 39.252 |
| 17 | 19.511 | 20.489 | 21.615 | 24.769 | 27.587 | 30.191 | 33.409 | 35.718 | 40.790 |
| 18 | 20.601 | 21.605 | 22.760 | 25.989 | 28.869 | 31.526 | 34.805 | 37.156 | 42.312 |
| 19 | 21.689 | 22.718 | 23.900 | 27.204 | 30.144 | 32.852 | 36.191 | 38.582 | 43.820 |
| 20 | 22.775 | 23.828 | 25.038 | 28.412 | 31.410 | 34.170 | 37.566 | 39.997 | 45.315 |
| 21 | 23.858 | 24.935 | 26.171 | 29.615 | 32.671 | 35.479 | 38.932 | 41.401 | 46.797 |
| 22 | 24.937 | 26.039 | 27.301 | 30.813 | 33.924 | 36.781 | 40.289 | 42.796 | 48.268 |
| 23 | 26.018 | 27.141 | 28.429 | 32.007 | 35.172 | 38.076 | 41.638 | 44.181 | 49.728 |
| 24 | 27.096 | 28.241 | 29.553 | 33.196 | 36.415 | 39.364 | 42.980 | 45.558 | 51.179 |
| 25 | 28.172 | 29.339 | 30.675 | 34.382 | 37.652 | 40.646 | 44.314 | 46.928 | 52.620 |
| 26 | 29.246 | 30.434 | 31.795 | 35.563 | 38.885 | 41.923 | 45.642 | 48.290 | 54.052 |
| 27 | 30.319 | 31.528 | 32.912 | 36.741 | 40.113 | 43.194 | 46.963 | 49.645 | 55.476 |
| 28 | 31.391 | 32.620 | 34.027 | 37.916 | 41.437 | 44.461 | 48.278 | 50.993 | 56.893 |
| 29 | 32.461 | 33.711 | 35.139 | 39.087 | 42.557 | 45.722 | 49.588 | 52.336 | 58.302 |
| 30 | 33.530 | 34.800 | 36.250 | 40.256 | 43.773 | 46.979 | 50.892 | 53.672 | 59.703 |

Abridged Version of Table IV from R. A. Fisher and F. Yates: *Statistical Tables for Biological, Agricultural and Medical Research* published by Oliver & Boyd Ltd., Edinburgh and by permission of the publishers and authors.

## TABLE II

## CUMULATIVE NORMAL DISTRIBUTION

$$p(t) = \frac{1}{\sqrt{(2)\pi}} \int_0^t e^{-\frac{1}{2}t^2} dt$$

| $t$ | 0.00 | 0.01 | 0.02 | 0.03 | 0.04 | 0.05 | 0.06 | 0.07 | 0.08 | 0.09 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0.0 | 0.0000 | 0.0040 | 0.0080 | 0.0120 | 0.0159 | 0.0199 | 0.0239 | 0.0279 | 0.0319 | 0.0359 |
| 0.1 | 0.0398 | 0.0438 | 0.0478 | 0.0517 | 0.0557 | 0.0596 | 0.0636 | 0.0675 | 0.0714 | 0.0753 |
| 0.2 | 0.0793 | 0.0832 | 0.0871 | 0.0909 | 0.0948 | 0.0987 | 0.1026 | 0.1064 | 0.1103 | 0.1141 |
| 0.3 | 0.1179 | 0.1217 | 0.1255 | 0.1293 | 0.1331 | 0.1368 | 0.1406 | 0.1443 | 0.1480 | 0.1517 |
| 0.4 | 0.1555 | 0.1591 | 0.1628 | 0.1664 | 0.1700 | 0.1736 | 0.1772 | 0.1808 | 0.1844 | 0.1879 |
| 0.5 | 0.1915 | 0.1950 | 0.1985 | 0.2019 | 0.2054 | 0.2088 | 0.2123 | 0.2157 | 0.2190 | 0.2224 |
| 0.6 | 0.2257 | 0.2291 | 0.2324 | 0.2356 | 0.2389 | 0.2421 | 0.2454 | 0.2486 | 0.2517 | 0.2549 |
| 0.7 | 0.2580 | 0.2611 | 0.2642 | 0.2673 | 0.2703 | 0.2734 | 0.2764 | 0.2793 | 0.2823 | 0.2852 |
| 0.8 | 0.2881 | 0.2910 | 0.2939 | 0.2967 | 0.2995 | 0.3023 | 0.3051 | 0.3078 | 0.3108 | 0.3133 |
| 0.9 | 0.3159 | 0.3186 | 0.3212 | 0.3238 | 0.3264 | 0.3289 | 0.3315 | 0.3340 | 0.3365 | 0.3389 |
| 1.0 | 0.3413 | 0.3437 | 0.3461 | 0.3485 | 0.3508 | 0.3531 | 0.3554 | 0.3577 | 0.3599 | 0.3621 |
| 1.1 | 0.3643 | 0.3665 | 0.3686 | 0.3708 | 0.3729 | 0.3749 | 0.3770 | 0.3790 | 0.3810 | 0.3830 |
| 1.2 | 0.3849 | 0.3869 | 0.3888 | 0.3906 | 0.3925 | 0.3943 | 0.3962 | 0.3980 | 0.3997 | 0.4015 |
| 1.3 | 0.4032 | 0.4049 | 0.4066 | 0.4082 | 0.4099 | 0.4115 | 0.4131 | 0.4147 | 0.4162 | 0.4177 |
| 1.4 | 0.4192 | 0.4207 | 0.4222 | 0.4236 | 0.4251 | 0.4265 | 0.4279 | 0.4292 | 0.4306 | 0.4319 |
| 1.5 | 0.4332 | 0.4345 | 0.4357 | 0.4370 | 0.4382 | 0.4394 | 0.4406 | 0.4418 | 0.4429 | 0.4441 |
| 1.6 | 0.4452 | 0.4463 | 0.4474 | 0.4484 | 0.4495 | 0.4505 | 0.4515 | 0.4525 | 0.4535 | 0.4545 |
| 1.7 | 0.4554 | 0.4564 | 0.4573 | 0.4582 | 0.4591 | 0.4599 | 0.4608 | 0.4616 | 0.4625 | 0.4633 |
| 1.8 | 0.4641 | 0.4648 | 0.4656 | 0.4664 | 0.4671 | 0.4678 | 0.4686 | 0.4693 | 0.4699 | 0.4706 |
| 1.9 | 0.4713 | 0.4719 | 0.4726 | 0.4732 | 0.4738 | 0.4744 | 0.4750 | 0.4756 | 0.4761 | 0.4767 |
| 2.0 | 0.4772 | 0.4778 | 0.4783 | 0.4788 | 0.4793 | 0.4798 | 0.4803 | 0.4808 | 0.4812 | 0.4817 |
| 2.1 | 0.4821 | 0.4826 | 0.4830 | 0.4834 | 0.4838 | 0.4842 | 0.4846 | 0.4850 | 0.4854 | 0.4857 |
| 2.2 | 0.4861 | 0.4864 | 0.4868 | 0.4871 | 0.4874 | 0.4878 | 0.4881 | 0.4884 | 0.4887 | 0.4890 |
| 2.3 | 0.4893 | 0.4896 | 0.4898 | 0.4901 | 0.4904 | 0.4906 | 0.4909 | 0.4911 | 0.4913 | 0.4916 |
| 2.4 | 0.4918 | 0.4920 | 0.4922 | 0.4924 | 0.4927 | 0.4929 | 0.4930 | 0.4932 | 0.4934 | 0.4936 |
| 2.5 | 0.4938 | 0.4940 | 0.4941 | 0.4943 | 0.4945 | 0.4946 | 0.4948 | 0.4949 | 0.4951 | 0.4952 |
| 2.6 | 0.4953 | 0.4955 | 0.4956 | 0.4957 | 0.4958 | 0.4960 | 0.4961 | 0.4962 | 0.4963 | 0.4964 |
| 2.7 | 0.4965 | 0.4966 | 0.4967 | 0.4968 | 0.4969 | 0.4970 | 0.4971 | 0.4972 | 0.4973 | 0.4974 |
| 2.8 | 0.4974 | 0.4975 | 0.4976 | 0.4977 | 0.4977 | 0.4978 | 0.4979 | 0.4979 | 0.4980 | 0.4981 |
| 2.9 | 0.4981 | 0.4982 | 0.4982 | 0.4983 | 0.4984 | 0.4984 | 0.4985 | 0.4985 | 0.4986 | 0.4986 |
| 3.0 | 0.4986 | 0.4987 | 0.4987 | 0.4988 | 0.4988 | 0.4989 | 0.4989 | 0.4989 | 0.4990 | 0.4990 |
| 3.1 | 0.4990 | 0.4991 | 0.4991 | 0.4991 | 0.4991 | 0.4992 | 0.4992 | 0.4992 | 0.4993 | 0.4993 |
| 3.2 | 0.4993 | 0.4993 | 0.4994 | 0.4994 | 0.4994 | 0.4994 | 0.4994 | 0.4995 | 0.4995 | 0.4995 |
| 3.3 | 0.4995 | 0.4995 | 0.4995 | 0.4996 | 0.4996 | 0.4996 | 0.4996 | 0.4996 | 0.4996 | 0.4996 |
| 3.4 | 0.4997 | 0.4997 | 0.4997 | 0.4997 | 0.4997 | 0.4997 | 0.4997 | 0.4997 | 0.4997 | 0.4998 |

# TABLE III

## CUMULATIVE t DISTRIBUTION

| f \ P | 55 | 60 | 70 | 80 | 90 | 95 | 97.5 | 99 | 99.5 | 99.9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.158 | 0.325 | 0.727 | 1.376 | 3.078 | 6.314 | 12.71 | 31.82 | 63.66 | 318.0 |
| 2 | 0.142 | 0.289 | 0.617 | 1.061 | 1.886 | 2.920 | 4.303 | 6.965 | 9.925 | 22.30 |
| 3 | 0.137 | 0.277 | 0.584 | 0.978 | 1.638 | 2.353 | 3.182 | 4.541 | 5.841 | 10.20 |
| 4 | 0.134 | 0.271 | 0.569 | 0.941 | 1.533 | 2.132 | 2.776 | 3.747 | 4.604 | 7.173 |
| 5 | 0.132 | 0.267 | 0.559 | 0.920 | 1.476 | 2.015 | 2.571 | 3.365 | 4.032 | 5.893 |
| 6 | 0.131 | 0.265 | 0.553 | 0.906 | 1.440 | 1.943 | 2.447 | 3.143 | 3.707 | 5.208 |
| 7 | 0.130 | 0.263 | 0.549 | 0.896 | 1.415 | 1.895 | 2.365 | 2.998 | 3.499 | 4.785 |
| 8 | 0.130 | 0.262 | 0.546 | 0.889 | 1.397 | 1.860 | 2.306 | 2.896 | 3.355 | 4.501 |
| 9 | 0.129 | 0.261 | 0.543 | 0.883 | 1.383 | 1.833 | 2.262 | 2.821 | 3.250 | 4.297 |
| 10 | 0.129 | 0.260 | 0.542 | 0.879 | 1.372 | 1.812 | 2.228 | 2.764 | 3.169 | 4.144 |
| 11 | 0.129 | 0.260 | 0.540 | 0.876 | 1.363 | 1.796 | 2.201 | 2.718 | 3.106 | 4.025 |
| 12 | 0.128 | 0.259 | 0.539 | 0.873 | 1.356 | 1.782 | 2.179 | 2.681 | 3.055 | 3.930 |
| 13 | 0.128 | 0.259 | 0.538 | 0.870 | 1.350 | 1.771 | 2.160 | 2.650 | 3.012 | 3.852 |
| 14 | 0.128 | 0.258 | 0.537 | 0.868 | 1.345 | 1.761 | 2.145 | 2.624 | 2.977 | 3.787 |
| 15 | 0.128 | 0.258 | 0.536 | 0.866 | 1.341 | 1.753 | 2.131 | 2.602 | 2.947 | 3.733 |
| 16 | 0.128 | 0.258 | 0.535 | 0.865 | 1.337 | 1.746 | 2.120 | 2.583 | 2.921 | 3.686 |
| 17 | 0.128 | 0.257 | 0.534 | 0.863 | 1.333 | 1.740 | 2.110 | 2.567 | 2.898 | 3.646 |
| 18 | 0.127 | 0.257 | 0.534 | 0.862 | 1.330 | 1.734 | 2.101 | 2.552 | 2.878 | 3.610 |
| 19 | 0.127 | 0.257 | 0.533 | 0.861 | 1.328 | 1.729 | 2.093 | 2.539 | 2.861 | 3.579 |
| 20 | 0.127 | 0.257 | 0.533 | 0.860 | 1.325 | 1.725 | 2.086 | 2.528 | 2.845 | 3.552 |
| 21 | 0.127 | 0.257 | 0.532 | 0.859 | 1.323 | 1.721 | 2.080 | 2.518 | 2.831 | 3.527 |
| 22 | 0.127 | 0.256 | 0.532 | 0.858 | 1.321 | 1.717 | 2.074 | 2.508 | 2.819 | 3.505 |
| 23 | 0.127 | 0.256 | 0.532 | 0.858 | 1.319 | 1.714 | 2.069 | 2.500 | 2.807 | 3.485 |
| 24 | 0.127 | 0.256 | 0.531 | 0.857 | 1.318 | 1.711 | 2.064 | 2.492 | 2.797 | 3.467 |
| 25 | 0.127 | 0.256 | 0.531 | 0.856 | 1.316 | 1.708 | 2.060 | 2.485 | 2.787 | 3.450 |
| 26 | 0.127 | 0.256 | 0.531 | 0.856 | 1.315 | 1.706 | 2.056 | 2.479 | 2.779 | 3.435 |
| 27 | 0.127 | 0.256 | 0.531 | 0.855 | 1.314 | 1.703 | 2.052 | 2.473 | 2.771 | 3.421 |
| 28 | 0.127 | 0.256 | 0.530 | 0.855 | 1.313 | 1.701 | 2.048 | 2.467 | 2.763 | 3.408 |
| 29 | 0.127 | 0.256 | 0.530 | 0.854 | 1.311 | 1.699 | 2.045 | 2.462 | 2.756 | 3.396 |
| 30 | 0.127 | 0.256 | 0.530 | 0.854 | 1.310 | 1.697 | 2.042 | 2.457 | 2.750 | 3.885 |
| 40 | 0.126 | 0.255 | 0.529 | 0.851 | 1.303 | 1.684 | 2.021 | 2.423 | 2.704 | 3.307 |
| 60 | 0.126 | 0.254 | 0.527 | 0.848 | 1.296 | 1.671 | 2.000 | 2.390 | 2.660 | 3.232 |
| 120 | 0.126 | 0.254 | 0.526 | 0.845 | 1.289 | 1.658 | 1.980 | 2.358 | 2.617 | 3.160 |
| ∞ | 0.126 | 0.253 | 0.524 | 0.842 | 1.282 | 1.645 | 1.960 | 2.326 | 2.576 | 3.090 |

This table is reproduced from Table III of R. A. Fisher and F. Yates: *Statistical Tables for Biological, Agricultural and Medical Research* published by Oliver & Boyd Ltd., Edinburgh and by permission of the publishers and authors.

## III. APPLICATION TO UNRESOLVED GENERIC NUCLEAR SAFETY ISSUES

A generic nuclear safety issue refers to an issue that applies to a reactor system in general and is not specific to a particular utility plant design. Thus, generic nuclear safety issues are some of the most important and most difficult issues to resolve. In some of these issues, probabilistic means of resolution have been discarded (as for the ATWS issue by the NRC staff); in others, such analysis seems to be the only way to resolve the issue since a choice between mitigation systems must be made. The issue of ATWS is one of the more famous of the unresolved nuclear safety issues confronting both regulators and the industry. Other issues include decisions on appropriate control systems for hydrogen generated in accident scenarios by metal-water reactions and deciding between various suggested new containment designs to reduce the likelihood of containment breaks during accidents. After Three-Mile Island, attention has also been placed on human factors engineering and the necessary modifications required for improved control room design.[1] TMI has forced the NRC and the industry to take a hard look at many of these unresolved safety problems; the next several months will be some of the most active in the licensing-safety area.

This section summarizes the work done at MIT and elsewhere in applying reliability and probabilistic risk assessment methods to four unresolved generic nuclear safety issues:

(i) the anticipated transient without scram (ATWS) issue;

(ii) the containment inerting issue;

(iii) the issue of hydrogen control in PWRs; and

(iv) the issue of the reactor core melt frequency after TMI.

Summarized here is work done on each of these subject categories indicating what probabilistic studies have concluded with respect to each area and the additional data and analysis required to reach resolution. The examples make use of the most recent studies available on each issue and present original results forthcoming from the analyses performed at MIT. Use of WASH-1400 and recent EPRI-NSAC studies are included.

In part A, the ATWS issue is reviewed including the work done at EPRI by Lellouche et al. and by Garrick and Lowe - UCLA for the Oyster Creek probabilistic risk study. Data and information on the recent incident at Brown's Ferry is also summarized and reviewed with respect to its impact on the ATWS assessment. In part B, the containment inerting issue is analyzed making use of data and specific systems design from the Vermont Yankee nuclear power stations and from the General Electric Co. licensing staff. Part C summarizes the work done at MIT on the hydrogen deflagration and detonation problem, particularly for PWRs. Models developed to calculate the expected pressure rise due to a hydrogen burn or explosion are described and results shown. A comparison of recombiners with other methods for in-containment hydrogen control in PWRs is also shown. Finally, in part D, a method for updating estimates of the core melt accident frequency is described based on Bayesian updating techniques. A sample calculation of such an updated estimate is performed inclusive of the experience at Three Mile Island. Reference to these examples of nuclear safety analyses should provide nuclear safety and licensing engineers with detailed examples to guide similar such endeavors.

## A. The Issue of Anticipated Transients Without Scram (ATWS)

The issue of anticipated transients without scram, or the ATWS issue, has been raging in the nuclear industry for over ten years. In 1968, a consultant to the Advisory Committee on Reactor Safeguards (ACRS), which advises the NRC on licensing matters, brought forth a concern about a potential failure phenomena threatening nuclear power safety. This concern was over the potential for a simultaneous failure of the multiple defense system of the reactor scram system while the reactor was experiencing a normal or abnormal transient event. This "common mode" failure possibility resulted in the creation of the acronym ATWS.

Conceptually, an ATWS event might occur whenever the reactor was scrammed during a transient. The Oyster Creek study[2] identifies over 40 possible scram initiating events. Ten of the most important in the case of a BWR are: (1) high reactor pressure, (2) low reactor water level, (3) high drywell pressure, (4) high main steam line radiation, (5) main steam line isolation valve closure, (6) low condenser vacuum, (7) high-high water level in the scram discharge volume, (8) high-high neutron flux, (9) turbine acceleration (turbine trip), and (10) stop valve closure. For PWRs, similar events also cause scrams.

The consequences of an ATWS event could be major. Although the precise definition of a specific ATWS event has been debated, failure to scram a reactor during a transient event could lead to a major accident with a subsequent release of large amounts of radiation. The usual definition employed to define a failure of the scram system in various safety studies is that between 3 to 5 adjacent control rods fail to fully insert to their full position when placed on demand. The effects on reactivity as a result of such a failure are conservatively estimated to appreciably increase the overall risk of a core melt scenario. Also, WASH-1400 has pointed out the increased significance of an ATWS event for a BWR as compared to a PWR; WASH-1400 identifies an ATWS event as contributing approximately 30 to 40 percent of the total accident risk in a BWR.[3]

The debate over the significance and probability of an ATWS event has resulted from the inconclusive nature of operating history to render an estimate of scram failure frequency that is acceptably low to the NRC. The NRC perspective on ATWS is found in NUREG-0460,[4] prepared by the NRC staff in 1978. In that document, a summary of the NRC position is presented. Briefly, the NRC position is given in the following excerpt from that report:

> "The significance of ATWS...is that some ATWS events could result in melting of the reactor fuel and the release of a large amount of radioactive fission products. The questions in contention concern whether the probability of such events is great enough to justify their consideration and if so, what degree of protection is required."
>
> "We estimate that the probability of scram failure, based on nearly 700 reactor years of operating experience in foreign and domestic commercial reactors is in the range of $10^{-4}$ to $10^{-5}$ per demand. Thus the expected frequency of ATWS events that could result in serious consequences is $\sim 2 \times 10^{-4}$ per reactor-year. We recommend that a safety objective of $10^{-6}$ unacceptable ATWS events per reactor-year is more appropriate and therefore, that some corrective measures to reduce the probability or consequences of ATWS are required."

A utility perspective on ATWS is provided by A. Kimmins of Washington Public Power Supply Systems:[5]

> "...ATWS has not been shown to be a significant problem and the high estimated costs for mitigation cannot be justified...the original issue has escalated from the need to address a hypothetical concern to a full scale scenario of abnormal events...today, we still don't know definitely what an ATWS is so how can the design of nuclear power plants be adjusted to prevent such an event? The addition of more systems and equipment has been suggested by the NRC but such "fixes" have the potential to worsen the net safety and operability of plants."

## A.1 Analyzing the Occurence of an ATWS Event: Probability Statement in Inferential and Classical Notation

A.1.1 Definition of ATWS: An ATWS event may occur when the reactor protection system (i.e., the control rod assemblies) fails to operate or "scram" completely at the time an anticipated transient is simultaneously taking place in the reactor. The consequence of such an event could include core meltdown with subsequent release of radioactive fission products to the environment in large, significant amounts. Anticipated transients refer to those conditions of normal operation which are expected to occur one or more times during the service life of a plant including such events as loss of all offsite power and tripping of the turbine generator set.

A.1.2 Occurrence of ATWS Events: The frequency of ATWS events is the product of the frequency of anticipated transients in the reactor and the conditional probability of scram failure given the occurrence of a transient, or:

$$P(ATWS) = P(AT) \cdot P(WS|AT)$$

where $P(ATWS)$ = probability of an ATWS event

$P(AT)$ = probability of an anticipated transient (frequency per year)

$P(WS|AT)$ = probability of a scram failure (without scram event) given an anticipated transient event

= unavailability on demand

These estimates are placed on a yearly basis. The probability of failure of the reactor protection system given a transient event $P(WS|AT)$ is the sum of two components: (i) the probability that the event occurs and then remains undetected and therefore uncorrected until tested or challenged, and (ii) the probability that the scram system fails as a result of the transient. This can be expressed mathematically as:

$$P(WS|AT) = P(WS|ATB) + P(WS|ATR)$$

where $P(WS|ATB)$ = probability that the scram system fails before the anticipated transient event occurs

$P(WS|ATR)$ = probability that the scram system fails as a result of the anticipated transient event

Experience has shown that $P(WS|ATB) >> P(WS|ATR)$ so that most analyses have neglected $P(WS|ATR)$ while concentrating attention on the more significant component.

## A.2 Estimation of Probabilities for Scram System Reliability and Anticipated Transients

### A.2.1 Scram System Reliability Estimates

The estimation of failure rates for the reactor protection system from experience data is made difficult because the systems have been very reliable;[4] only one event that can be construed to relate to scram failure has ever taken place.* Although many components and

*This was the KAHL event which took place at the 15 MWt BWR KAHL reactor in Germany in 1963. After the situation was discovered, modifications in quality assurance procedures were instituted by the NRC and were applied to all plants.[6] It should also be noted that an anticipated transient did not occur at the time of the "without scram" event at KAHL. There has yet to have been an ATWS event.

subsystems have failed these systems are designed to be redundant and capable of performing their safety function even with the occurrence of single failures.[4] Failure of the common mode type that could cause all or a significant number of the control rods to fail to insert have been very rare events indeed.

Two methods have been used to estimate scram system reliability:[4] (i) the "system experience method", which evaluates reliability based on actual experience of the system without identifying specifically the modes of failure, and (ii) the "synthesis method", which uses fault and event trees to identify failure paths and individual component failure rates to quantify the estimate of reliability.

### A.2.2 The System Experience Approach

On the basis of existing reactor operating data from the U.S. and similar foreign experience, the system experience approach can give an estimate of scram system reliability as follows:

$$\{AT,WS|\varepsilon\} = \{AT|\varepsilon\} \cdot \{WS|AT,\varepsilon\}^{*}$$

where $\{AT,WS|\varepsilon\}$ = probability of both an anticipated transient (AT) and a failure of the reactor protection system (WS) occurring simultaneously

$\{AT|\varepsilon\}$ = frequency of an anticipated transient per year

$\{WS|AT,\varepsilon\}$ = probability of having a failure of the reactor protection system <u>given a demand is placed on that system by an anticipated transient event</u>

Historical data for the above probabilities is given in the following table (Table I).

[*] From definition of conditional probability (see II.A).

## Table I

CALCULATION OF ATWS PROBABILITY BASED ON EXPERIENCE DATA ($\varepsilon$)

$$\{AT,WS|\varepsilon\} = \{AT|\varepsilon\}\ \{WS|AT,\varepsilon\}$$

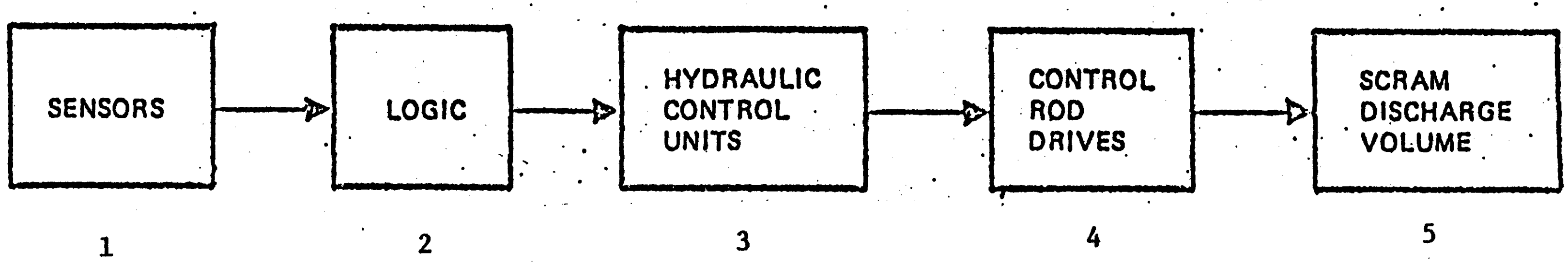
| Category of Event | Estimated Range | Suggested Value[6] |
|---|---|---|
| No. AT (demands) per reactor year $\{AT\|\varepsilon\}$ | .01-10 | 1.68 |
| No. tests performed per reactor year | 20-200 | 92 |
| Probability of WS per demand $\{WS\|AT,\varepsilon\}$*<br>$= \dfrac{\text{No. failures to scram completely}}{\text{total no. demands}}$<br>$= \dfrac{\text{1 (KAHL Event)}}{\text{[(659 reactor-yrs)(tests per reactor-yr)} + \text{(659 reactor-yrs)(other scrams per reactor-yr)]}}$<br>$\cong \dfrac{\text{1 (KAHL Event)}}{\text{(2)(659)(no. tests)}}$ | $.38\text{-}3.79\text{x}10^{-5}$ | mean $8.25\text{x}10^{-6}$<br>median $5\text{x}10^{-6}$ |
| $\{AT,WS\|\varepsilon\}$<br>(per reactor-year) | mean $.64\text{-}6.4\text{x}10^{-5}$<br>median $.39\text{-}3.9\text{x}10^{-5}$ | mean $1.39\text{x}10^{-5}$<br>median $8.4\text{x}10^{-6}$ |

*According to EPRI analysis $\{WS|AT,\varepsilon\}$ can be estimated by dividing the historical number of WS events by twice the number of tests (demands) multiplied by the amount of experience in reactor-years. There have been 659 reactor years of experience as of 1978; currently, the total has risen to 850 excluding naval experience . The use of naval reactor operating data has been debated and presently the NRC rejects the notion of using such data for its reliability estimates.[4] Inclusion of such data adds another 1500-1600 years of reactor operating experience to the data base.[6]

## A.3 Using the Bayesian Approach to Analyze the System Unavailability per Demand

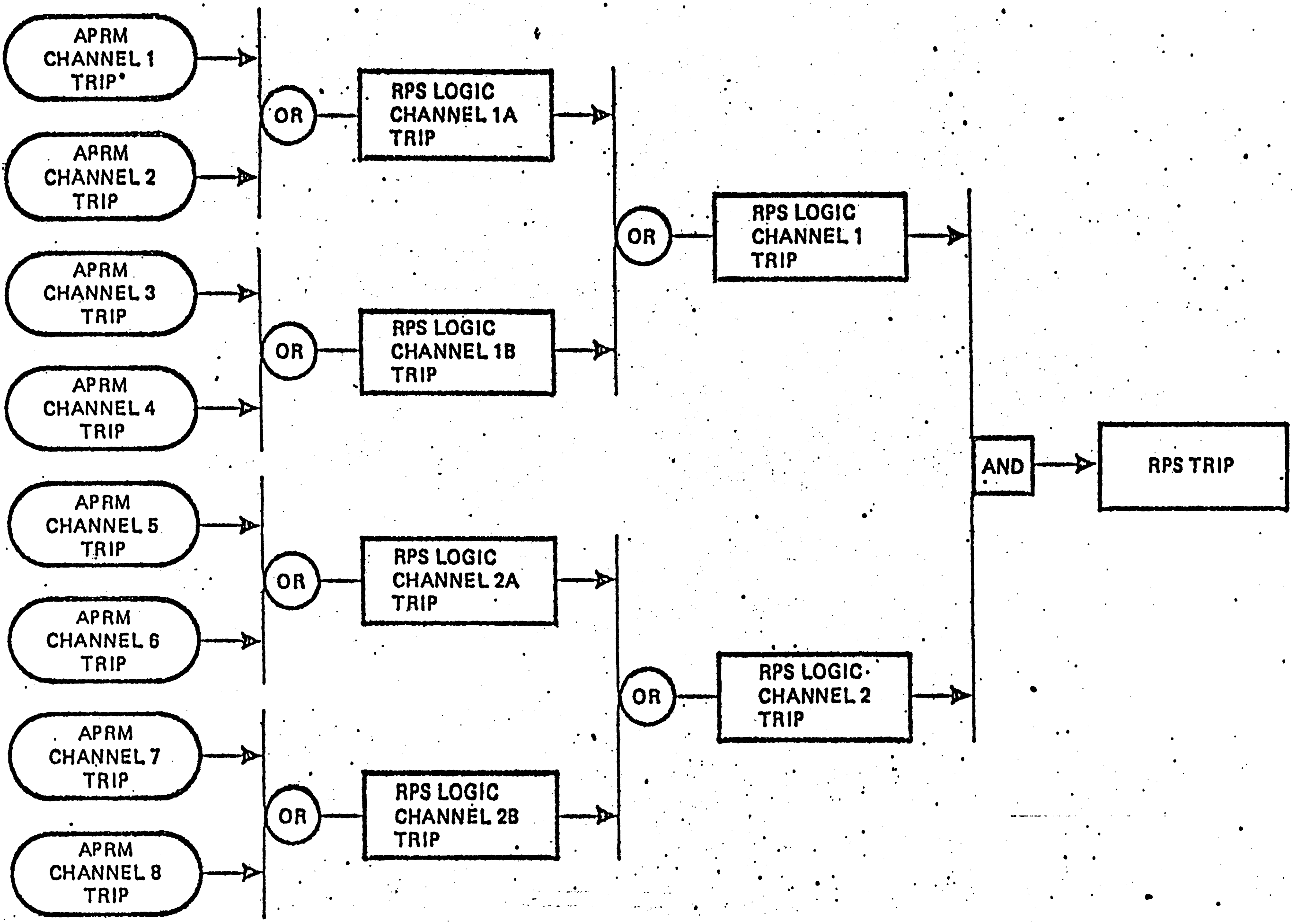
A more detailed analysis of the scram system (reactor protection system (RPS)) was carried out for the Oyster Creek BWR plant.[2] Basically the RPS is made up of five subsystems shown in Figure 1: (1) sensors, (2) logic, (3) hydraulic control units, (4) control rod devices, and (5) scram discharge volume. Each of these systems perform a different function in protecting the reactor from undesirable transients. The sensors first detect the undesirable circumstances (e.g., high-high reactor pressure or neutron flux) sending electrical signals to the logic circuitry, which determine whether the signals are spurious or real. An example of the RPS trip logic is shown in Figure 2 for the Average Power Range Monitoring (ARPM) sensors. At Oyster Creek, the logic used in the APRM input circuit is called a "one-out-of-two-twice" system since the signal must come from either of two sets of dual detectors twice and then be matched against the existence of a signal on the opposite channel.

In a BWR, the signals from the sensors cause the logic circuit to de-energize as each logic channel is basically a set of relays and contacts; when a detector senses a parameter out of limit, the input to the associated logic channel results in a contact being opened. The resulting open circuit leads to de-energization of a relay which in turn leads to further de-energization of other relay sets. When both logic channels are fully de-energized, the logic system causes power to all scram pilot valves to shut off. Each of the 137 control rod drives has a hydraulic control unit (HCU) governed by the position



Five Subsystems of RPS
(BWR)

Figure 1 Reactor Protection System Model (RPS).



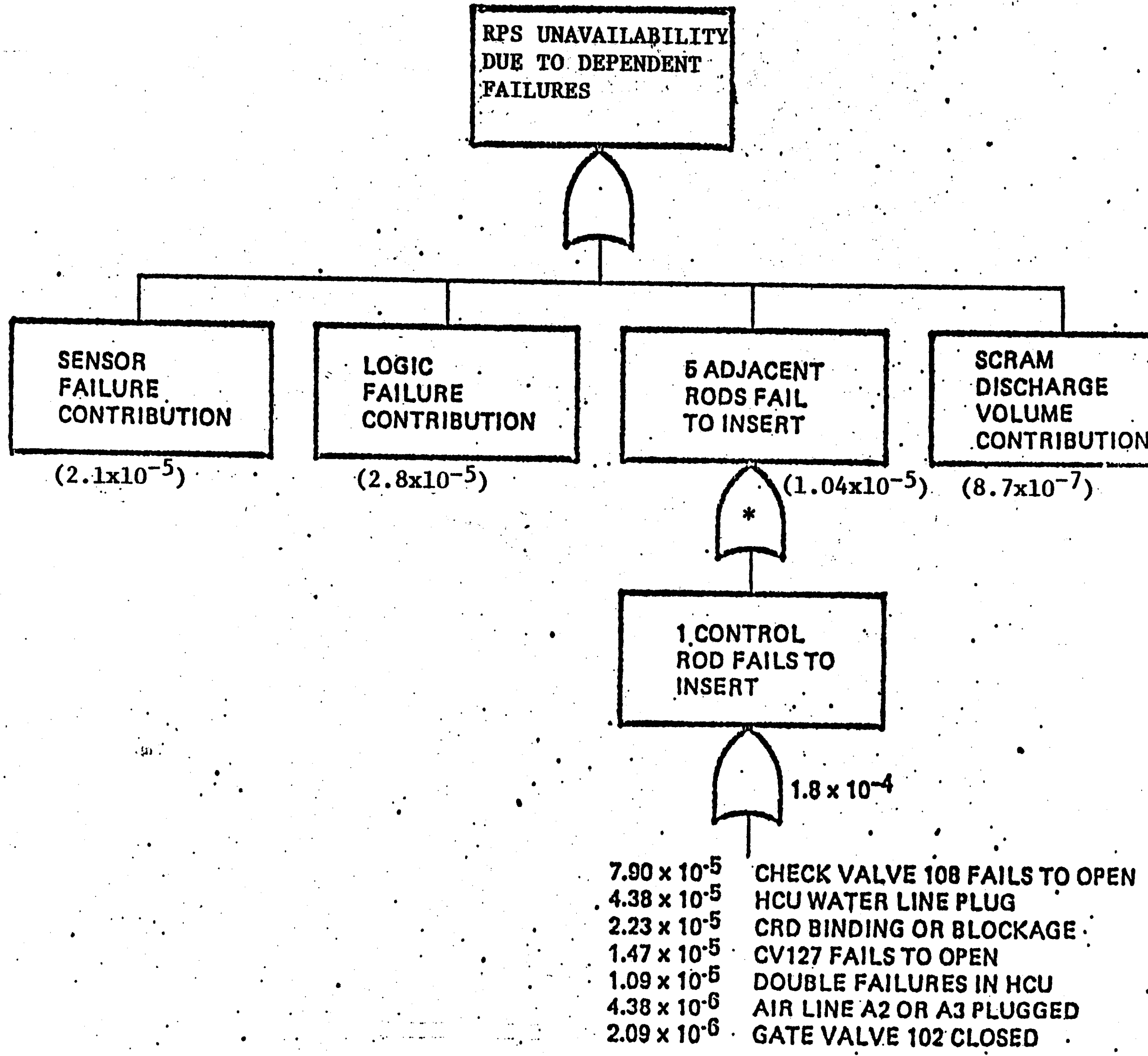
*APRM Upscale or Inoperative

Figure 2 RPS Trip Logic (Average Power Range Monitoring).

of the scram pilot valve. The two scram pilot valves transfer to an open position and bleed the instrument air that holds two scram valves in the closed position. This exerts a change in pressure ΔP that is exerted under the control rod piston. Reactor pressure and the ΔP drive the control rods the full distance into the core. When this happens, water is driven out of the control rod drives and is exhausted through the discharge side of the hydraulic control units. The scram discharge volume, which is the fifth sub-system, collects the water from all 137 control rod drives.

Both dependent and independent failure modes of the five sub-systems were analyzed with fault trees to arrive at histograms on the failure frequency per demand. The RPS summary fault tree for Oyster Creek is shown in Figure 3. Results are shown in the figure and indicate that dependent failures outweigh the independent modes of failure. The largest single contributor to the overall failure frequency is the logic sub-system followed by sensor failure, and then by the failure of 5 out of the 137 control rods to insert fully upon demand. The scram discharge volume contributes only in a minor way to the total failure frequency, but note that the dependent and independent failures are roughly equivalent. The final histograms of the failure frequency is shown in Figure 4 and combines the histograms of the five sub-systems.

The Bayesian approach was used in the Oyster Creek study to incorporate the existing experiencial data into the calculations of scram failure per demand. Because of the uncertainty and debate surrounding the number of scram failure occurrences and the uncertainty on the number of total tests of the scram system in the world, the Oyster Creek study points out (p. A-201):


RPS UNAVAILABILITY DUE TO DEPENDENT FAILURES
SENSOR FAILURE CONTRIBUTION
(2.1x10^-5)
LOGIC FAILURE CONTRIBUTION
(2.8x10^-5)
5 ADJACENT RODS FAIL TO INSERT
(1.04x10^-5)
*
SCRAM DISCHARGE VOLUME CONTRIBUTION
(8.7x10^-7)
1 CONTROL ROD FAILS TO INSERT
1.8 x 10^-4
7.90 x 10^-5 CHECK VALVE 108 FAILS TO OPEN
4.38 x 10^-5 HCU WATER LINE PLUG
2.23 x 10^-5 CRD BINDING OR BLOCKAGE
1.47 x 10^-5 CV127 FAILS TO OPEN
1.09 x 10^-5 DOUBLE FAILURES IN HCU
4.38 x 10^-6 AIR LINE A2 OR A3 PLUGGED
2.09 x 10^-6 GATE VALVE 102 CLOSED

PROBABILITY OF 5 ADJACENT ROD FAILURES CALCULATED ACCORDING TO SECTION A.2.3.3.5

Figure 3 Reactor Protection System Summary Fault Tree

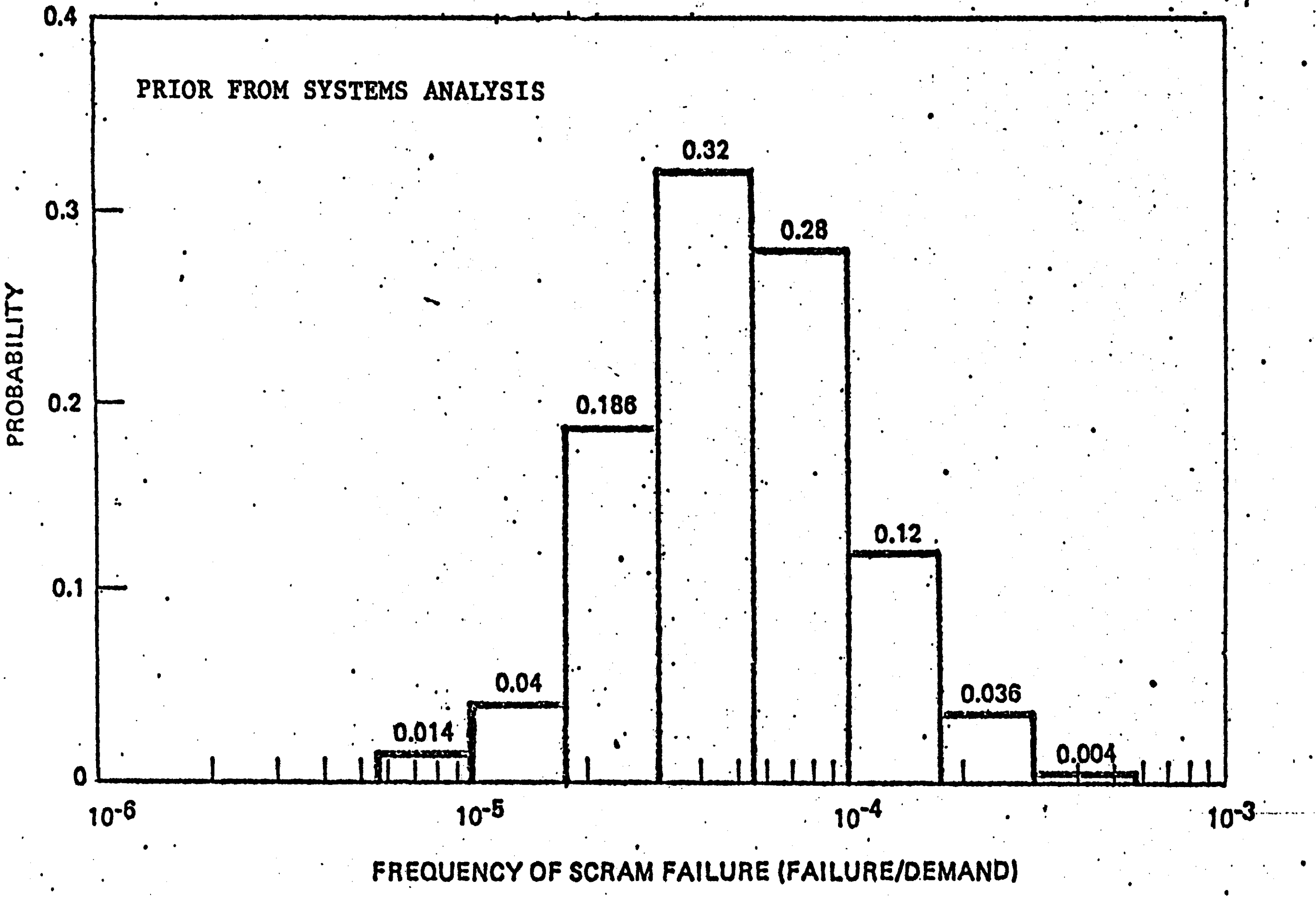


Figure 4 Prior Probability Distribution for Scram System Failure.

> "Subjective judgment is inevitable when dealing with uncertainty. Subjective judgment is essential. All that the Bayesian approach does is to formalize the use of judgment and make it visible and explicit so that inconsistencies will be prevented."

To use the Bayesian approach a prior distribution must be constructed. This was done for Oyster Creek by combining the failure frequency histograms for the five sub-systems (Figure 4).

Next, posterior distributions were calculated from Bayes theorem (Figure 5) incorporating both the prior distribution derived from the systems analysis and the available experience data. The experience data consists of estimates made by EPRI and NRC on the number of scram failures r experienced out of n test trials in the world to date. The process of incorporating this data with the prior estimate is analogous to the I.Q. problem described in an earlier section (see II.A.4). The "r-out-of-n trials" is also analogous to the coin-tossing experiments discussed in earlier sections where r = number of heads and n = number of scrams (tests) which have occurred over the lifetime of the world's nuclear power industry. Results of the analysis for Oyster Creek are shown in Figure 6. Note the prior distribution derived from the system fault tree analysis and the observed data points $\bar{x}_i$. The characteristic mean of the prior and posterior distributions are also shown.

The final result is that the best estimate of the scram failure frequency per demand is $\{WS|AT,\bar{x}\}$; i.e., the probability distribution function of having a without scram event (WS) given an anticipated transient (demand) is conditioned on the observed data $\bar{x}$ expressed in composite form. (Note that the inferential notation allows the analyst

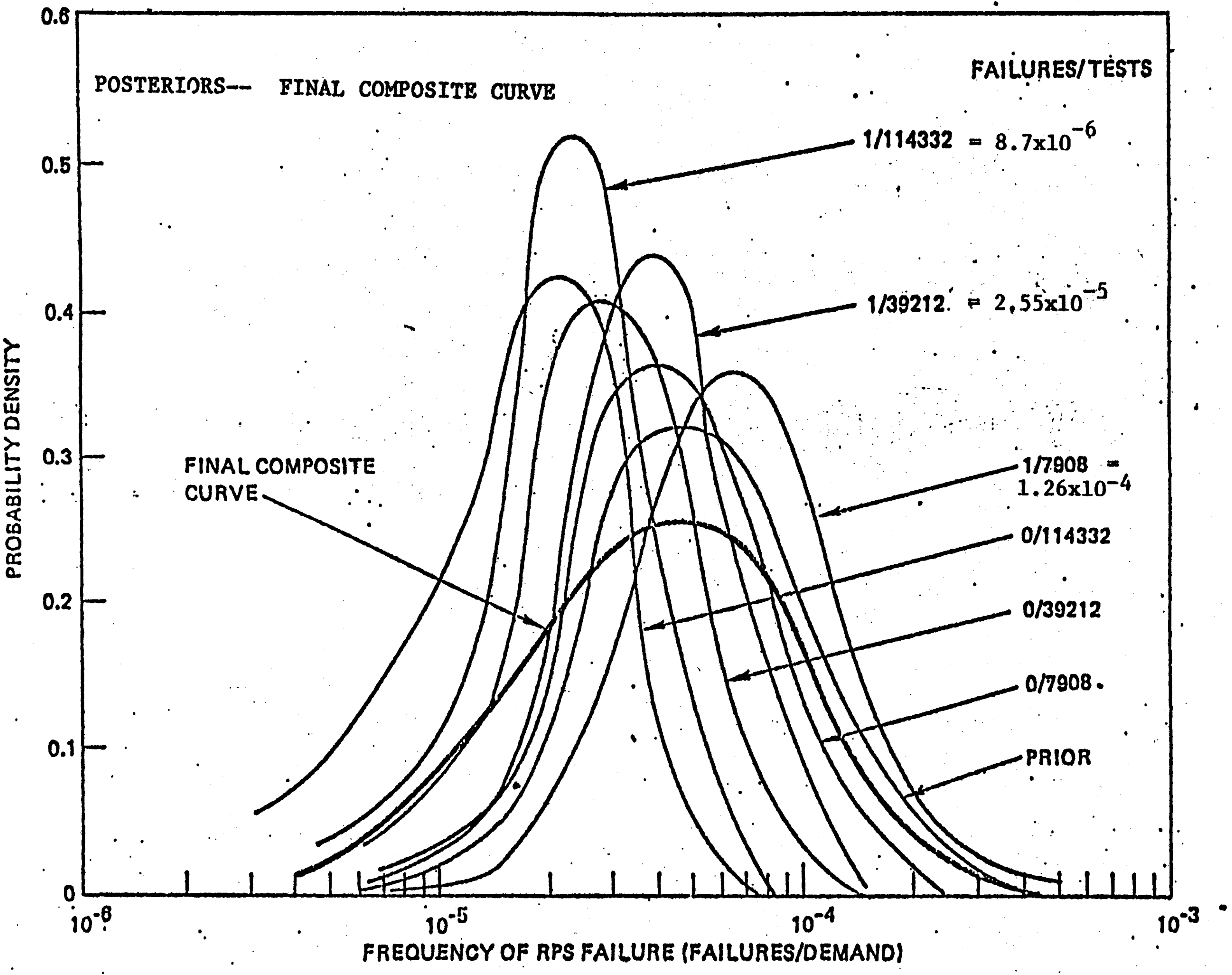
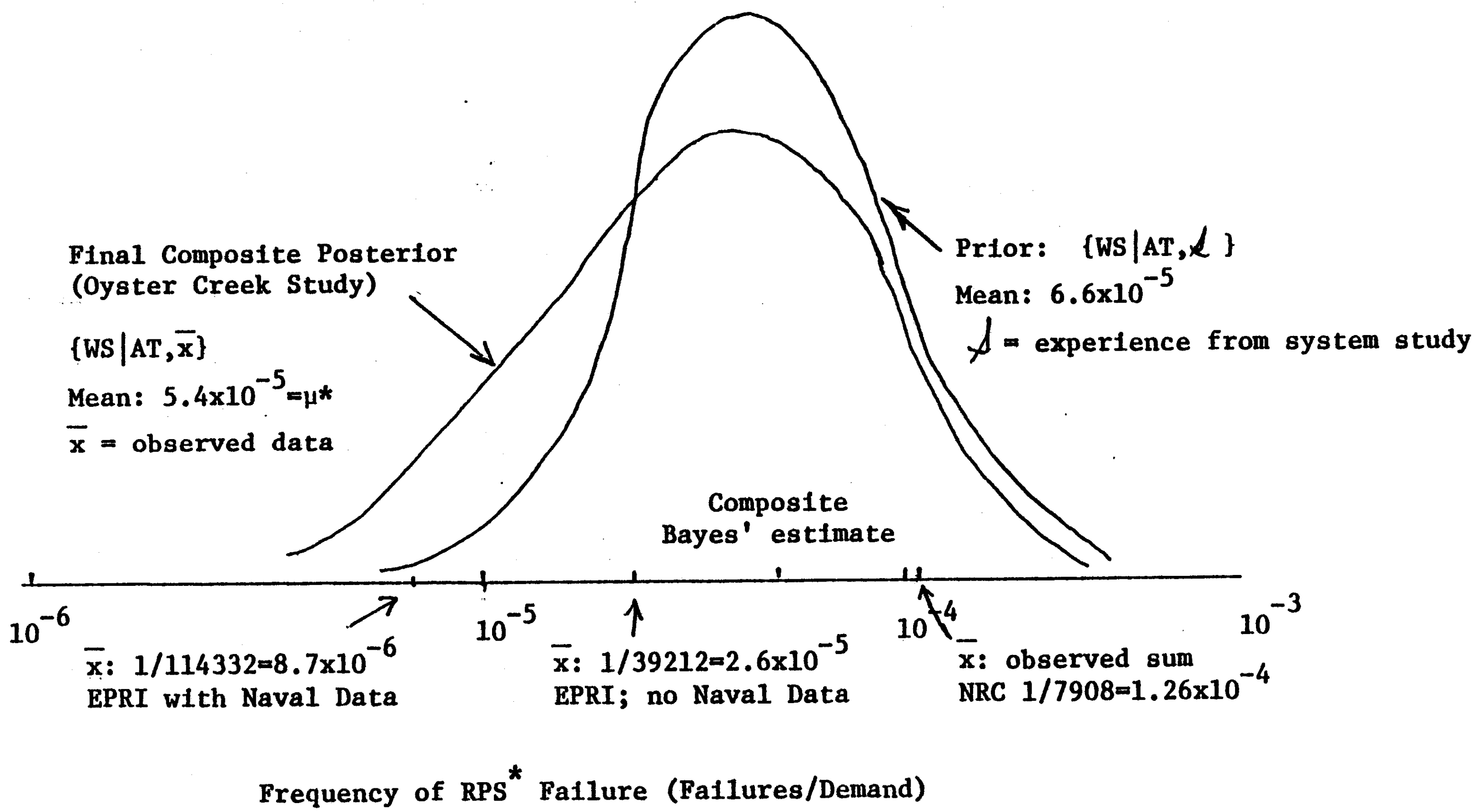


Figure 5 Final Composite Probability Curve for Scram Failure Rate.

Figure 6 Final Results: Oyster Creek Analysis of RPS Failure.



*RPS = reactor protection system

to define the probability statement explicitly.) Numerically, the expectation of this p.d.f. is $<WS|AT,\bar{x}> \simeq 5x10^{-5}$/demand for Oyster Creek. However, if it is assumed that two anticipated transients are likely per reactor year the resulting mean estimate of an ATWS event at Oyster Creek is $10^{-4}$ per reactor year. This value does not meet the NRC's desired criterion of $10^{-6}$ undesirable ATWS events per reactor year. This limit can only be reached if each sub-system's failure frequency is reduced to $\sim10^{-6}$. Such a risk reduction is estimated to cost several tens of millions of dollars and is particularly expensive and costly for operating plants. Plant outage for extended retrofits such as would be required to satisfy the NRC's ATWS guidelines could run into hundreds of millions of dollars because of the expense of replacement power.* Thus, a possible next step in ATWS analysis is to do a cost-benefit tradeoff between mitigation system alternatives and retrofit costs and the expected benefits (or disbenefits) of such alternatives expressed as the reduction (or increase) in public health risks.

## A.4 <u>The Browns Ferry Incident</u>

On June 28, 1980 76 of the 185 control rods failed to fully insert during a routine shutdown at TVA's Browns Ferry Unit No. 3 located at Athens Alabama. The reactor was manually scrammed from about 30 percent power in accordance with routine shutdown procedures. The shutdown was initiated to repair the feedwater system. The 76

*At TMI for example over 60% of the expense of the accident is estimated to be due to payments for replacement power.

control rods that failed to fully insert were all on the east side of the core.

Following scram discharge volume (SDV) high level bypass and a short drain period of the SDV, a second manual scram was initiated and all partially inserted rods were observed to drive inward but 59 remained partially withdrawn. A third manual scram was made again following high level in the SDV and bypassing for another short drain of the SDV with the result that 47 rods remained partially withdrawn. Following a longer drain of the SDV an automatic scram occurred that was initiated by a scram discharge volume tank high water level signal when the scram reset switch was placed in "Normal"; with this scram all remaining rods fully inserted. The total time elapse from the initial scram to the time that all rods were inserted was approximately 15 minutes. Core coolant flow, temperature and pressure remained normal for plant conditions. The unit is now shutdown and additional testing indicates that a possible cause of the malfunction was the retention of a significant amount of water in the east bank scram discharge volume.

As a result of this incident, the NRC has required that all BWRs perform a test of their scram system to identify any safety related problem as they relate to the scram discharge volume and associated piping. A subsequent test performed at the Dresden BWR plant revealed that after manually scramming the reactor the banks of the CRD scram discharge volumewere over half full.[9] This was discovered by ultrasonic tests. Diagnosis revealed that the suction ball valve on the scram discharge volume vent line had failed to open. It also revealed that the SDV takes too long to vent on one bank when this ball valve fails due to a long "trickle line" back to the CRD instrument volume. The NRC therefore required all BWR-3s to cut this vent line (or at least make a hole in it) to alleviate the consequences of a valve failure and consequent failure to scram. They required the vent line to be cut on both banks of CRDs. General Electric Co. is currently preparing design changes to the overall SDV system including an improved suction valve, new drain lines, and direct monitoring of the SDV rather than inferred monitoring via the instrument volume level. It was also discovered that the alarm points on the instrument volume were mixed (i.e., warning points and scram point reversed). Thus, the NRC was greatly concerned that the unit had operated in this condition for so long. Further information on the Dresden tests is available through the NRC bulletin on these tests.

The tests on the scram system in BWRs may provide additional data to confirm or reject the failure rate postulated for the SDV in the Oyster Creek probabilistic analysis study. The controversey surrounding ATWS will remain until an acceptability criterion on the frequency of ATWS occurrence can be agreed upon. The NRC staff has already decided to resolve the ATWS controversey apart from the analytic approach since the staff claims[10] that the analytic approach renders too wide a range of answers depending upon the assumptions used. The industry has argued continually that the analytic approach be emphasized and that debate surround the assumptions used rather than the quantitative framework itself.[7] At this time it seems likely that ATWS will continue as an unresolved issue.

## B. The Issue of Nitrogen Inerting in BWR Primary Containments

### B.1 Summary of Study Results

Hydrogen control is important in post-accident situations because of possibilities for containment rupture because of hydrogen deflagration or detonation. Post-accident hydrogen generation in BWR containments is analyzed as a function of engineered hydrogen control system assumed either nitrogen inerting or air dilution. Fault tree analysis was applied to assess the failure probability per demand of each system. These failure rates were then combined with the probability of accidents producing various hydrogen generation rates to calculate the overall system hydrogen control probability. Results indicate that both systems render approximately the same overall hydrogen control failure rate on demand (air dilution: $8.3 \times 10^{-2}$ - $1.1 \times 10^{-2}$; nitrogen inerting: $1.3 \times 10^{-2}$ - $2 \times 10^{-3}$). Drywell entries and unscheduled shutdowns were also analyzed to determine the impact on the total BWR accident risk as it relates to the decay heat removal system. Results indicate that inerting may increase the overall risk due to a possible increase in the number of unscheduled shutdowns due to a lessened operator ability to correct and identify "unidentified" leakage from the primary coolant system. Further, possible benefits of inerting due to reduced torus corrosion and fire risk in containment appear to be dominated by the possible operations related disadvantages.

## B.2 Introduction

The accident at Three Mile Island (TMI) has led to a reevaluation of federal safety regulations and utility operating procedures. Because of concern over hydrogen production from zircalloy fuel cladding oxidation in accidents where fuel temperatures rise substantially, the Nuclear Regulatory Commission (NRC) has made several recommendations for change in operating facilities. One of these recommendations would require all BWR containment structures to be inerted with nitrogen. Although most Mark I BWRs are now inerted, it has not been quantitatively established that public health risk has been reduced by this procedure. Moreover, many utility engineers remain concerned over the possibility that inerting might actually increase public health risk. They argue that a readily accessible containment may be a significant factor affecting accident mitigation. Also, utilities are concerned that inerting may increase occupational health risks. Concern over worker safety arises from the replacement of oxygen by nitrogen in the containment, producing an inhabitable atmosphere.

This study applies probabilistic risk assessment (PRA) methods to assess the safety impact of containment inerting, comparing the inerting system with that of the air dilution hydrogen control system installed at the Vermont Yankee plant. This analysis provides a basis upon which conclusions can be drawn concerning the value of containment inerting as a safety device.

This paper is divided into five sections, discussing first the hydrogen generation problem during the Three Mile Island incident, NRC response to the incident and previous regulatory history related to inerting, and a brief review of the hazards of inerting. The second section discusses the hydrogen generation problem, mechanisms for hydrogen production, properties of hydrogen-oxygen mixtures and methods for control in BWRs. In the third section, a probabilistic framework for analyzing the probability of controlling post-accident hydrogen in BWRs is outlined and results reviewed. In the fourth section, related issues regarding the impact of containment inerting on reactor safety are also analyzed including the impact on unscheduled shutdowns, torus corrosion and fire risk. Finally, a discussion and summary of results follow.

During the accident at TMI, a significant amount of hydrogen was produced through the oxidation of zirconium cladding as it interacted with steam. The amount of cladding that reacted is estimated to be between 50 to 70 percent (NSAC(1)). (In the design of hydrogen control systems for accidents, the design basis had expected less than a .1% metal-water reaction.) About nine hours into the accident, a pressure pulse of 28 psig was recorded in the containment building due to a hydrogen burn. The pressure spike was below the 60 psig design pressure of the containment building, and well below the expected burst pressure of 160 psig (Wooten et al. [2]). The hydrogen generated by the large metal-water reaction at TMI and the resulting pressure increase in the containment were considered in the NRC TMI-2 Lessons-Learned Task Force (NRC [3]). Recommendations were made for the control of hydrogen including that all BWR containments should be inerted with nitrogen to prevent hydrogen burns or explosions. Following a prolonged set of hearings, a memorandum and order were issued in 1974 stating that inerting was not justified pending the outcome of a full hearing because the evidence presented showed that inerting creates problems with greater consequences than those it was intended to solve (Farrar et al. [4]).

### B.3 The Hydrogen Generation Problem

Hydrogen presents two potential threats to containment integrity; first, increasing the internal gas pressure, and secondly, burning or exploding when combined with the oxygen present in the containment resulting in containment failure by overpressurization. Hydrogen can be produced during an accident by high temperature metal-water reactions between cladding and reactor coolant, by radiolytic decomposition of water, and by corrosion of metals by solutions used for emergency cooling or containment sprays. The main source of hydrogen from metal-water reactions is produced through the high temperature zircalloy-water and steel-water reactions, which is the initial source of hydrogen when steam contacts the overheated zircalloy fuel cladding.

### B.3.1 Pressure Rise Due to Hydrogen Deflagration

The pressure rise due to combustion of hydrogen can be predicted from the burning rate, which depends on the geometry of the vessel and velocity of the propagating flame. The maximum possible pressure rise in a closed vessel can be determined by assuming complete combustion of hydrogen with no heat loss to the vessel walls (Slifer et al. [5]). The combustion energy is absorbed by the mixture of combustion products. The overall energy balance is:

$$\Delta U = \overline{C}_v n_f (T_f - T_o) = n_o [H_2] \Delta u^o \qquad (1)$$

where:

$H_2$ = mole fraction of hydrogen

$n_o$ = total moles of initial mixture

$T_o$ = initial temperature before combustion

$\Delta u^o$ = combustion energy per mole of hydrogen

$\Delta U$ = internal energy difference

$n_f$ = total moles of final mixture

$C_v$ = average specific heat at constant volume

$T_f$ = temperature of the final mixture

Assuming ideal gas behavior, the ratio of the final pressure $P_f$ to the initial pressure $P_o$ is:

$$\frac{P_f}{P_o} = \frac{n_f}{n_o} \frac{T_f}{T_o} \qquad (2)$$

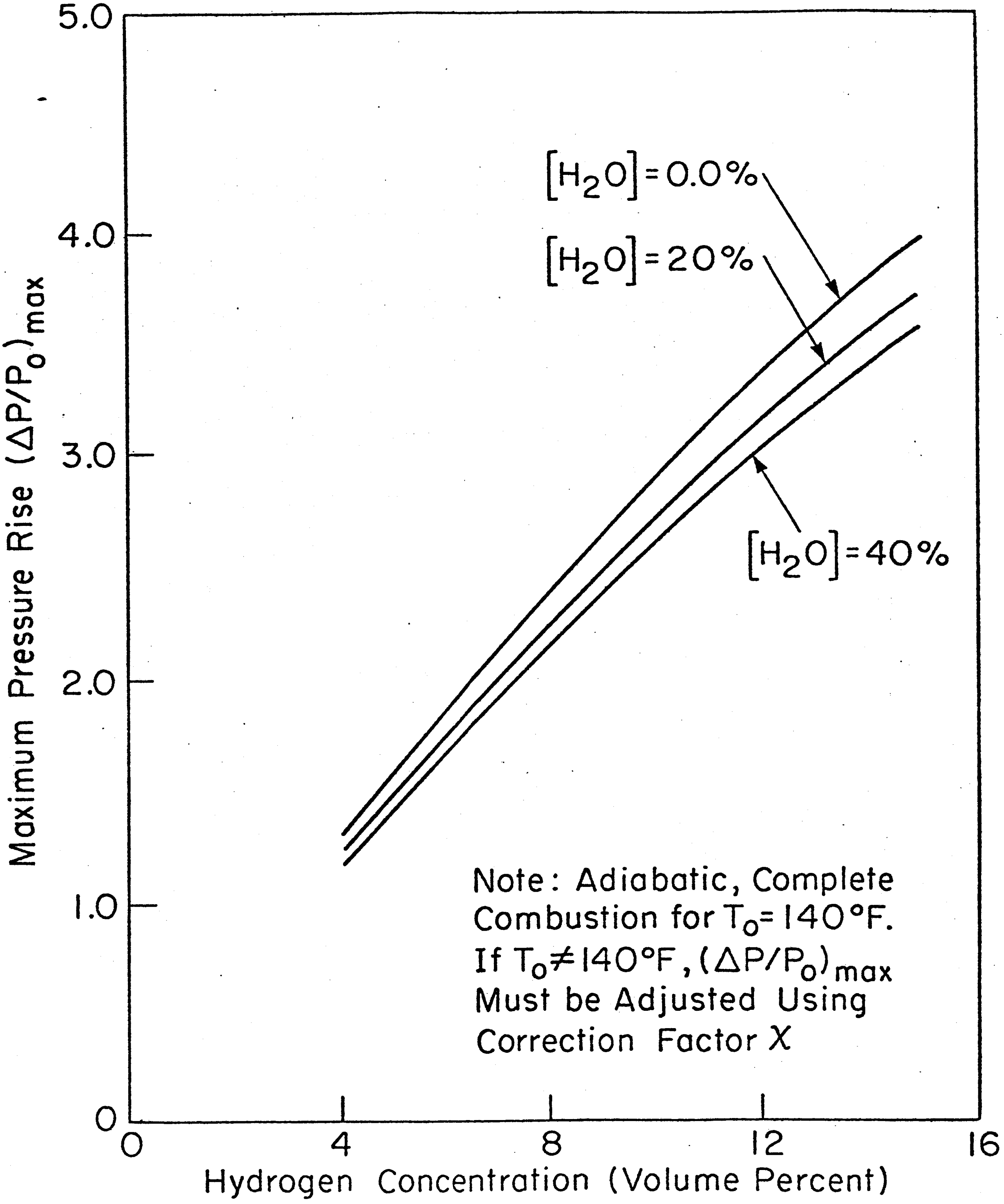


Figure 1a Final Pressure vs Hydrogen Concentration

Solving for $T_f$ from equation (1) and substituting into equation (2) gives the maximum pressure rise as:

$$\left.\frac{\Delta P}{P_o}\right|_{max} = \frac{P_f - P_o}{P_o} = \frac{\Delta u^o[H_2]}{\overline{C}_v T_o} + \frac{n_f}{n_o} - 1 \qquad (3)$$

This result is plotted against the intial percentage of hydrogen for initial water vapor concentrations (Figure 1a). This model can be used to predict the pressure transients associated with burning of various concentrations. The pressure transients in a Mark I drywell for hydrogen concentrations of up to 18 volume percent are also shown (Figure 1b).

### B.3.2 Methods for Hydrogen Control in Boiling Water Reactors

Several systems have been used to control flammable hydrogen-oxygen mixtures by maintaining the hydrogen below the flammability limits established by the regulatory guides (four volume percent hydrogen concentration and five percent volume oxygen (NRC[6])). Methods besides inerting include combinations of air dilution systems, recombiners and controlled venting. Containment inerting consists of purging the containment atmosphere with nitrogen until the oxygen concentration is below five volume percent during operation. In the event of an accident, a nitrogen make-up system is activated to help reduce the hydrogen concentration to four volume percent and maintain the oxygen concentration below five volume percent. Controlled venting through the standby gas treatment system (SGTS) is provided to reduce the pressure inside the containment (Boston Edison [7]).

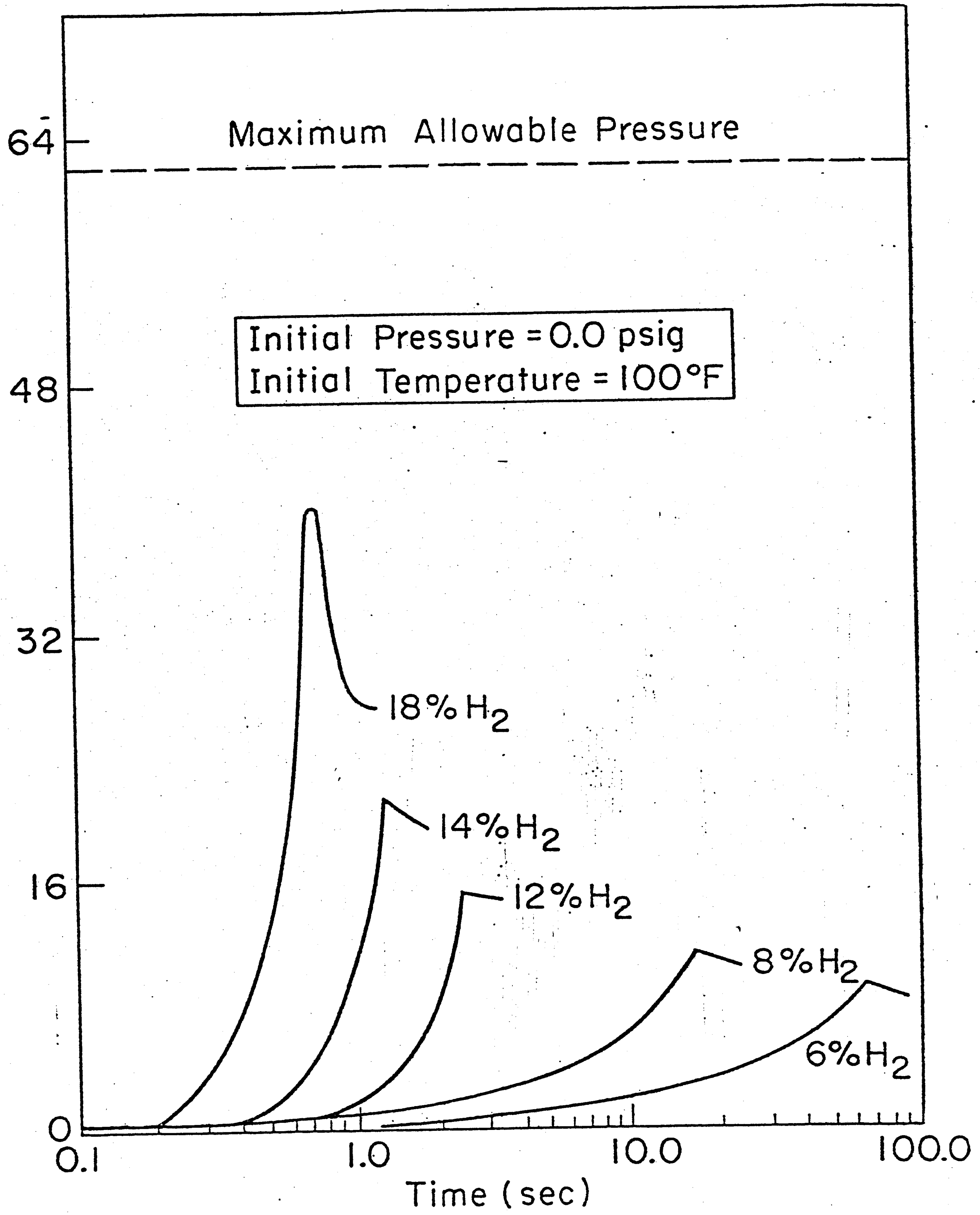


Figure 1b Pressure Response for Hydrogen Combustion in BWR Mark I Drywells.

In the containment air dilution system (CAD), the atmosphere in the containment is diluted with air during and after an accident (Wilson and Slifer [8]). System design is based on the requirement that the containment atmosphere be maintained below four volume percent hydrogen in the event of an accident. The system monitors the hydrogen gas concentration and injects additional air as required to dilute the hydrogen and maintain it below the flammability limit. Controlled venting is manually initiated when, during an accident, the pressure reaches half the drywell design pressure of 28 psig (Vandenburgh [9]). Venting of the containment atmosphere occurs only if after an accident, the hydrogen concentration approaches four volume percent. Venting times are designed on the basis of dose acceptability (Commonwealth Edison [10]). Fission product releases are minimized by passing the vented gas through chemical scrubbers or charcoal filters in the standby gas treatment system. However, control of noble gas radioactivity under venting conditions is very difficult (Keilholtz [11]).

If filtered venting is acceptable, there are a variety of non-venting recombiner schemes available. Chemical recombination of hydrogen is a way to prevent hydrogen burning and at the same time control increases in hydrogen pressure. Applied to BWRs, recombiners would need to be more complex and expensive, requiring a supplementary oxygen supply to consume all the hydrogen that might be produced. Recombiners can be classified into flame, catalytic and electrical types (Keilholtz [11]). The principal disadvantages of flame recombiners is the possibility of extinguishing the flame and having it "flash back" through the injector. Catalytic recombiners use a catalytic bed that maintains the gas mixture through chemical recombination below the flammability limits and are now in use in PWRS. Recent designs include nickel and nickel-chromium oxide combinations supported on aluminum-oxide bases and platinized honeycomb ceramic disks. Disadvantages include choice of diluent, condensing or non-condensing reactions, catalyst, preheat temperature, pressure-drop specifications, vessel materials and number of recombining stages. Electric recombiners use electric resistance heaters to heat the continuous flow of containment atmosphere to above the hydrogen-oxygen reaction temperature.

## B.4 Quantification of the Probability of Controlling Post-Accident Hydrogen in BWRs

A comparative analysis of the air dilution system (CAD) and the inerting system (CIS) is made to find the influence on the probability of containment failure due to post-accident hydrogen generation as a function of control system installed. In order to assess the overall probability that the CAD or the CIS systems are capable of handling a given amount of hydrogen generated during an accident, a set of probabilities need to be calculated. Fault trees are used to calculate the probabilities of failure on demand, denoted $P_f(S)$, of the CAD and CIS hydrogen control systems. Using probabilities of failure of each system, the probability that the systems are available to work, denoted $P_{CAD}(S)$ and $P_{CIS}(S)$, are defined as follows:

$$P_{CAD}(S) = 1 - P_f(S) \tag{4}$$

$$P_{CIS}(S) = 1 - P_f(S) \tag{5}$$

The next step in the analysis is to calculate the probability of hydrogen generation, or percent metal-water reaction, given that an accident occurs. From WASH-1400, large LOCA accidents in BWRs have a probability of producing a core melt of ∿ $3x10^{-5}$/reactor-year (U.S.N.R.C. [12]). For these accidents, it is assumed that all the zirconium reacts with water to produce hydrogen. The following important assumption was made in this work based on a linear interpolation process reflecting our best engineering estimates. For small accidents with probabilities in the range of $3x10^{-3}$/reactor-year, it is assumed that the metal-water reaction linearly decreases from about 100% to almost zero and remains zero over the range of the higher probability yet less serious accidents (Figure 2a).

The maximum amount of hydrogen produced by a metal-water reaction is shown (Figure 3). For a 100% metal-water reaction, the maximum hydrogen concentration in a BWR Mark I containment is 72 volume percent. At this value, the percent metal-water reaction required to reach four volume percent hydrogen concentration is achieved in four or five minutes, implying a generation rate between $144x10^3$ and $180x10^3$ cuft/hr. These values are the upper bound of the hydrogen generation rate plotted (Figure 2b). The accident at Three Mile Island generated hydrogen at approximately $100x10^3$ cuft/hr (Batelle Colombus [2]) (Figure 2b).

The air dilution system is designed to work when the hydrogen concentration reaches four volume percent, which in the design basis accident occurs in approximately nineteen hours. If a generation rate of ∿ 1000 cuft/hr is assumed, the probability of success of the CAD in controlling the hydrogen is 1 from equation 4 (fault tree analysis showed a failure rate of $8.3x10^{-2}$ - $1.1x10^{-2}$). During normal operations, the CAD system pressurizes the containment to reduce the hydrogen concentration, and then vents through the standby gas treatment system to reduce the pressure at a maximum venting rate of 2400 cuft/hr. If the four volume percent hydrogen limit is reached in one hour, this corresponds to a generation rate of ∿ 12,000 cuft/hr and a

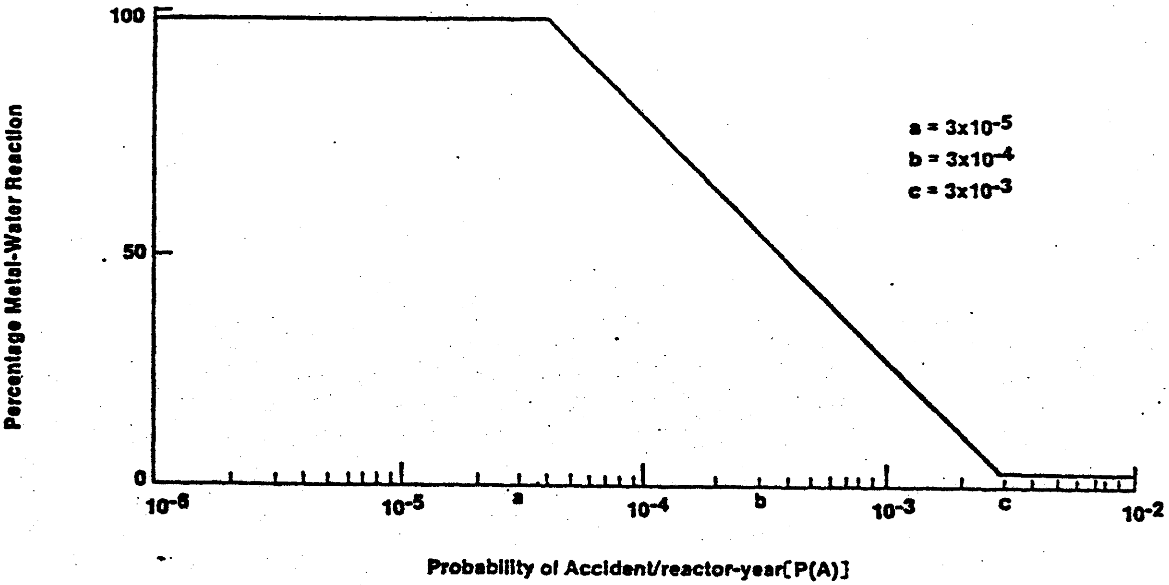


Figure 2a Percentage Metal Water Reaction vs Probability of Accident per Reactor-Year.

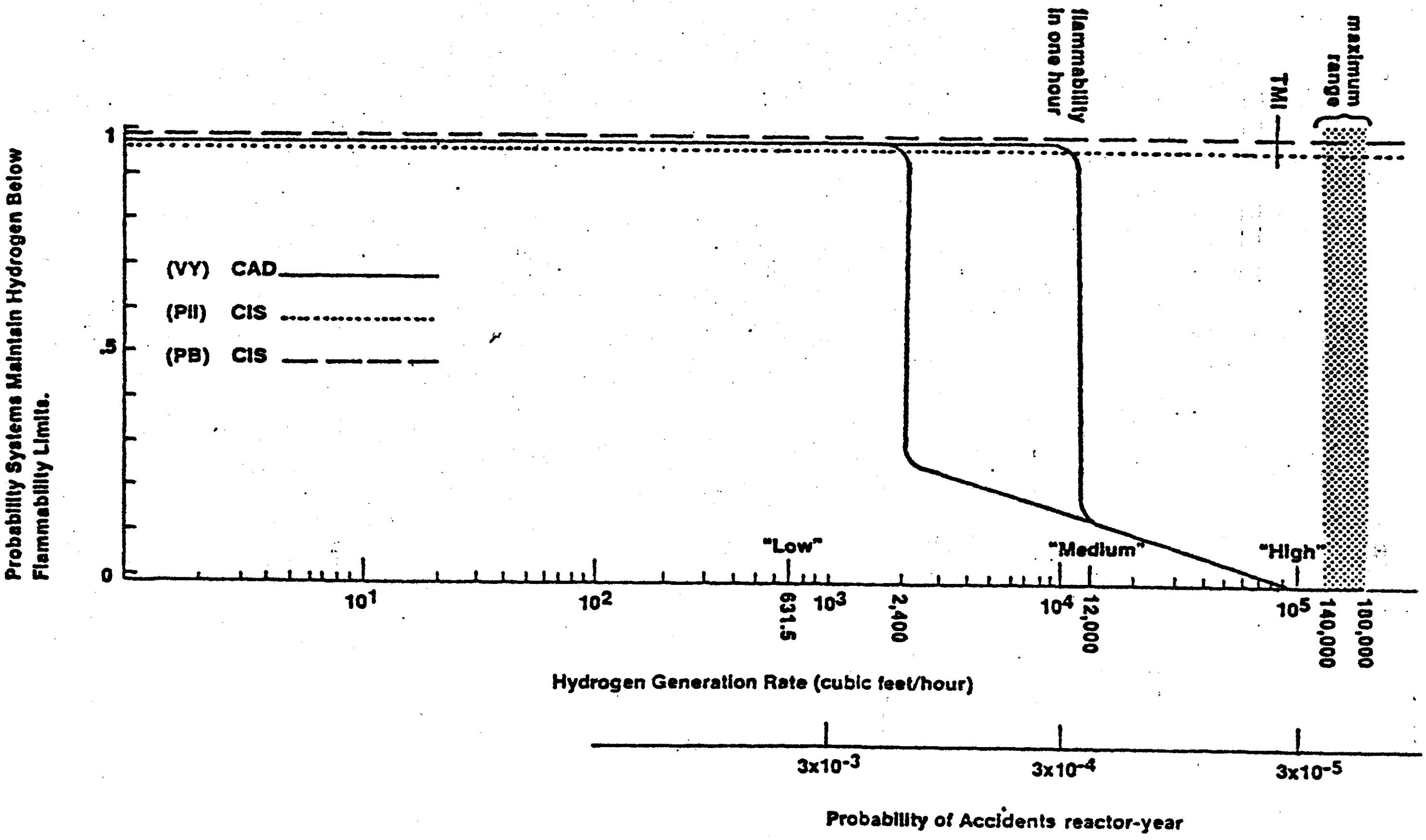


Figure 2b Probability of Air Dilution (CAD) and Inerting (CIS) Systems to Control Hydrogen vs Hydrogen Generation Rate.

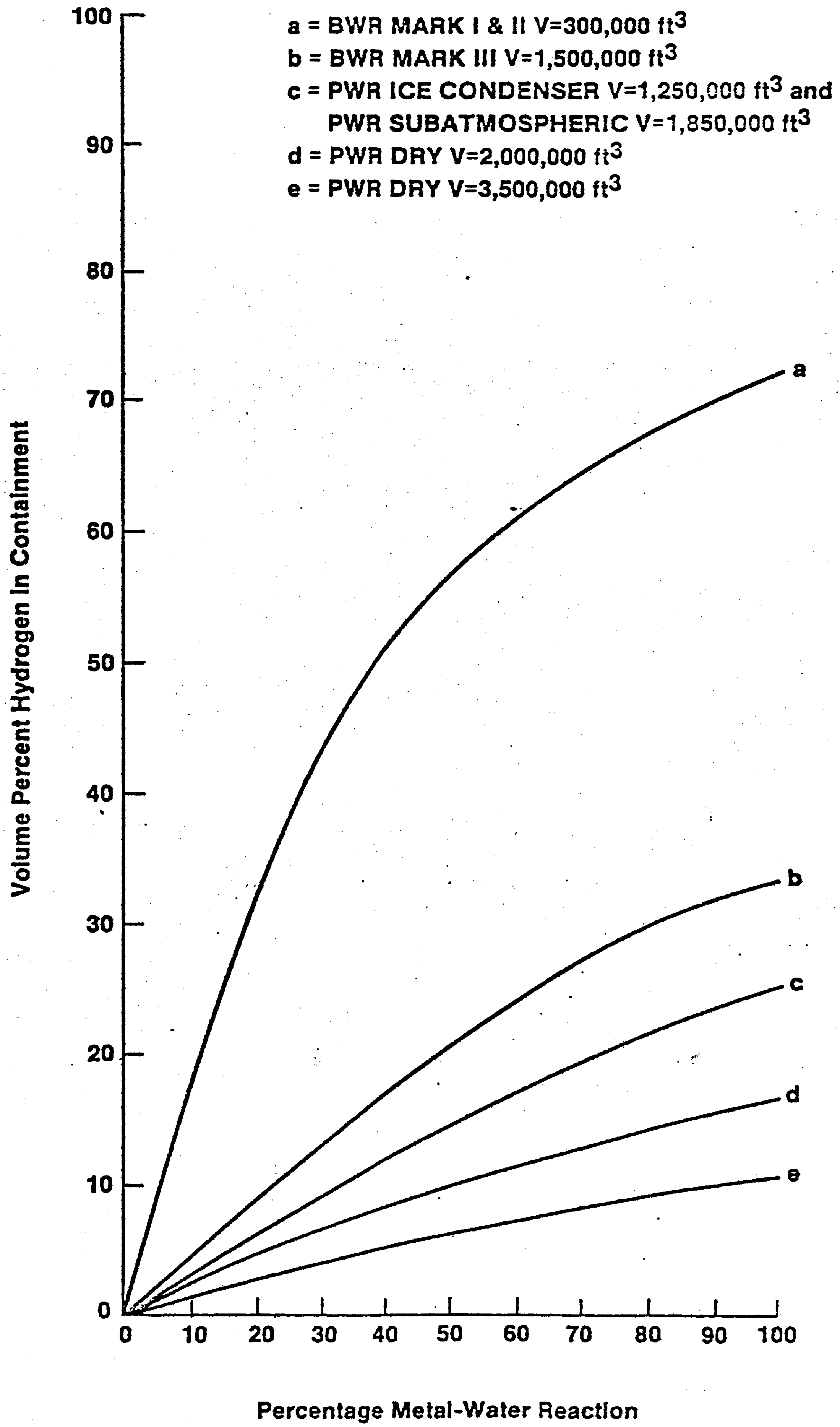


Figure 3 Volume Percent Hydrogen in Containment vs Percentage Metal Water Reaction.

probability of accident of ∿ $3x10^{-4}$/reactor-year using the assumed linear interpolation of Fig. 2a.

As the hydrogen generation rate increases, the probability of accident decreases (Figure 2a). For low probability accidents, the probability of the air dilution system being able to handle high hydrogen generation rates drops almost to zero. For the inerting system, the probability of controlling the hydrogen remains at about one during normal reactor operations, since the hydrogen cannot burn. However, during the 24 hour period prior to shutdown and after startup when the drywell is not inerted, the probability of having a combustible mixture increases because the oxygen concentration is above five volume percent.

### B.4.1 Hydrogen Related Event Tree

The design basis LOCA in a BWR is defined as a double-ended rupture of the primary coolant recirculation line (U.S.N.R.C. [12]). A small LOCA is defined as a break in the cooling system of about 1/2 to 2 inches in diameter. The sequence of events for both large and small LOCAs is very similar, the differences are in the emergency coolant injection and scram requirements. A reduced event tree is developed here with emphasis on those sequences that lead to hydrogen generation and eventually to failure of the containment due to hydrogen overpressurization (Figure 4).

The initiating event is assumed a rupture in the reactor coolant system defined as a break in the recirculation lines. The next branch point occurs at electric power followed by the reactor protection system that provides the reactor trip in case of an accident. The next branch point occurs at the vapor suppression system. If the vapor suppression system fails, the primary containment fails due to overpressurization. The next event refers to the

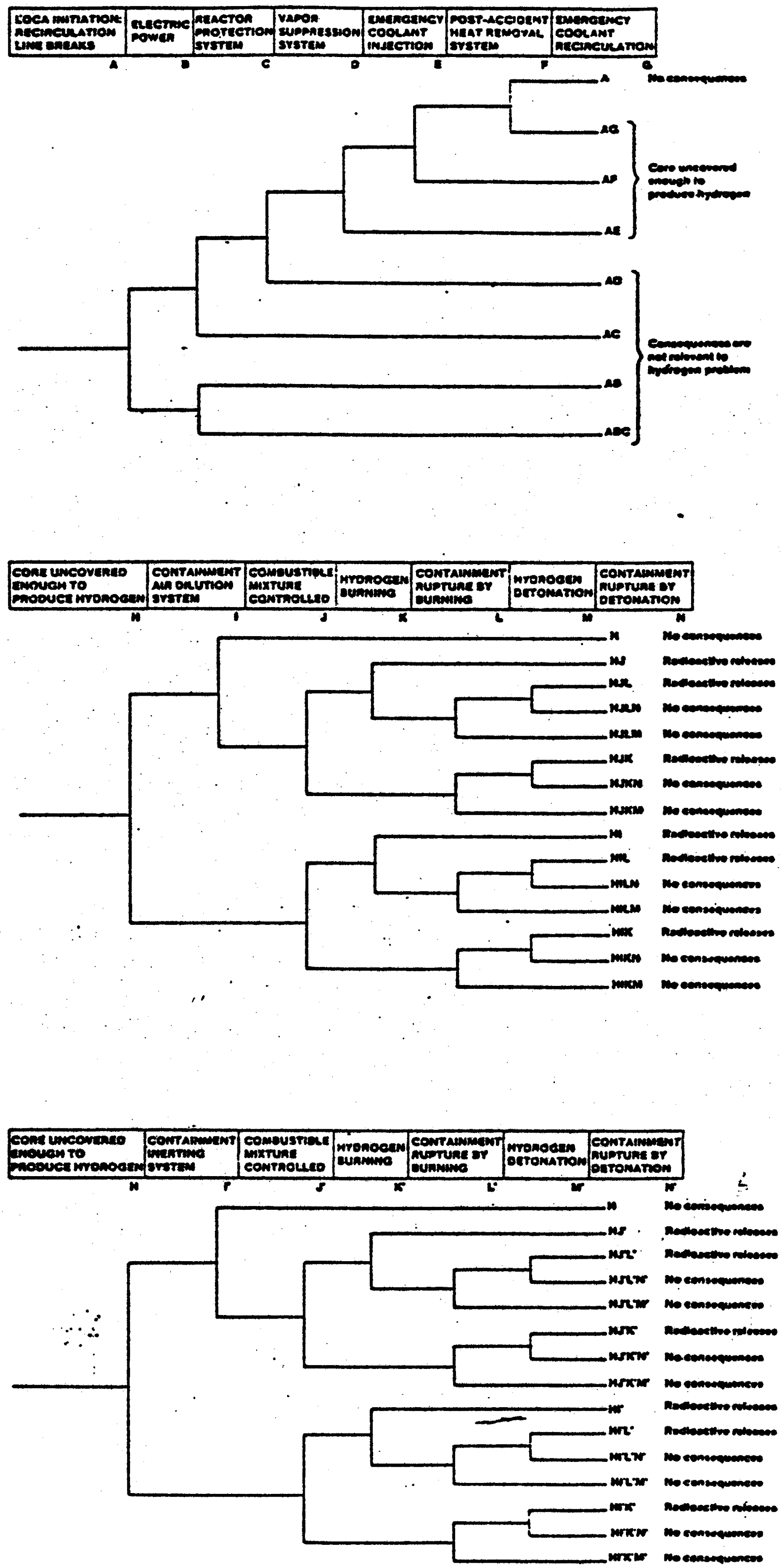


Figure 4 Hydrogen Related BWR LOCA Event Tree.

emergency coolant injection system. Failure of this system could leave the core uncovered long enough to produce significant amounts of hydrogen.

The hydrogen event tree indicates the sequence of events required in hydrogen control. The first column in the tree relates to the control system in place (CAD or CIS); if this system is not used or fails on demand, the hydrogen is not controlled. If the system works and is used, the system may control the hydrogen mixture. If the combustible mixture is uncontrollable, the next event in the sequence will be hydrogen burning. If the hydrogen burns, the next event is containment failure due to overpressurization. If there is no rupture or no hydrogen burning, the hydrogen concentration could increase to the detonation limits (20 volume percent) and explode; the final event is containment rupture by detonation.

Assuming the combustible mixture is controlled and there is no containment failure, the core could remain uncovered, increasing the rate of hydrogen production while building up radioactivity. If the core continues to stay uncovered, eventually it will start to melt and other events may dominate the hydrogen problem. The different stages affect the probabilistics of hydrogen control (Figure 4). In order to assess the probability that the air dilution or inerting systems can handle the hydrogen generated in an accident, a detailed analysis was next attempted.

### B.4.2 Fault Tree Analysis of Hydrogen Control Systems

The potential failure modes of the air dilution and inerting systems were analyzed and failure probabilities derived using plant specific data from three utilities, and failure data from WASH-1400 (Tables I and II). Fault tree analysis was applied to perform the analysis and derive the failure probability estimates. The following assumptions were made in performing the analysis: (i) independent component failures were considered; (ii) electric power was assumed operable during the time of the accident;

Table I

EVENT PROBABILITIES USED IN CONTAINMENT AIR DILUTION SYSTEM FAULT TREE

| EVENT DESCRIPTION | FAILURE PER DEMAND | ERROR FACTOR* |
|---|---|---|
| Loss of Power | $1x10^{-6}$ | 30 |
| Valves drywell wrong position | $>1x10^{-10}$ | — |
| Valves torus wrong position | $>1x10^{-10}$ | — |
| Operator error: at leat one valve per line | $>1x10^{-10}$ | — |
| Operator fails to stop compressor | $1x10^{-2}$ | 10 |
| Compressor fails to stop | $1x10^{-4}$ | 10 |
| Sample pump failure | $1x10^{-3}$ | 3 |
| Hydrogen analyzer wrong concentration | $1x10^{-6}$ | 10 |
| Operator fails to start primary hydrogen analyzer | $1x10^{-2}$ | 10 |
| Operator fails to start secondary hydrogen analyzer | $3x10^{-1}$ | 10 |
| Hydrogen analyzer start mechanism mechanism failure | $1x10^{-4}$ | 10 |
| Portable compressor unavailable when needed | $1x10^{-1}$ | 10 |
| No power from diesel-generator | $3x10^{-2}$ | 10 |
| Compressor fails to start | $1x10^{-3}$ | 10 |
| Operator fails to start compressor 1 | $1x10^{-2}$ | 10 |
| Operator fails to start compressor 2 | $1x10^{-1}$ | 10 |

*Error factor is to be used to multiply failure per demand to obtain the upper bound, and to divide

Table II

EVENT PROBABILITIES USED IN CONTAINMENT INERTING SYSTEM FAULT TREE

| EVENT DESCRIPTION | FAILURE PER DEMAND | ERROR FACTOR* |
|---|---|---|
| Valves between containment and make-up subsystem closed | $1x10^{-6}$ | — |
| Oxygen analyzer failure | $1x10^{-6}$ | 10 |
| Operator error: at least one valve per line | $>1x10^{-10}$ | — |
| Loss of Power:all valves closed | $1x10^{-6}$ | 30 |
| Operator fails to open make-up valves | $1x10^{-2}$ | 10 |
| Make-up valves fails to open as required | $3x10^{-4}$ | 10 |
| Nitrogen line frezzes | $1x10^{-8}$ | 10 |
| Cryogenic tank breaks | $1x10^{-8}$ | 10 |
| No $LN_2$ trucks supply | $3x10^{-3}$ | 10 |
| Hydrogen analyzer failure | $1x10^{-2}$ | 10 |

*Error factor is to be used to multiply failure per demand to obtain the upper bound, and to divide it to obtain the lower bound.

(iii) the stack gas treatment system was assumed operational when required; (iv) the rare event approximation was used; (v) failure probabilities are placed on a per demand basis, referring to component unavailability or human error, and are assumed independent of time; and (vi) point values are used from fixed data and error propagation follows the procedures of WASH-1400. For the air dilution system, an additional assumption was made: the failure probability of the air compressor refers to initial usage with availability assumed to decrease during the cycling process. For the inerting system, the assumption was made that the containment is inerted at the time of the accident; further performance during the accident reflects the individual design characteristics of the particular inerting system analyzed.

The first step in developing a fault tree is to define a top event. For the CAD system, the top event is defined as the failure of the system to maintain the hydrogen concentration below the NRC mandated flammability limit of four volume percent (Figure 6a). For the inerting system, the top event is the failure to maintain both hydrogen and oxygen concentrations below the NRC mandated flammability limits.

The air dilution system consists of three subsystems: (i) the hydrogen analyzer system, (ii) the air injection system consisting of redundant air compressors, and (iii) a manually initiated containment venting system connected to the stack gas treatment system. The inerting system consists of three subsystems designed to function as follows: (i) initial purging of the primary containment within 24 hours after startup, (ii) providing a

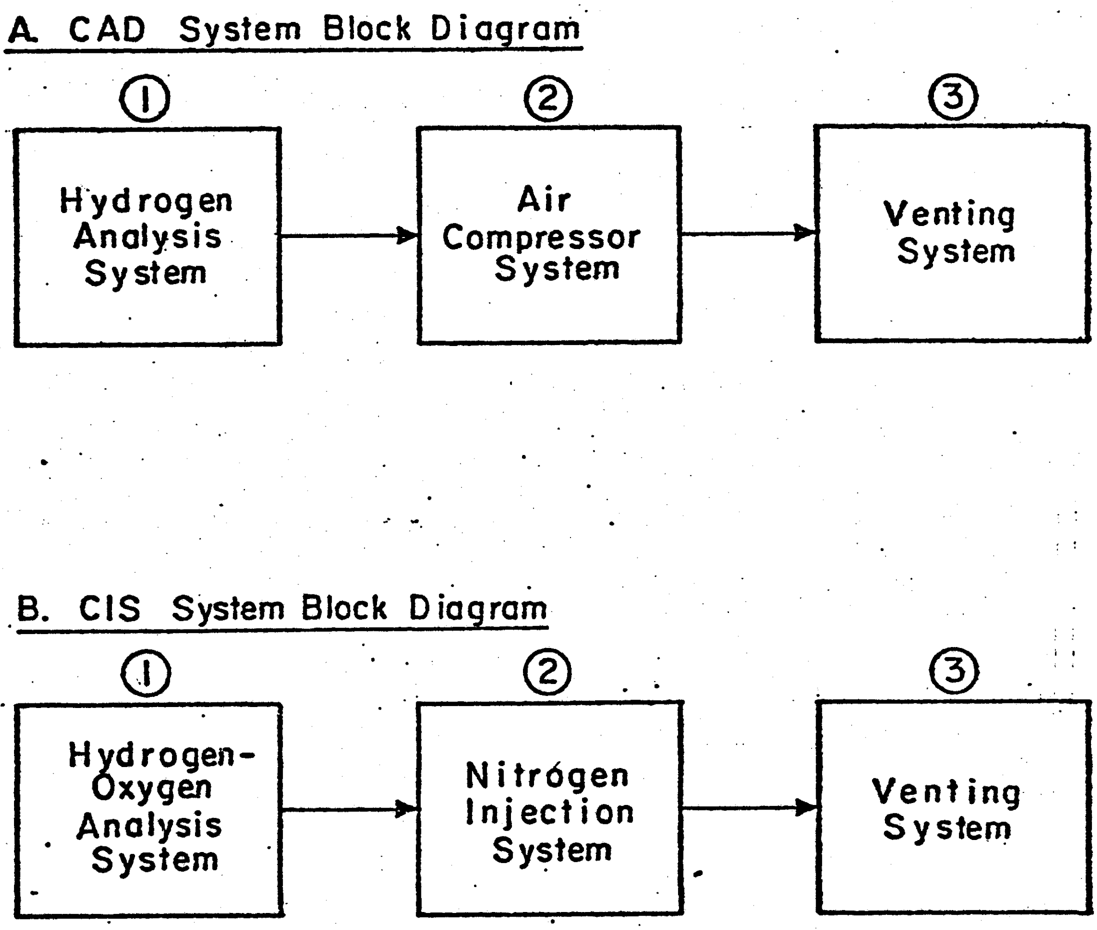

A. CAD System Block Diagram
1
Hydrogen Analysis System
2
Air Compressor System
3
Venting System
B. CIS System Block Diagram
1
Hydrogen-Oxygen Analysis System
2
Nitrógen Injection System
3
Venting System

Figure 5.Critical Sub-Systems of Hydrogen Control Systems

Block diagrams of each of the analyzed hydrogen control systems are shown here for the air dilution (CAD) and inerting (CIS) systems.

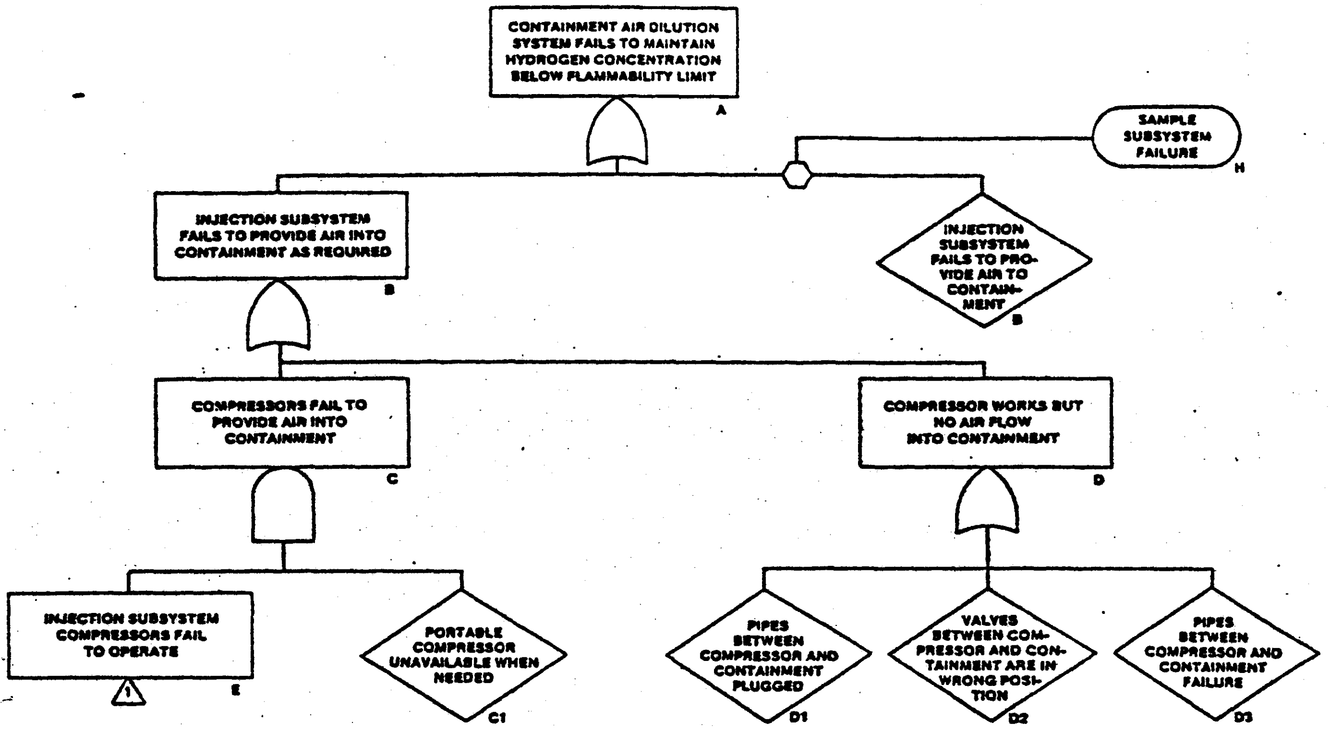

CONTAINMENT AIR DILUTION SYSTEM FAILS TO MAINTAIN HYDROGEN CONCENTRATION BELOW FLAMMABILITY LIMIT
A
SAMPLE SUBSYSTEM FAILURE
H
INJECTION SUBSYSTEM FAILS TO PROVIDE AIR INTO CONTAINMENT AS REQUIRED
B
INJECTION SUBSYSTEM FAILS TO PRO-VIDE AIR TO CONTAIN-MENT
B
COMPRESSORS FAIL TO PROVIDE AIR INTO CONTAINMENT
C
COMPRESSOR WORKS BUT NO AIR FLOW INTO CONTAINMENT
D
INJECTION SUBSYSTEM COMPRESSORS FAIL TO OPERATE
1
E
PORTABLE COMPRESSOR UNAVAILABLE WHEN NEEDED
C1
PIPES BETWEEN COMPRESSOR AND CONTAINMENT PLUGGED
D1
VALVES BETWEEN COM-PRESSOR AND CON-TAINMENT ARE IN WRONG POSI-TION
D2
PIPES BETWEEN COMPRESSOR AND CONTAINMENT FAILURE
D3

Figure 6a Abbreviated Fault Tree for the Containment Air Dilution System.

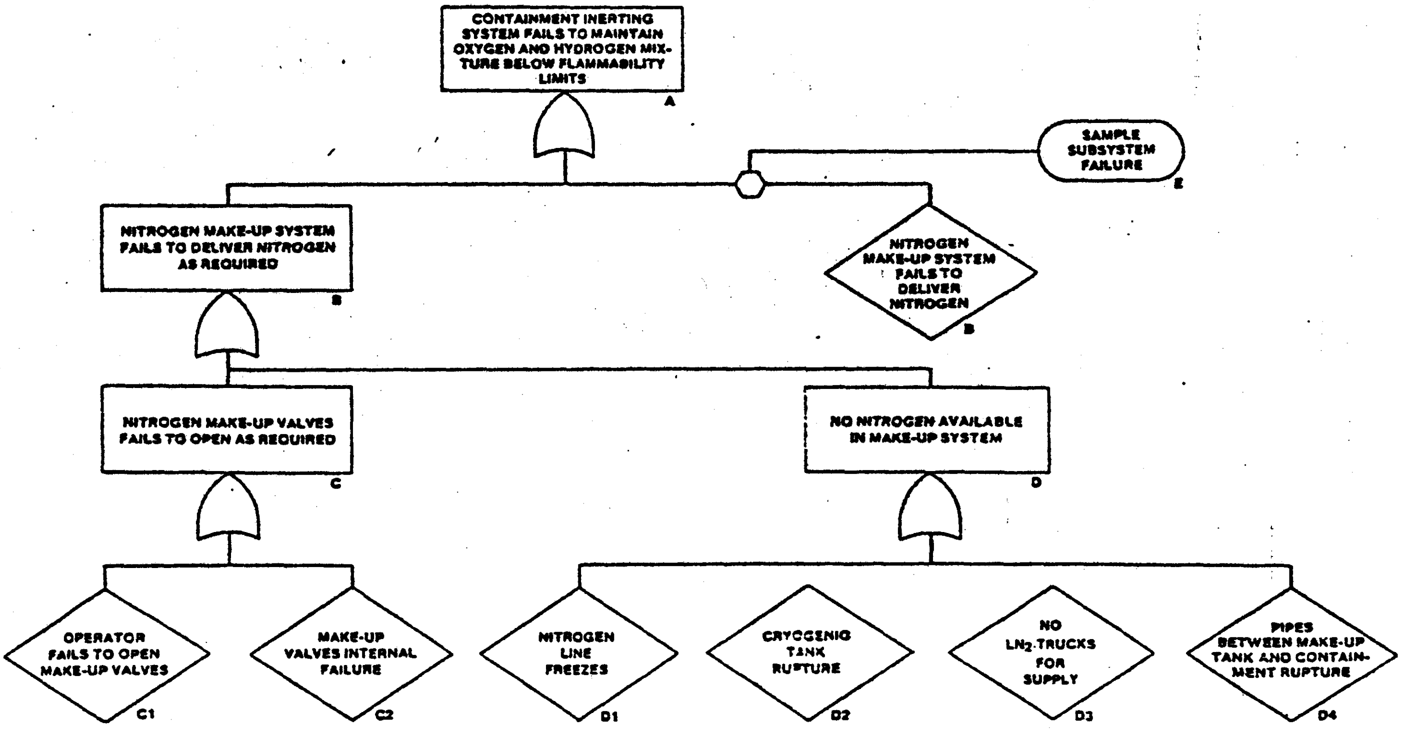

CONTAINMENT INERTING SYSTEM FAILS TO MAINTAIN OXYGEN AND HYDROGEN MIX-TURE BELOW FLAMMABILITY LIMITS
A
SAMPLE SUBSYSTEM FAILURE
E
NITROGEN MAKE-UP SYSTEM FAILS TO DELIVER NITROGEN AS REQUIRED
B
NITROGEN MAKE-UP SYSTEM FAILS TO DELIVER NITROGEN
B
NITROGEN MAKE-UP VALVES FAILS TO OPEN AS REQUIRED
C
NO NITROGEN AVAILABLE IN MAKE-UP SYSTEM
D
OPERATOR FAILS TO OPEN MAKE-UP VALVES
C1
MAKE-UP VALVES INTERNAL FAILURE
C2
NITROGEN LINE FREEZES
D1
CRYOGENIC TANK RUPTURE
D2
NO LN2 TRUCKS FOR SUPPLY
D3
PIPES BETWEEN MAKE-UP TANK AND CONTAIN-MENT RUPTURE
D4

Figure 6b Abbreviated Fault Tree for the Containment Inerting System.

supply of make-up nitrogen during accidents that produce hydrogen, and (iii) providing a way to sample the drywell and torus for oxygen concentration and the drywell for hydrogen concentration. (Figure 5)

In the air dilution case, the top event can occur if the injection subsystem fails to provide air to the containment as required. The failure probability of the injection subsystem could be increased if the sample subsystem fails to detect the hydrogen concentration correctly. In this case, the operator would not know when to correctly start the air compressors. The failure of the sample subsystem takes place with the failure of the hydrogen analyzers to detect the hydrogen concentration (Figure 6a), or with the failure of the component pipes, valves, pumps due to malfunction. The two redundant hydrogen analyzers could fail due to improper calibration. Another failure mode is the failure of the analyzer to start due to malfunction or operator error. The air injection system can fail because of failure of the system air compressors, and the unavailability of a portable compressor that could be connected to the system in the case of failure of the principal compressors. However, if at least one of the available compressors work, failure could still occur due to failure of the air to flow into the containment due to a rupture or plug of the connecting air pipes, or valves in wrong position. The failure of the main compressors is dependent upon one of more of the following events occurring: power failure, malfunction of the compressors, operator failure to start the compressors, or failure of the analyzers to perform on demand.

The inerting system prevents a flammable mixture from developing by maintaining the oxygen concentration below five volume percent; a make-up system is used during an accident to maintain the oxygen below five volume percent. Failure of the make-up system can therefore lead to the occurrence of the top event (Figure 6b). A failure of the sample subsystem to detect both oxygen or hydrogen concentration affects the failure probability of the make-up system since the operator would not be able to open the valves of the make-up system when required. Operator failure to open the make-up valves, or failure of the valves themselves, leads to failure of the nitrogen make-up valves to open as required. This event, along with the unavailability of nitrogen in the system, leads to the failure of the make-up system to deliver nitrogen to the containment as required. Nitrogen can also become unavailable due to the rupture of the cryogenic make-up tank, a break in the pipes connecting the tank to the containment, freezing or plugging of the pipes, and/or the lack of nitrogen due to unavailability of delivery trucks.

Results of the fault tree analysis indicate that the CAD system has a median probability of failure on demand of $1.6\text{x}10^{-3}$ with a lower bound of $1.6\text{x}10^{-4}$ and an upper bound of $1.6\text{x}10^{-2}$. This means that there exists an approximate 99.8% probability that the CAD system would be able to maintain the hydrogen concentration below the flammability limit for those accident sequences that result in a design basis hydrogen generation rate corresponding to a 1.3% metal-water reaction (approximately 1000 cubic feet hydrogen per hour). For the inerting system (CIS), the results show a median probability of failure on demand of $1.3\text{x}10^{-2}$ with a lower bound of $1\text{x}10^{-3}$ and an upper bound of $1\text{x}10^{-1}$. If the CIS has a redundant nitrogen make-up system, as is the case of the Peachbottom nuclear power plant (Helwig [13]), the mean probability of failure on demand is reduced to $1.04\text{x}10^{-3}$ with an upper bound of $1\text{x}10^{-2}$ and lower bound of $1\text{x}10^{-4}$.

### B.4.3 Final Results: Probability of Post-Accident Hydrogen Control

Using the probabilities calculated in the previous section, the final overall probability that the CAD and the CIS systems are capable of handling a given amount of hydrogen can be assessed. The hydrogen generation rate is discretized into "high", "medium" and "low" categories, with the "high" generation rate corresponding to 180,000 cuft/hr, the "medium" generation rate corresponding to 12,000 cuft/hr, and the "low" hydrogen generation rate to ∿ 1000 cuft/hr (631.5 cuft/hr based on the Vermont Yankee CAD design basis accident). In order to assess the probability that the CAD system can control the hydrogen generated in an accident, a probability of zero is assumed for the "high" generation rates because of the CAD system physical inability to dilute such large amounts of hydrogen.

For "medium" generation rates, the problem can be analyzed from two points of view; first, if it is assumed that the hydrogen is generated in one hour at 12,000 cuft/hr., the concentration will approach the flammability limit so the CAD system will maintain the hydrogen concentration below the flammability limit with a probability of success equal to its availability (0.9984). Secondly, if the hydrogen is produced at a rate of 12,000 cuft/hr over a period longer than one hour, the break point will occur at the maximum injection and venting capacity of the CAD system (2400 cuft/hr). In this case, the probability of controlling the hydrogen from reaching the flammability limit is assumed to be ∿ .2. For "low" generation rates, the CAD system availability of .9984 is used. For the inerting system, probabilities of success of 0.9870 (Pilgrim I) and 0.9989 (Peachbottom) are used for all three hydrogen generation categories as it is assumed that the hydrogen could not burn in an inerted atmosphere under any conditions.

The final failure probabilities for the CAD system to prevent hydrogen flammability over the range of theoretically possible hydrogen generation rates are based on the Vermont Yankee CAD system design:

$$P_f\ (S/A)_{CAD} = 1 - 0.917 \quad = 8.26\text{x}10^{-2}/\text{demand} \tag{6}$$

to

$$P_f(S/A)_{CAD} = 1 - 0.989 \quad = 1.06\text{x}10^{-2}/\text{demand} \tag{7}$$

For the CIS system, the final failure probabilities are, for Pilgrim 1:

$$P_f(S/A)_{CIS} = 1 - 0.987 \quad = 1.3\text{x}10^{-2}/\text{demand} \tag{8}$$

and, for Peachbottom:

$$P_f(S/A)_{CIS} = 1 - 0.998 \quad = 2.0\,\text{x}10^{-3}/\text{demand} \tag{9}$$

These results indicate that both systems have approximately the same overall probabilities of controlling hydrogen generated during reactor accidents. Assuming that the "low" hydrogen generation rates have higher probabilities of occurrence, both systems depend on the reliability of the system design. When comparing the probability of success of the Vermont Yankee air dilution system with the inerting system of Pilgrim 1 for "low" hydrogen generation rates, the CAD is more reliable than the CIS (Table III). When the CAD is compared with the CIS of Peachbottom, which has a redundant nitrogen make-up subsystem, both systems have approximately the same overall hydrogen control probability.

## Table III

## PROBABILITIES OF POST-ACCIDENT HYDROGEN CONTROL

| HYDROGEN PRODUCTION RATE | PROBABILITY OF ACCIDENT P(A) (per reactor-yr) | WEIGHTING FUNCTION OF P(A) | ASSUMED HYDROGEN PRODUCTION RATE (cubic. feet per hr) | PROBABILITY SUCCESS CAD SYSTEM P(S) (per design demand) |
|---|---|---|---|---|
| "HIGH" | $3x10^{-5}$ | 0.00901 | 180,000 | 0.00 |
| "MEDIUM" | $3x10^{-4}$ | 0.09009 | 12,000 | 0.199 - 0.9984 |
| "LOW" | $3x10^{-3}$ | 0.90090 | 631.5 | 0.9984 |

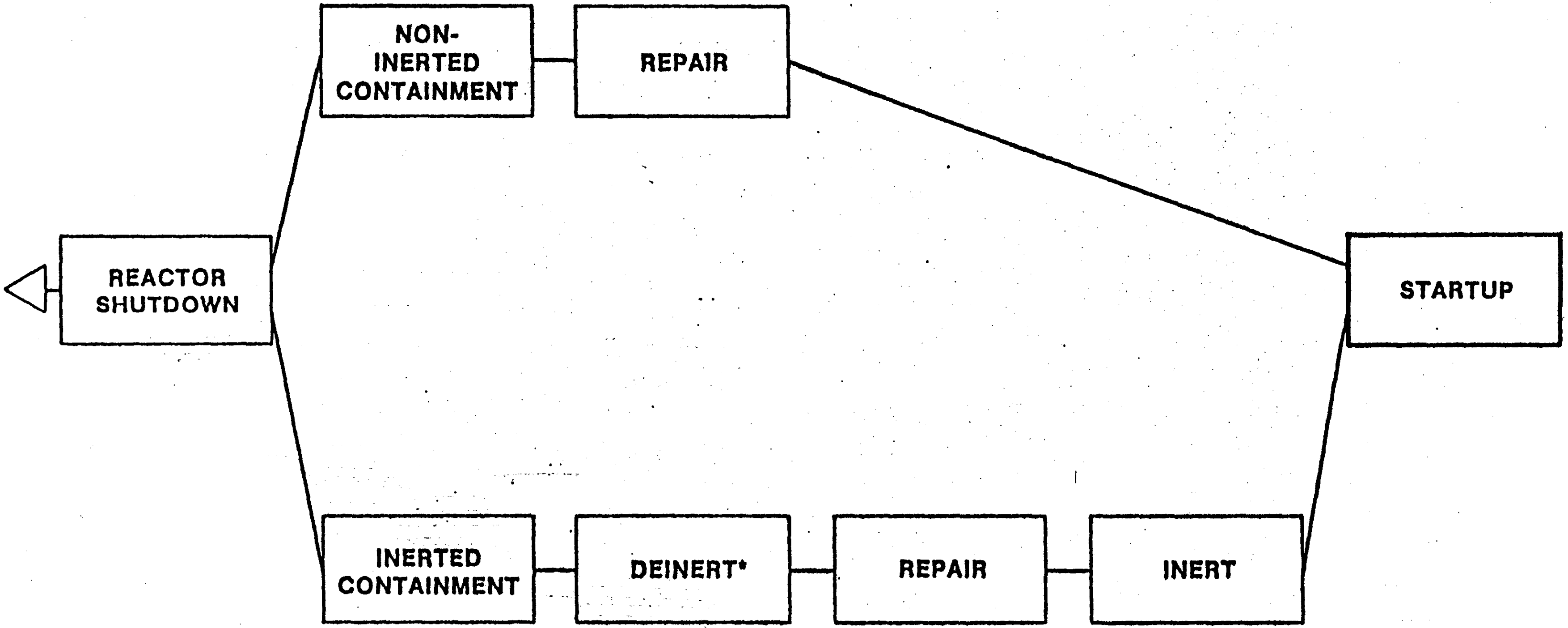
| | CIS PILGRIM I P(S) (per design demand) | CIS PEACH BOTTOM P(S) (per design demand) | CAD SYSTEM P(S\|A) (per accident) | CIS PILGRIM I P(S\|A) (per accident) | CIS PEACH BOTTOM P(S\|A) (per accident) |
|---|---|---|---|---|---|
| H - | 0.9870 | 0.9989 | 0.00 | 0.00889 | 0.0090 |
| M - | 0.9870 | 0.9989 | 0.0179-0.0899 | 0.08892 | 0.0899 |
| L - | 0.9870 | 0.9989 | 0.89946 | 0.88919 | 0.8999 |
| | | | 0.9174-0.9894 | 0.9870 | 0.9988 |

Note: $P(S|A) = \frac{P(S)_i \times P(A)_i}{\Sigma P(A)_i}$

For medium generation rates, the CAD system can be compared with the CIS in the same way as for the low case. For low probability accidents with high hydrogen generation rates, the CAD system cannot prevent hydrogen deflagration, although it can increase times to detonation. Inerting can control larger amounts of hydrogen due to maintaining oxygen concentration below five volume percent. However, the inerting system is not in operation 24 hours prior to shutdown and after startup; during this period, the containment is not protected against hydrogen generation reducing the overall probability per reactor-year of hydrogen control.

## B.5 Impact of Containment Inerting on Reactor Safety

Inerting can affect operational procedures with regard to correcting leakage inside the primary containment, thus impacting upon the probability of various accident initiating events and increasing the number of unscheduled shutdowns. During normal operation, the drywell is monitored by the control room. Symptoms requiring immediate and subsequent corrective actions can thus be identified (Figure 7). The major symptom of a developing problem is an increase in the primary coolant system leakage rate. Such leaks are annunciated in the control room through several monitoring systems, including the drywell unit cooler annunciators, drywell air cooler high drain flow, and radiation leak detectors. Changes in drywell humidity and/or significant changes in pressure, along with



*Deinerting can be done 24 hours before shutdown but the drywell entry has to be performed after shutdown

Figure 7. Leaks from Primary Coolant System in Drywell: Operator Procedures in Inerted and Non-Inerted Containments.

excessive sump pump operation can also indicate the evolution of such a problem (Boston Edison [14]; Vermont Yankee [15]). In order to control leakage, operator actions must be initiated such as monitoring the reactor vessel power, pressure and water level, referring to the pipe break procedure if appropriate, monitoring the drywell floor and equipment sump readings, and determining the location of the leak. When the total unidentified leakage reaches 5 gpm or the identified leakage reaches 25 gpm, technical specifications require the operators to shutdown the reactor (Vermont Yankee [16]; Boston Edison [17]).

In the non-inerted case, drywell entries at power can take place if the power level is sufficiently reduced to between 50-70% full power. Entry can take place without recourse to the use of bulky breathing apparatus. Inspection permits the operators to determine the seriousness of the problem aiding them in their decision as to whether to continue operation or to shut down to make major repairs. The option to make inspections in the drywell during operation can potentially reduce the number of plant shutdowns, reducing the stress placed on the system that occurs with shutdown and the probability of failure of the decay heat removal system. Also, in those cases where shutdown occurs, unnecessary delays in startup can be avoided since inerting is not required.

During inerted containment operation, drywell entries at power are not permitted by industry practice because of the excessive danger such entry would represent to plant personnel. Leakage identification is therefore made more difficult. Technical specifications require that the operator insure that drywell fans are operating at all times, and that the torus temperature is below 80°F. The torus spray system is initiated if torus pressure should exceed 175 psig as is venting of the primary containment through the standby gas treatment system (Boston Edison [14]). Entry usually requires that the containment be purged until the oxygen concentration reaches 20 volume percent, which usually requires 24 hours.

### B.5.1 Analysis of Drywell Entries at Power

In order to evaluate the safety aspects involved in the location, evaluation and isolation of primary system leakage inside the drywell, it is necessary to know the circumstances under which an entry is made and its effects on the overall safety of the plant. Entries have been made under four different circumstances: (i) entries to perform preventive maintenance during scheduled shutdown, (ii) emergency situations wherein the reactor is shutdown due to malfunction of equipment inside the drywell, (iii) entries during an unscheduled shutdown for inspection purposes, and (iv) entries after reduction of power as a consequence of monitoring a malfunction inside the drywell that does not require an immediate shutdown (Thomas [18]). The last three types of entries are affected by containment inerting. For example, in an emergency situation requiring an immediate shutdown, entry could be delayed three to ten hours because of the need to deinert the containment.

Entries to the drywell have been made at Vermont Yankee at low power to investigate bonnet leaks in the recirculation valves, and for inspection of the recirculation pumps to check possible water-to-oil cavity leaks. During these entries, other malfunctions, such as loose belts, stuck valves and fan failures were discovered and the problems solved before resuming full-power operation (Vermont Yankee [15]). Entry data was used as a way to conservatively estimate the leakage rate, which can translate into estimates on the probability of breaks in the recirculation system (Table IV). Where data was not available, WASH-1400 failure data was used. The sequence of events that can lead to loss-of-coolant from the recirculation system is shown in Figure 8.

Using the failure rates of Table IV, the fault tree of Figure 8 was quantified to estimate the contribution of valve leakage to the initiation of a small to medium size LOCA. From Vermont Yankee drywell entry data, the probability of valve rupture varies between $10^{-8}$ and $10^{-7}$/hr. Uncertainty in the data implies an overall uncertainty of ± 10. From WASH-1400 failure data, the same probability is $4x10^{-8}$/hr. The contribution from circumferential break, feedwater line break and steam line break is approximately $3x10^{-9}$/hr. The analysis indicates a possible reduction in the LOCA initiation rate of approximately one order of magnitude from $6x10^{-8}$/hr to $6x10^{-9}$/hr. This reduction could theoretically be achieved by following the Vermont Yankee operating procedures for citing and correcting problems accessible to drywell entries at power.

### B.5.2 Effects of Additional Shutdowns on Overall BWR Accident Risk

The possibility that inerting may increase the number of unscheduled shutdowns can impact upon the overall BWR accident risk by affecting the probability of failure per reactor year of core melt due to increases in demands upon the heat removal system. The decay heat removal system is required to operate to prevent core melt after a reactor shutdown. WASH-1400

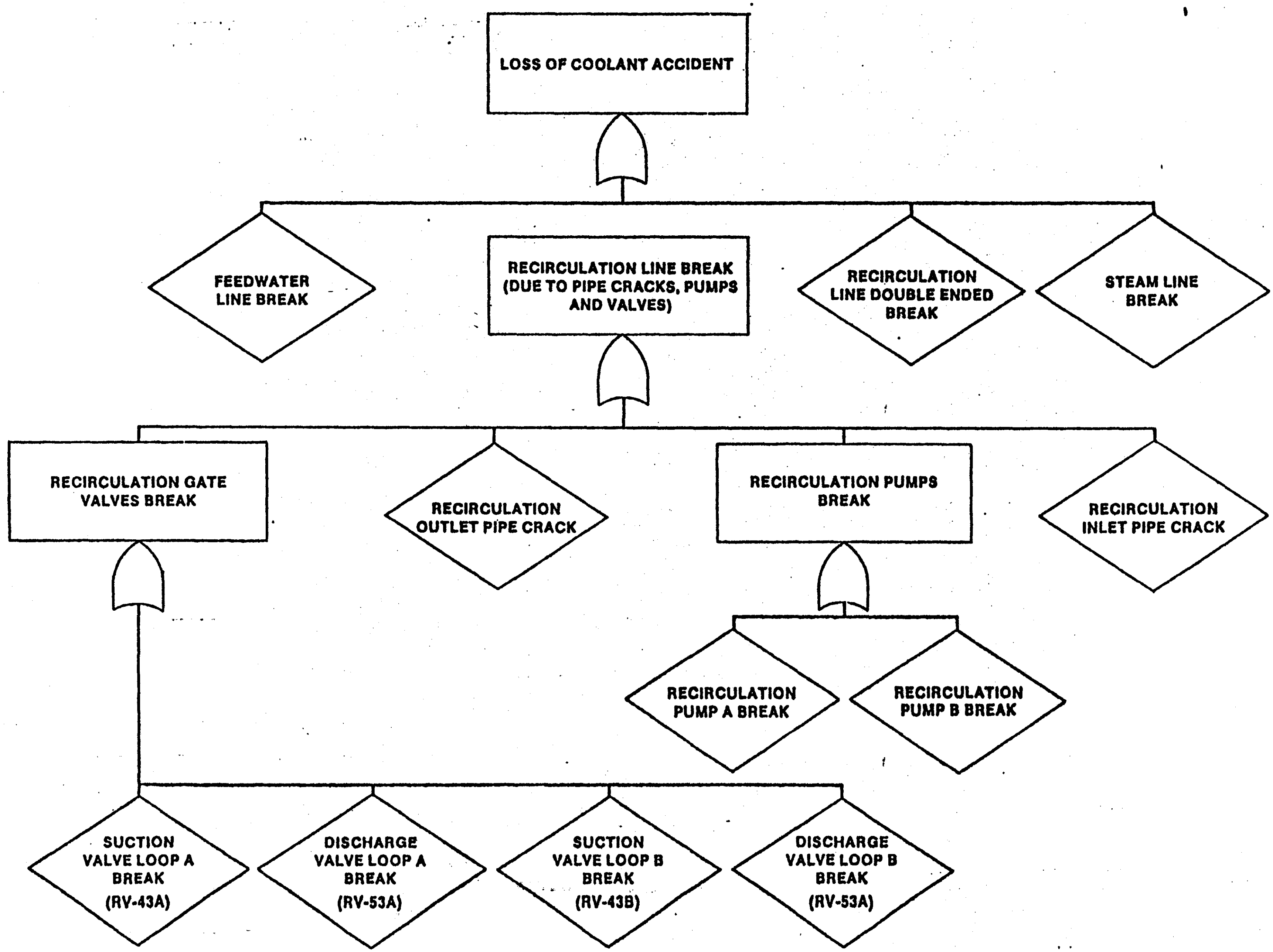

LOSS OF COOLANT ACCIDENT
FEEDWATER LINE BREAK
RECIRCULATION LINE BREAK (DUE TO PIPE CRACKS, PUMPS AND VALVES)
RECIRCULATION LINE DOUBLE ENDED BREAK
STEAM LINE BREAK
RECIRCULATION GATE VALVES BREAK
RECIRCULATION OUTLET PIPE CRACK
RECIRCULATION PUMPS BREAK
RECIRCULATION INLET PIPE CRACK
RECIRCULATION PUMP A BREAK
RECIRCULATION PUMP B BREAK
SUCTION VALVE LOOP A BREAK (RV-43A)
DISCHARGE VALVE LOOP A BREAK (RV-53A)
SUCTION VALVE LOOP B BREAK (RV-43B)
DISCHARGE VALVE LOOP B BREAK (RV-53A)

Figure 8 Fault Tree for LOCA Initiating Events.

Table IV

LEAKAGE FAILURE RATES FOR VALVES OF THE RECIRCULATION SYSTEM
(65 months period)

| VALVE | LEAKAGE FAILURE RATE (leak increase/hour) | |
|---|---|---|
| RV-43A | $1.07x10^{-4}$ | * |
| RV 53A | $2.13x10^{-5}$ | * |
| RV-43B | $6.41x10^{-5}$ | * |
| RV-53B | $1.00x10^{-8}$ | ⊕ |

* Data from drywell entries at Vermont Yankee nuclear power station.

⊕ Data from WASH-1400.

showed that this condition is included in the transient events that dominate the releases in almost all the BWR risk categories. The probability of failure of the decay heat removal system was determined in WASH-1400 to be $\sim 1.6 \times 10^{-6}$/r-yr, which can be combined with the number of total shutdowns. The difference between the number of shutdowns in a BWR operating with a CAD system and the number of shutdowns in a BWR operating with an inerted containment will directly affect the transient events that are dominant in BWR accident sequences. To determine this number, it is necessary to investigate the operational histories of BWR inerted containment shutdowns that could have been avoided if the containment had not been inerted. For example, about three unscheduled shutdowns per year can be expected in a BWR with an inerted containment with a range of 1 to 6 per year (Table V).

Combining the probability of failure of the decay heat removal system with the three transients per reactor year yields $4.8 \times 10^{-6}$/r-yr for the sequence (Table VI). A reduction in probability of this sequence directly affects the overall BWR accident risk. According to WASH-1400, the unavailability of the decay heat removal system is responsible for ∿64.5% of the total risk. A recent EPRI study indicates that the decay heat removal system is responsible for ∿83% of the total risk (EPRI [19]). Also, recent studies by Buhl [20] and Bernero [21] show that transient events and their consequences remain essentially unaffected by use of non-inerted containments.

## Table V

### COMPARISON OF EXPERIENCE:INERTED BWRs VS. NON-INERTED BWRs*

| Plant Name | Avg. No. of unscheduled entries/yr | % of entries resulting in plant shutdown for repair | # shutdowns/yr | Plants normally operated with small leakage | Entries normally performed with plant inerted |
|---|---|---|---|---|---|
| Hatch, Unit 1 | 5 | 64 | 3.2 | Yes | No |
| Cooper | 1 | 100 | 1 | Yes | No |
| Nine Mile Point, Unit 1 | 3 | 92 | 2.8 | Yes | No |
| Brunswick, Unit 1 | 6 | 70 | 4.2 | Yes | No |
| FitzPatrick | 2 | 100 | 2 | Yes | No |
| Quad Cities, Unit 1 | 4 | 54 | 2 | Yes | No |
| Quad Cities, Unit 2 | 2 | 43 | 1 | Yes | No |
| Peach Bottom, Unit 2 | 3 | ? | 3 | Yes | No |
| Peach Bottom, Unit 3 | 4 | ? | 4 | Yes | No |
| Monticello | 2 | 100 | 2 | Yes | No |
| Pilgrim | 3 | 100 | 3 | Yes | No |
| Dresden, Unit 2 | 3 | 90 | 2.7 | Yes | No |
| Dresden, Unit 3 | 2 | 90 | 1.8 | Yes | No |
| Duane Arnold | 2 | 100 | 2 | Yes | No |
| Browns Ferry, Unit 1 | 3 | ? | 3 | Yes | No |
| Browns Ferry, Unit 2 | 1 | ? | 1 | Yes | No |
| Browns Ferry, Unit 3 | 4 | ? | 4 | Yes | No |
| Vermont Yankee | 4 | 20 | .8 | Yes | N/A |
| Hatch, Unit 2 | 9 | 100 | 9 | Yes | N/A |

* From NRC staff position (Butler, 1980).

Table VI

DECAY HEAT REMOVAL SYSTEM PROBABILITY PER NUMBER OF REACTOR SHUTDOWNS IN A YEAR

| NUMBER OF REACTOR SHUTDOWNS | PROBABILITY/REACTOR-YEAR DECAY HEAT REMOVAL SYSTEM |
|---|---|
| 1 | $1.6x10^{-6}$ |
| 2 | $3.2x10^{-6}$ |
| 3 | $4.8x10^{-6}$ |
| 4 | $6.4x10^{-6}$ |
| 5 | $8.0x10^{-6}$ |
| 6 | $9.6x10^{-6}$ |
| 7 | $1.1x10^{-5}$ |
| 8 | $1.3x10^{-5}$ |
| 9 | $1.4x10^{-5}$ |
| 10 | $1.6x10^{-5}$ |

### B.5.3 Other Considerations

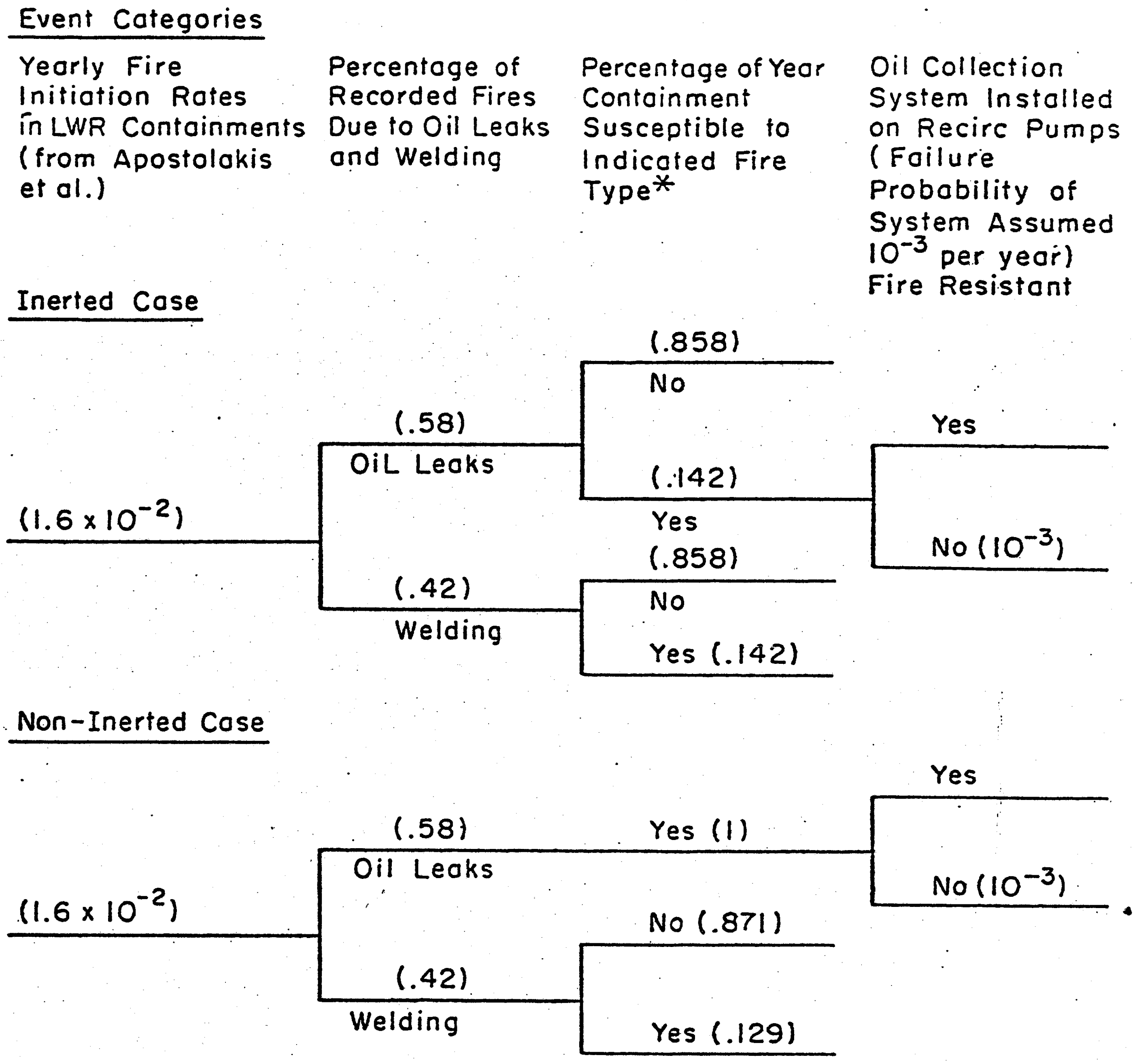
Two other considerations related to inerting were identified as having potential benefits: (1) reducing the corrosion rates of the torus vessel and the termination boxes of the electrical outlets found in the torus, and (2) reducing the likelihood of fires inside the drywell. Reduced corrosion in the torus at the Pilgrim I and Millstone BWR plants has been observed (Musolf [20]; Rosen [21]). This effect has been attributed to the reduction in the oxygen content in the torus atmosphere due to inerting. However, a quantitative comparison of corrosion effects between non-inerted and inerted BWRs has not been made. One safety impact torus corrosion may have is in producing debris that could clog screens on the ECCS system; however, only large corrosion rates could produce the size of debris particle that might pose such a problem. Other utilities have not observed reduced corrosion effects indicating that the protective painted coating on the torus surface protects sufficiently against major corrosion problems, and therefore that the potential advantage of inerting due to corrosion is not significant (Northeast Utilities [22]).

Reduction of fires in the BWR primary containment compartment was identified as being a significant potential benefit of inerting (Rosen [21]). Two sources of combustible material reside inside the primary containment (Holtzclaw [23]; Sawyer [24]): (i) the reactor recirculation pump fuel oil (50 gallons in each of the two pumps found on the primary coolant loop), and (ii) the electrical cable, which is fire resistant but can ignite at high temperatures. A fire inside the containment can be initiated three ways: (i) oil leak from the recirculation pump during operation, (ii) during shutdown and maintenance a welding related oil fire, and (iii) electrical motor pump fire. All of these events relate to the recirculation pump; cases (i) and (ii) can potentially lead to a major fire where the electrical cabling would also be affected; in case (iii), the fire would be confined to the pump and would result in pump failure. The last case would not be a significant problem since adequate cooling can be maintained by either of the recirculation pumps; in the event of a simultaneous failure of both pumps, the BWR can be sufficiently cooled by natural recirculation (Holtzclaw [23]).

The worst possible scenario involving a fire in the primary containment would be a loss of both recirculation pumps as a result of an oil leak for one pump igniting a fire spreading to the electrical cables, then igniting the second recirculation pump oil supply. In this scenario, both pumps would be made inoperative requiring auxiliary cooling systems to ensure adequate cooling. Loss of primary coolant would not be expected.

Although a fire in the drywell would result in an additional unscheduled shutdown, the estimated fire occurrence probability of $1.6\times10^{-2}$-$10^{-3}$ per reactor-year (Apostolakis and Kazarians [25]; U.S.N.R.C. [12]) indicates that the impact on the total number of expected unplanned shutdowns (2-6 per reactor-year) is negligible. Moreover, since auxiliary coolant system components are located exterior to the primary containment, a drywell fire would not likely lead to a failure of the residual heat removal system because active components are located exterior to the drywell.

An event tree (Figure 9) was constructed to estimate the significant fire initiation rate on an hourly basis for comparison with the hourly LOCA initiation rate estimated earlier for the inerted and non-inerted cases ($6\times10^{-8}$/hr inerted; $6\times10^{-9}$/hr non-inerted). The effect on the fire initiation rate of an oil spill collection system installed on each of the two primary system recirculation pumps was also estimated (Table VII). With the addition of an oil leak collection system, the estimates of the fire initiation rate drops from $1\times10^{-6}$/hr to $1\times10^{-7}$/hr in the non-inerted case, compared with a range of $3\times10^{-7}$/hr to $1.0\times10^{-7}$/hr in the inerted case (see Table VII). If no oil spill collection system is installed in the non-inerted case, the fire initiation rate is ∿ 5 times greater than for the inerted case. The installation of the collection system causes the welding initiated fires to dominate such that the difference between the inerted and non-inerted cases is small. Since inerting may result in more unscheduled reactor shutdowns per year, the fire initiation rate may be less for the non-inerted case by a factor of ∿ 1.08 given that oil collection systems are installed in both cases and assuming twice as many unscheduled shutdowns per reactor-year for the inerted case.


Event Categories
Yearly Fire Initiation Rates in LWR Containments (from Apostolakis et al.)
Percentage of Recorded Fires Due to Oil Leaks and Welding
Percentage of Year Containment Susceptible to Indicated Fire Type*
Oil Collection System Installed on Recirc Pumps (Failure Probability of System Assumed 10^-3 per year) Fire Resistant
Inerted Case
(1.6 x 10^-2)
(.58)
OiL Leaks
(.858)
No
(.142)
Yes
Yes
No (10^-3)
(.42)
Welding
(.858)
No
Yes (.142)
Non-Inerted Case
(1.6 x 10^-2)
(.58)
Oil Leaks
Yes (1)
Yes
No (10^-3)
(.42)
Welding
No (.871)
Yes (.129)

* For the inerted case, the containment is only susceptible to fires of any type during periods of shutdown; likewise, for the non-inerted case in the welding event sequence. The percentages were calculated assuming 6 weeks for annual refueling added to the number of unscheduled shutdowns per year (assumed 4 per year for inerting, 2 per year for non-inerting).

Figure 9 Event Tree for Fires Initiated Inside BWR Drywell Containment Structures.

Table VII

SERIOUS FIRE INITIATION RATE PER HOUR IN A BWR DRYWELL
(WITH/WITHOUT OIL LEAK COLLECTION SYSTEM ON RECIRCULATION PUMPS)

| Fire Initiation Event | Inerted | | Non-Inerted | |
|---|---|---|---|---|
| | With | Without | With | Without |
| Welding | $1.09 \times 10^{-7}$ | | $9.89 \times 10^{-8}$ | |
| Oil Leak | $1.5 \times 10^{-10}$ | $1.5 \times 10^{-7}$ | $1.06 \times 10^{-9}$ | $1.06 \times 10^{-6}$ |
| Total | $1.09 \times 10^{-7}$ | $2.59 \times 10^{-7}$ | $1.01 \times 10^{-7}$ | $1.16 \times 10^{-6}$ |

## B.6 Discussion and Summary

Results of the probabilistic risk assessment indicate that the inerting and air dilution systems have approximately the same overall probability of post-accident hydrogen control. Results indicate that both systems render approximately the same overall hydrogen control probability (air dilution: .917-.989; nitrogen inerting: .987-.998). Drywell entries and unscheduled shutdowns were also analyzed to determine the impact on the overall BWR accident risk as it relates to the decay heat removal system. Results indicate that inerting may increase the overall risk due to a possible increase in the number of unscheduled shutdowns due to a lessened operator ability to correctly identify leakage in the primary coolant system. A reduction in the LOCA hourly initiation rate of an order of magnitude from $6x10^{-8}$/hr in the inerted case to $6x10^{-9}$/hr in the non-inerted case was estimated in the non-inerted case due to increased operator ability to inspect and correct possible LOCA initiation events.

Possible effects of inerting on torus vessel corrosion rates and drywell fires were also examined. Reduced corrosion due to inerting is thought not to be a significant problem due to the minor positive effect inerting has on such corrosion and the large degree of corrosion that would be required to impact significantly on safety. A probabilistic estimation of the effect of inerting on the drywell fire initiation rate showed that, with the installation of oil leak collection systems on the recirculation pumps, the hourly fire initiation rate is dominated by the contribution due to welding during shutdown based on experience to date. Since inerting may result in more unscheduled shutdowns per year, the fire initiation rate may be less for the non-inerted case by a factor of ∿ 1.08 given oil collection systems are installed in both the inerted and non-inerted cases, and assuming twice as many unscheduled shutdowns per year for the inerted case. It is therefore recommended that alternative hydrogen control systems to inerting be investigated and that these studies be undertaken in conjunction with other class 9 accident mitigation questions.

## III.C The Issue of Hydrogen Control in PWRs

### C.1 Summary of Study Results

Events at Three Mile Island related to hydrogen production and deflagration during the post-accident time sequence have led to a re-examination of the models used for predicting pressure response from non-condensible gases. In this paper, existing literature on hydrogen burns and explosions is review and summarized. Additionally, original models for calculating the pressure increase in containment due to hydrogen burns and/or explosions are derived and demonstrated. These models present a more in-depth treatment of physical phenomenon than exists at the present time, and are being integrated into existing codes for calculation of the containment pressure history in the event of a class 9 accident. Also, a brief comparison of hydrogen control systems for PWR containments is made.

### C.2 Introduction

The accident at Three Mile Island has emphasized many aspects of nuclear safety previously underestimated. One of these aspects relates to the production of hydrogen during a reactor accident and its subsequent behavior in containment. At Three Mile Island, it has been estimated that fifty to seventy percent of the fuel cladding underwent a metal-water reaction with an associated large production of hydrogen [1]. During the accident, it was feared that the hydrogen bubble formed at the head of the reactor vessel would explode causing a large release of radiation to containment, possibly leading to failure of the containment. This fear was later shown to be unfounded because the only oxygen present was due to radiolysis of the coolant and was not significant enough to permit a hydrogen explosion in the reactor head [2]. Some of the hydrogen produced escaped from the reactor vessel, presumably through the stuck-open pressure relief valve, and collected in the containment. Nine hours into the accident, a pressure pulse of 28 psia was recorded at a number of recording stations around the containment [3]. It was later deduced that the pulse was due to a hydrogen explosion, but as was noted by the operators in later testimony, the pulse was unexplained at the time [4].

Because of the experience at Three Mile Island, greater emphasis has been placed on the hydrogen problem as it relates to possible burns and explosions in containment that could lead to containment failure due to overpressurization with subsequent release of radiation to the environment [5]. In order to develop regulatory guidelines and/or possible plant design changes, it is imperative that the magnitude and behavior of pressure pulses and spikes due to hydrogen burns and explosions be investigated. This paper reviews the existing literature related to hydrogen burns, explosions and production mechanisms, and then proceeds to describe models of pressure response due to hydrogen deflagration and detonation.

## C.3 Hydrogen Burns and Explosions

Hydrogen burning may be initiated when the limits of flammability are reached — four percent hydrogen and five percent oxygen by volume. In a standard air mixture, the maximum hydrogen concentration that will support a burn is 76 volume percent. Burning can be maintained if the gas mixture falls below the flammability limits if the mixture is within those limits when the burn was initiated. Similarly, an explosion can only be sustained within the detonation limits. In this paper, "burn" refers to a relatively slow rate of reaction (∿2m/sec) while "explode" refers to a very fast rate of reaction (∿1000 m/sec) [6 ]:

$$H_2 + 1/2\ O_2 \rightarrow H_2O + \text{energy} \qquad (1)$$

The lower detonation limit falls between 18 to 22 volume percent hydrogen while the upper limit falls between 45 to 65 volume percent hydrogen, corresponding to an oxygen concentration of nine to twelve volume percent respectively (Figure 1). Burning leads to a slow increase in gas temperature and pressure, while in explosions the energy generation rate is so great that the reaction energy is imparted as kinetic energy to the product molecules which than slam into the walls of the containment vessel. The change in momentum, or impulse, is what creates a pressure spike at the containment surface.

### C.3.1 Review of Existing Literature

Hydrogen combustion can vary from separated flames that propagate upward, to coherent flames that propagate uniformly in all directions at subsonic velocities, to supersonic detonation waves [7]. Deflagration, or simple burning, can produce effects similar to those of explosions. Deflagration occurs as a chain reaction in which the principal carriers are the free radicals H, O, and OH. Ignition occurs in a hydrogen-oxygen mixture when the rate of production of the chain carriers exceeds the rate of their destruction [8]. Ignition can occur from sparks from electrical equipment or discharged accumulated static, or by temperature increases. Sparks can ignite a mixture below the flammability limit but the flames produced are not self-propagating and are extinguished when the source of

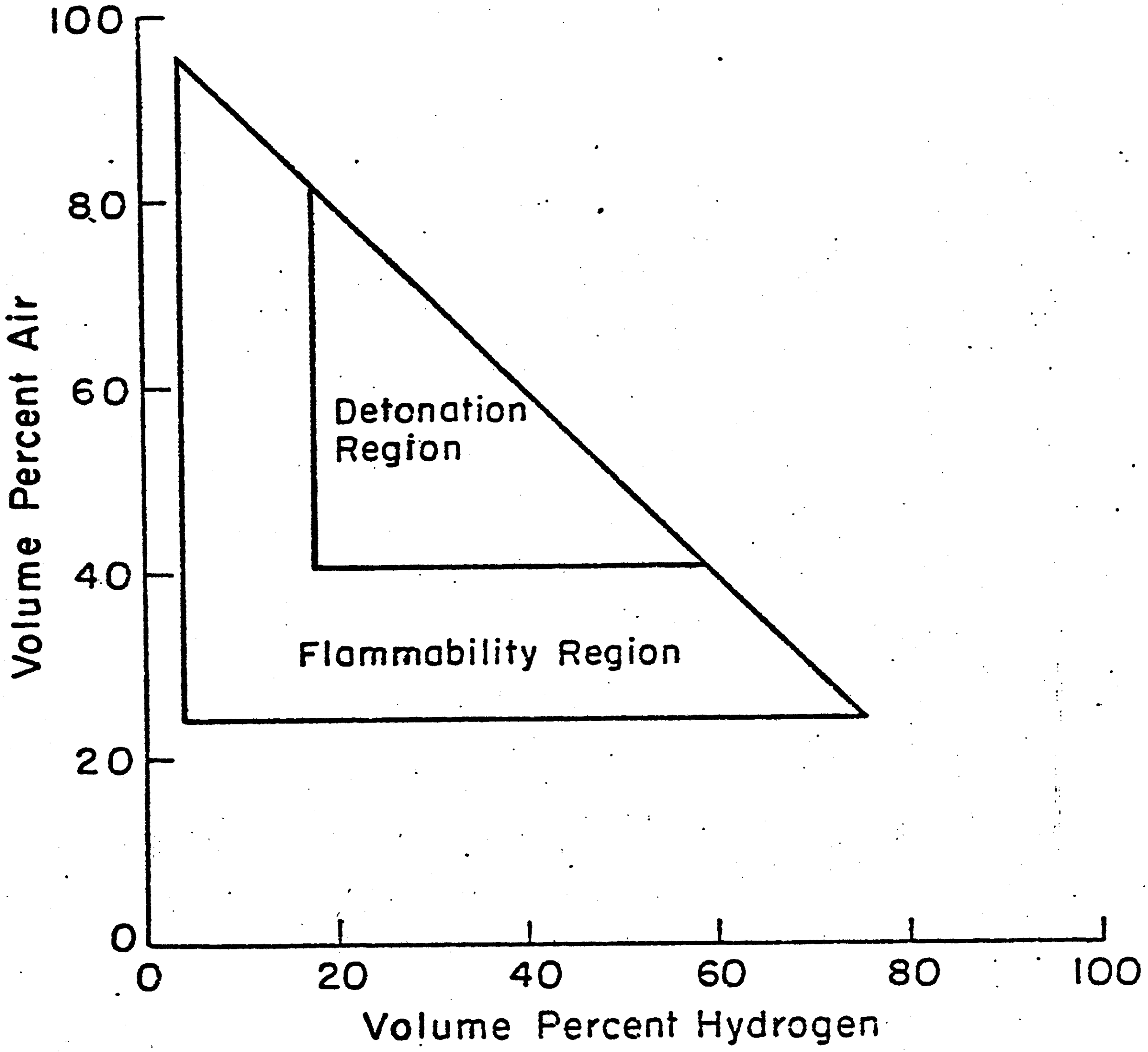


Figure 1 Approximate Flammability and Detonation Limits of Air and Hydrogen

ignition is removed. The spontaneous ignition temperture of a hydrogen-air mixture is 585°C although below this temperature, a self-propagating flame can be produced in a four volume percent mixture [9].

The flame propagates at a velocity dependent upon its direction resulting from the tendency of the burned gas to rise, and from the hydrogen concentration. Mixtures with compositions close to the flammability limit will not burn all of the available hydrogen. As the proportion of hydrogen in the mixture increases, greater amounts of hydrogen are burned. For example, only half of the hydrogen in a 5.6 volume percent mixture will burn. Combustion will not be complete until the percentage of hydrogen is increased to 10 percent or more.

Detonation is a rapid and violent process characterized by a chemically supported shock wave. The velocity of wave propagation is the same as the velocity of sound in the burning mixture [8]. The destructiveness of a detonation is due primarily to the destruction of the shock front, Shapiro and Moffette [9] show hydrogen detonation limits to occur between 19 and 45 volume percent; hydrogen concentrations within this range will not necessarily detonate. Experiments have shown that a detonation is more likely to occur in smaller tubes rather than larger ones, and that a detonation wave can be converted to that of normal combustion by suddenly widening the tube. A strong initiating source is also required to produce detonation. The use of flames or sparks does not produce detonation.

Experiments were conducted at General Electric [7] to determine the pressure and temperature responses from hydrogen burning. The experiments were carried out in a 134 cubic foot vessel, varying the hydrogen concentration, type of ignition source used, location of the igniation of the burn, and the initial atmosphere pressure, temperature and water vapor content. In all cases, the experimental results were lower than the theoretical predictions. The model used to predict the responses is the same as that given in this paper, using slightly different constants.

The rate of reaction of a bimolecular reaction can be given by

$$\text{rate } \alpha (\text{rate of collision}) \times (\text{number of molecules with energy} \geq E)$$

$$\alpha T^{1/2} e^{-E/kT} \qquad (2)$$

where E = activation energy of the reacti on

k = Boltzmann's constant

T = gas temperature.

In thermal explosions, ignition is defined as occurring when the heat generation rate is greater than, or equal to the heat absorption rate:

$$\text{heat generation rate } \alpha T^{1/2} e^{-E/kT} \text{volume } D^j$$

$$\text{heat absorption rate } \alpha (T-T_o) \text{surface area} \qquad (3)$$

where D is the density of the gas, $T_o$ is the temperature of the surface of the vessel, and $j$ is the order of the reaction. If at a given temperature the heat temperature rate is greater than the heat absorption for all temperatures, then as time progresses, the temperature will increase, increasing the rate of reaction, and the rate of temperature increase. This is an explosion. If, however, the energy generated is less than the energy absorbed, the temperature of the gas decreases, lowering the rate of reaction, and an explosion is impossible to sustain. The minimum temperature that will support detonation, $T_{ignition}$, is where heat generated = heat absorbed and d/dT heat generation rate = d/dT heat absorption rate. To first order, $T_{ignition} - T_o \sim kT_o^2/E$ [10].

Strehlow [11] defined five basic types of combustion:

(i) Vessel Explosions, or Well-Stirred Reactor reactions: these may be initiated by adiabatic compression, or by adiabatic, but not isentropic compression by a travelling shock wave;

(ii) Diffusion Flames: these occur in continuous flow chambers, with three physical distinct regions: unreacted fuel, unreacted oxidizer, and reacted gases. These two types differ from the rest, in that these do not involve wave processes;

(iii) Premixed Gas Flames;

(iv) Detonation: these are shock induced combustion waves. Their propagation is fairly independent of vessel geometry and can be initiated by a flame, spark or shock wave;

(v) Rocket Engine Combustion: this is of importance because of the thrust production involved.

Experiments were done [6, 12] to measure the effects of various parameters on the detonation and flammability limits, and their velocities. These limits and velocities are dependent on the ignition source, geometry of the vessel, and its surface. The velocity is slowere in narrow, rough tubes than in wide, smooth tubes. Beyond a certain roughness and narrowness, the flame is extinguished. The velocity of detonation increases as pressure and temperature are increases. The lower flammability limit increases, and the upper limit decreases with increasing gas temperature. The direction of change in the flammability limits with changing gas pressure depends on the gas involved. The limits widen at both ends by increasing the pressure in a methane-air mixture, narrow at both ends by increasing the pressure in a carbon-monoxide - air mixture, and in a hydrogen - air mixture, the upper limit increases and the lower limit remains the same with increasing pressure.

A trial and error method was developed [13] to predict the final conditions from hydrogen combustion. Five equations, from the mass, momentum and energy conservation, entropy definition, and ideal gas assumption, are solved simultaneously for five unknowns in the reacted gas, subject to the mass balance equations.

The mechanics involved in the combustion of hydrogen are not clearly known. However, certain characteristics stand out. The rate of reaction is slow, increasing slightly with increasing pressure, until $P_1$, the first explosion limit. This limit is inversely proportional to the vessel diameter. Addition of inert gases lowers this limit, possibly by "blocking" the surface, and hindering chain breaking reactions. For pressures in the Explosion Peninsula, between $P_1$ and $P_2$, the second explosion limit, the rate of reaction is infinite, and explosion occurs. The second explosion limit is fairly independent of the surface, and decreases with an increase in the inert gas concentration. At pressures above $P_2$ the rate of reaction is low, and increases with pressure until the third explosion limit $P_3$, where the rate again becomes infinite, and detonations occur.

The actual reactions involved are not agreed upon. One consistent set of reactions is:

$$OH + H_2 \rightarrow H_2O + H \qquad \text{(I)}$$

$$H + O_2 \rightarrow HO + O \qquad \text{(II)}$$

$$O + H_2 \rightarrow OH + H \qquad \text{(III)}$$

$$H + O_2 + M \rightarrow HO_2 + M \qquad \text{(IV)}$$

$$HO_2 + H_2 \rightarrow H_2O_2 + H \qquad \text{(Va)}$$

$$2HO_2 \rightarrow H_2O_2 + O_2 \qquad \text{(Vb)}$$

$$H + O_2 + H_2O_2 \rightarrow H_2O + O_2 + OH \qquad \text{(Vc)}$$

$$HO_2 + H_2O_2 \rightarrow H_2O + O_2 + OH \qquad \text{(Vd)}$$

$$H_2O_2 \rightarrow H_2O + 0.5\ O_2 \qquad \text{(Ve)} \qquad (4)$$

At low pressures, (below the first explosion limit) the reactions occurring are mainly I and III. The rate of reaction follows Arrhenius' Law (rate $\alpha$ $\exp(-E/kT)$) where E is the activation energy, k is Boltzmann's constant, and T is the gas temperature.

As the pressure increases, the rate of reaction of II, an endothermic, chain initiating reaction, increases, until the rate of steam production is infinite. At this point, "Isothermal Branching" is taking place, and the liberation of heat is not important. In the explosion peninsula, the rate of IV, a trimolecular chain breaking reaction starts to become significant with increasing pressure, until the second explosion limit, where it "overtakes" the chain initiating reaction of II, and explosions can no longer be sustained. At pressures above the third explosion limit, the energy released from the combustion cannot diffuse fast enough, and the phenomenon of self heating occurs, which causes an explosive situation [14, 15].

### C.3.2 Production Mechanisms

The production of hydrogen during the course of an accident presents two potential threats to containment integrity; first, by increasing the internal gas pressure in the system and secondly, by burning or exploding when combined with the oxygen present in the containment atmosphere. The additional thermal energy produced in the burning or detonation of the hydrogen raises the pressure inside the containment and eventually can result in containment failure by overpressurization [6].

Hydrogen can be produced during the course of a reactor accident through high temperature metal-water reactions between fuel cladding and reactor coolant, radiolytic decomposition of water, and corrosion of metals by solutions used for emergency cooling or containment sprays. The main source of hydrogen from metal-water reactions is produced through the high temperature zircalloy-water and steel-water reactions. These reactions take place according to the following relations:

$$Zr + 2H_2O \rightarrow ZrO_2 + 2H_2 + \text{heat} \qquad (5)$$

$$Fe(\text{steel}) + xH_2O \rightarrow Fe(\text{steel})\text{ oxides} + xH_2 + \text{heat} \qquad (6)$$

The initial source of hydrogen in a meltdown is produced in the reaction of Eqn. (2) and occurs when steam from water in the pressure vessel contacts overheated zircalloy fuel cladding. It has been estimated that the rate of consumption of zircalloy is about 10 percent per 1000 seconds. Figure 2 plots zircalloy consumption as a function of time derived from a comparison of BWR core heatup calculations [17]. Assuming a conservative constant consumption rate, all zircalloy would be consumed in less than three hours and could result in a 72% hydrogen containment concentration. Given that

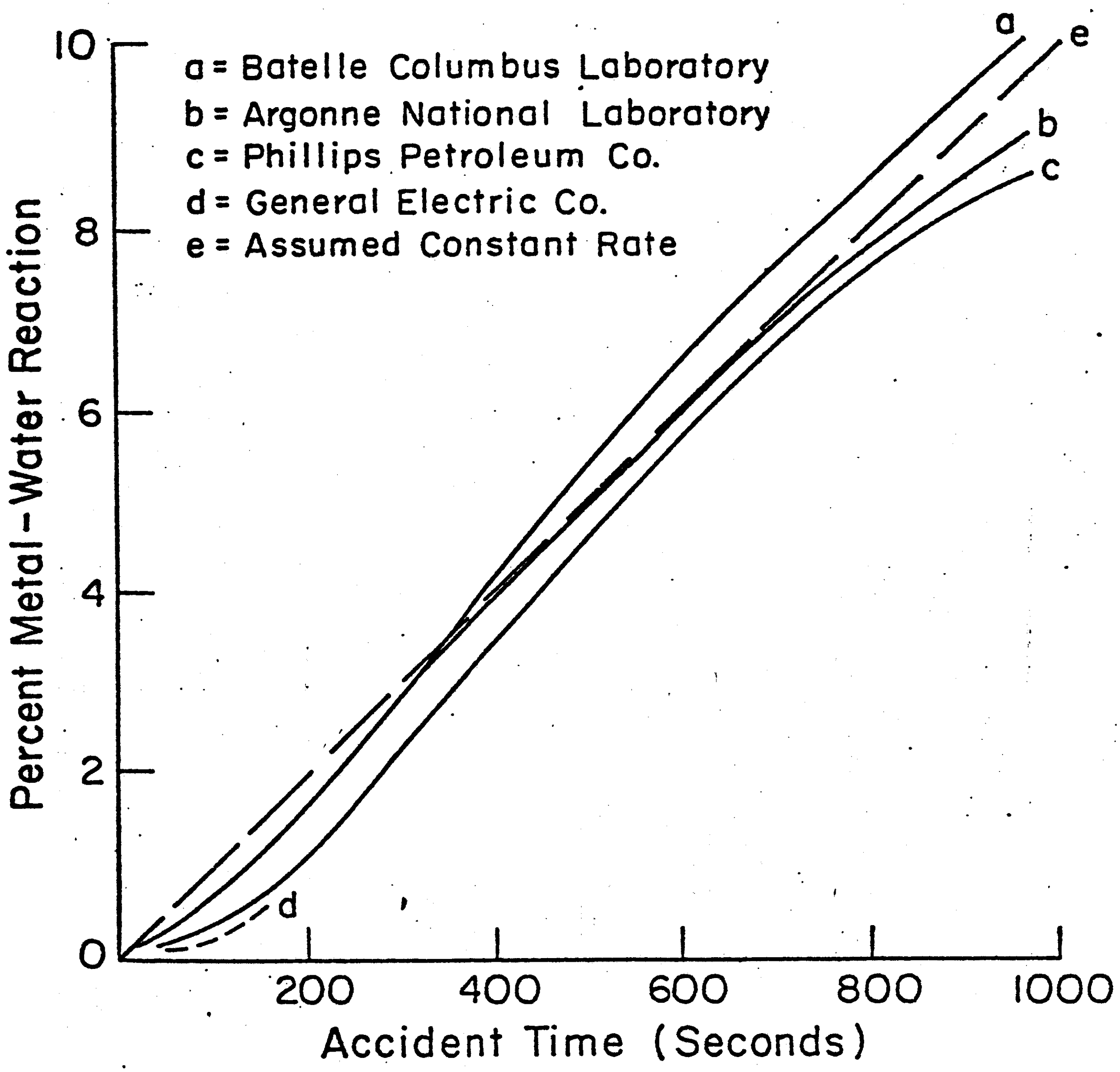


Figure 2  Percent Metal-Water Reaction vs Accident Time

the amount of steam decreases with time, the rate of zircalloy consumption will be lower but using a conservative approach, an upper bound for the consumption rate can be assessed.

Steel-water reactions (eqn. (3)) could generate massive amounts of hydrogen. However, experimental studies indicate that iron or steel must be nearly molten before appreciable reaction with steam occurs. Contact between large amounts of molten steel and water might cause steam explosions before the reaction could generate hydrogen.

The radiolytic decomposition of water is a delayed but potentially significant source of hydrogen. Beta or gamma radiation can cause ionization and subsequent decomposition of water molecules resulting in hydrogen. However, the production of large amounts of hydrogen in an accident would require that high radiation doses be applied to large volumes of water; for example, in the range of $10^8$ to $10^9$ rads applied to the entire water supply of the reactor. Since it would require several days or weeks to accumulate such exposures, this source of hydrogen is considered a long term rather than an immediate problem.

## C.4 Pressure Response Models

Three models were developed to calculate the pressure rise in containment due to a hydrogen burn or explosion. These models are discussed below and results of calculations shown.

### C.4.1 Hydrogen Burn Model

To calculate the pressure rise due to hydrogen burning, a number of assumptions were made: (i) the model disregards the flammability limits such that hydrogen can be burned at concentrations varying between 0 to 100%,

(ii) gases are assumed ideal such that $PV = nkT$ and $\Delta h = C_p(\Delta T)$, (iii) the heat capacity factor $C_p$ is assumed constant for each gas and (iv) the volume percent of any constituent gas equals the number of moles of the gas divided by the total number of moles. Also assumed was (v) that the energy released per mole of hydrogen consumed is independent of the initial temperature, pressure and gas composition and (vi) none of the energy released is dissipated to the surrounding structures or the water on the vessel floor. This is very conservative. Another assumption made was that (vii) the burning would be slow on the order of several meters/second. Since it is assumed that there is ideal mixing of the gas, an instantaneous equilibrium is achieved at all times; hence, there are no temperature or pressure gradients assumed in the vessel. Also assumed was that (viii) all of the energy released becomes internal energy of the entire gas mixture. Also, since during combustion, not all of the hydrogen is consumed (especially at low initial hydrogen concentrations), "hydrogen concentration" refers to "consumed-hydrogen concentration".

Under the assumptions listed above, the energy released in a hydrogen burn is equal to the number of moles of hydrogen consumed times the energy released per mole consumed:

$$\Delta h = n_i HK \tag{7}$$

where H = the minimum of either the hydrogen concentration or twice the volume fraction of consumed hydrogen

K = energy released per mole $H_2O$ produced

= energy released per mole $H_2$ consumed;

$\Delta h$ = change in total enthalphy; and

$n_i$ = number of moles of gas initially in the vessel.

The final gas mixture ($n_f$) consists of (Figure 3):

$$n_f = [(S + H) + (1 - S - 1.5H)]n_i \tag{8}$$

$$= (1 - .5H)n_i \tag{9}$$

where $n_f$ = number of moles of gas in the final vessel mixture;

S = initial steam volume fraction;

$(S+H)n_i$ = initial number of moles of steam added to the number of moles of steam produced; and

$(1-S-1.5H)n_i$ = initial number of moles of diatomic gas minus the number of diatomic gas moles consumed.

The energy released by the hydrogen burn is distributed in such a way that a uniform temperature results:

$$\Delta T = \Delta h(n_f \overline{C}_p)^{-1} \tag{10}$$

$$= H\,K[(S+H)C_{ps} + (1-S-1.5H)C_{p2}]^{-1} \tag{11}$$

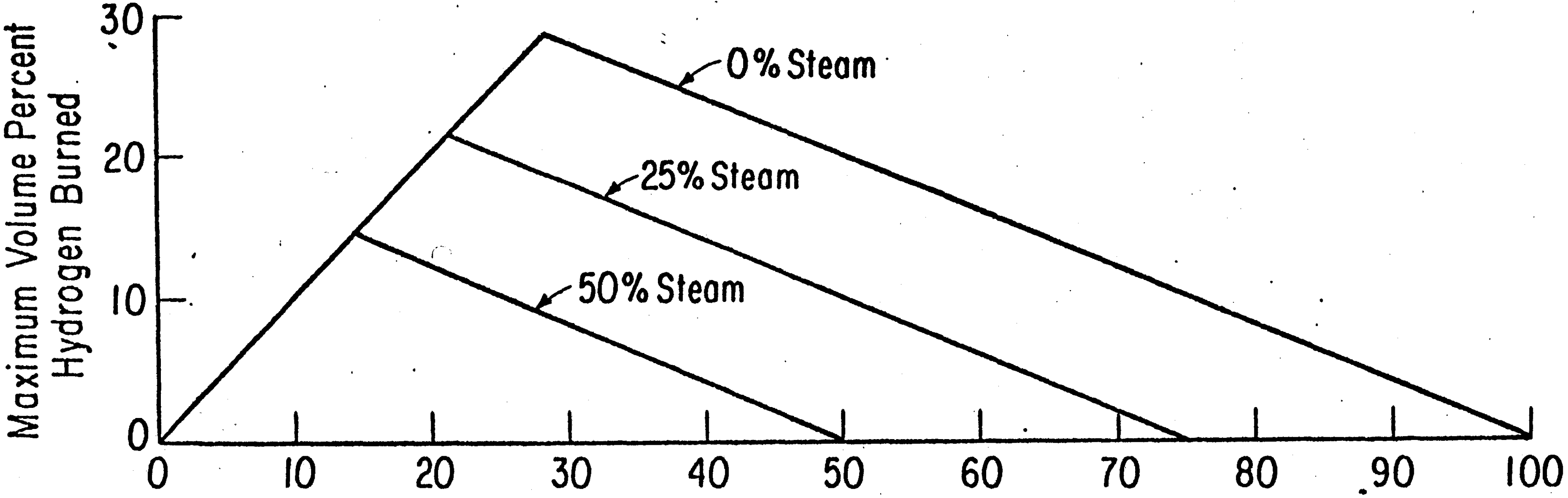


Figure 3   Maximum Volume Percent Hydrogen Burned

where $\overline{C}_p$ = molar weighted specific heat;

$C_{ps}$ = specific heat of steam;

$C_{p2}$ = specific heat of diatomic gas in the final mixture; and

$\Delta T$ = change in temperature.

Since

$$T_f = T_i + \Delta T \tag{12}$$

$$P_f = P_i + \Delta P \tag{13}$$

$$P_f = n_f RT_f V^{-1} \quad \text{and,} \tag{14}$$

$$P_i = n_i RT_i V^{-1} \tag{15}$$

then

$$P_f P_i^{-1} = n_f T_f (n_i T_i)^{-1} \tag{16}$$

$$= (1 - .5H) T_f T_i^{-1} \tag{17}$$

such that

$$\Delta P = P_i[(1-.5H) T_f T_i^{-1} - 1] \tag{18}$$

where $T_f$, $P_f$ are final temperature and pressure respectively, and

$T_i$, $P_i$ are initial temperature and pressure respectively.

Next, calculations were performed utilizing this simple model given $K$ = 57.8 Kcal/mole steam, $C_{p2}$ = 0.00695 Kcal/mole-$^oK$, and $C_{ps}$ = 0.00794 Kcal/mole-$^oK$. The predictions for room temperature and pressure (STP) using a value for K of 67.5 kcal/mole renders agreement between this model results and that of General Electric [7] with ± 3%, assuming initial conditions at STP were used in the GE model. (GE performed similar calculations using slightly different values for these constants [18].)

Sensitivity analysis shows that substitution of air by steam lowers the resulting pressure rise slightly; replacement of half of the total gas with water vapor drops the pressure by 7%. Adding steam raises the initial pressure such that the pressure rise ($P_f - P_i$) is smaller even though the final pressure is higher. For example, adding one volume of steam and 20 vol % hydrogen results in $P_i^{steam} = 29.4$ psia, $(P_f-P_i)^{steam} = 74$ psia, and $P_f^{steam} = 103$ psia compared with $(P_f-P_i) = 77$ psia and $P_f = 92$ psia for the undiluted system. Hence, adding steam results in a net increase in the final pressure (Figure 4). Increasing the initial temperature and pressure by the same factor causes the pressure rise to decrease slightly but causes the final pressure $P_f$ to be higher than the final pressure calculated for the case of standard initial conditions. For example, starting at room temperature and pressure with 20 vol % $H_2$ renders $P_f-P_i = 77.5$ psia; $P_f = 92.9$ psia compared with results for the case where the gas mixture is heated initially to 1500°K: $P_f-P_i = 77$ psia; $P_f = 145.2$ psia. Hence, although the differential pressure that results with heating is less, the final pressure being greater constitutes an aggrevation of the problem.

### C.4.2 Hydrogen Explosion Models

Two models were developed to calculate the pressure increase in containment due to a hydrogen explosion. The models are based on the same set of assumptions with the exception that the first model assumes an infinitesimally small impulse due only to the hydrogen immediately adjacent to the surface over an infinitesimally short time. The second model con-

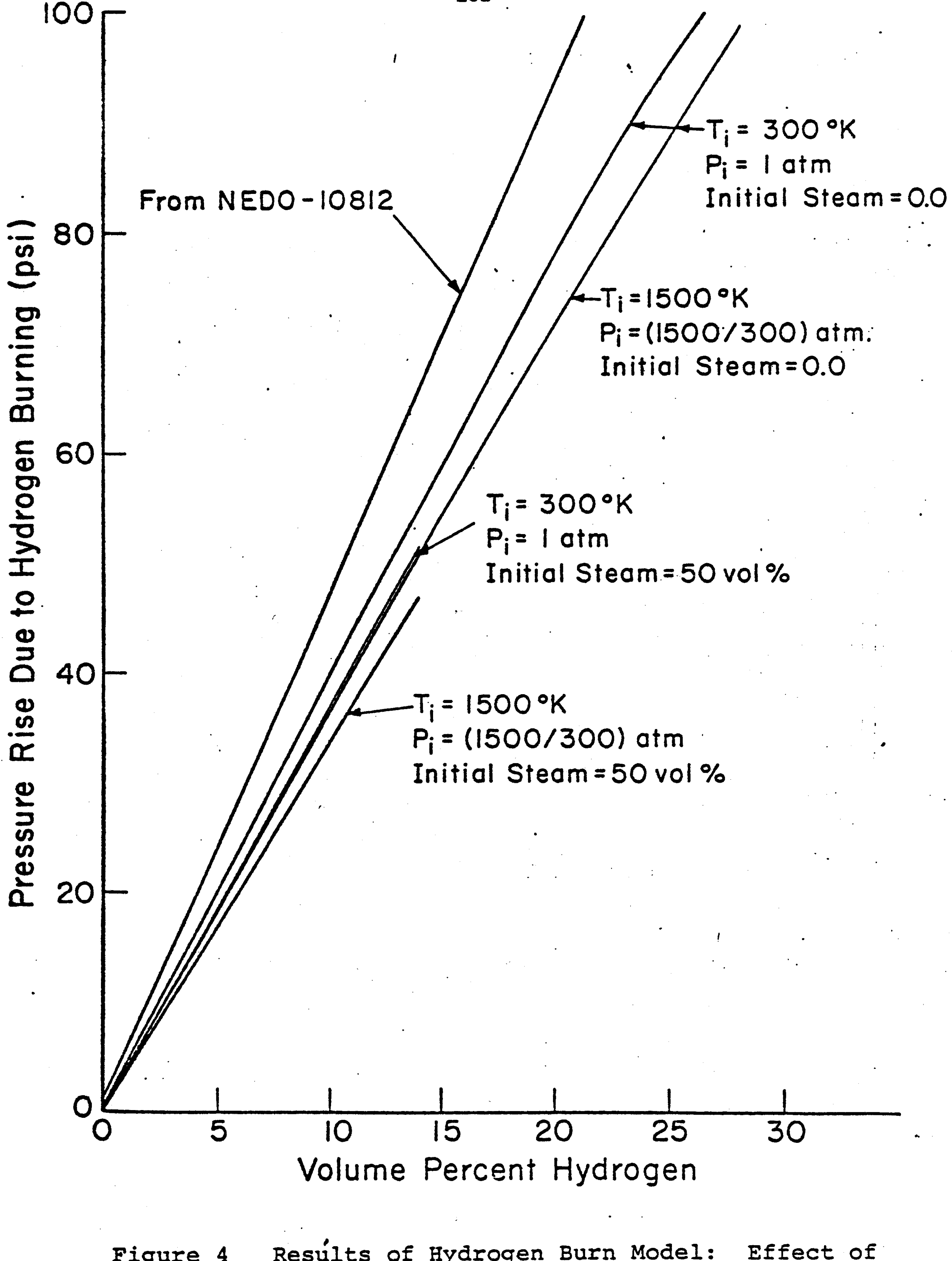


Figure 4 Resúlts of Hydrogen Burn Model: Effect of Steam on Pressure Rise Due to a Hydrogen Burn

siders the impulse contributions from the entire containment over a finite time. With this one exception, both models are based upon the following set of assumptions:

(i) detonation limits are disregarded for calculational purposes, i.e.: pressures pulses can be predicted across a wide spectrum of hydrogen-oxygen mixtures;

(ii) water vapor is assumed the final product of the hydrogen-oxygen reaction ozone and peroxide are neglected [15, 13];

(iii) the gas mixture is assumed initially uniformly distributed;

(iv) a spherical detonation front is assumed [7, 8];

(v) upon hitting a surface, the pressure front is assumed extinguished, the front continues uninterrupted in the other case;

(vi) it is assumed that all of the energy released in the detonation is converted to kinetic energy of the product steam;

(vii) the velocity distribution of the steam is assumed monoenergetic and isotropic; thus, the probability of finding a steam molecule of velocity $\underline{v}(p(\underline{v})d\underline{v})$ in a solid angle $d\Omega$ is (by definition) (see Fig. 5):

$$p(\underline{v})d\underline{v} = \delta(|\underline{v}| - v^*)dv(1/4\pi)d\underline{\Omega} \tag{19}$$

where the energy released per mole of $H_2$ divided by the weight per mole of steam is $1/2\ v^{*2}$, $\underline{v}$ = random variable representing the product steam velocity, and $v^*$ = magnitude of the velocity of the resulting product steam ($v^*$ is on the order of 5000 m/sec), and $\delta(|\underline{v}| - v^*)$ is the Dirac delta function;

Figure 5 Representation of Solid Angle Ω Used in Deriving Distribution in Steam Velocity ($\underline{v}$) [19]

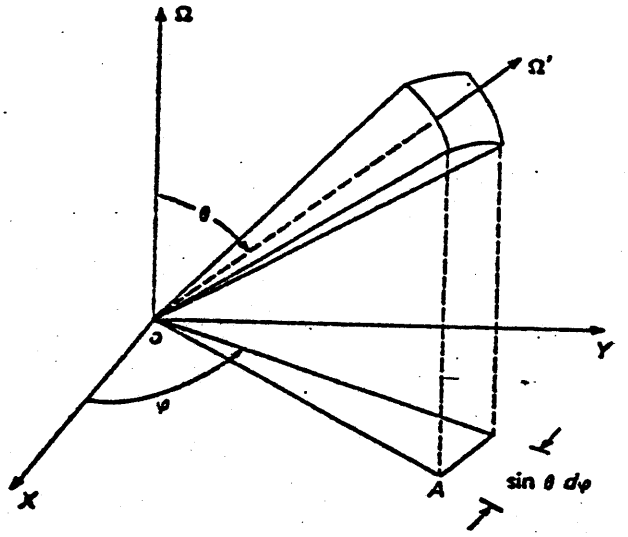
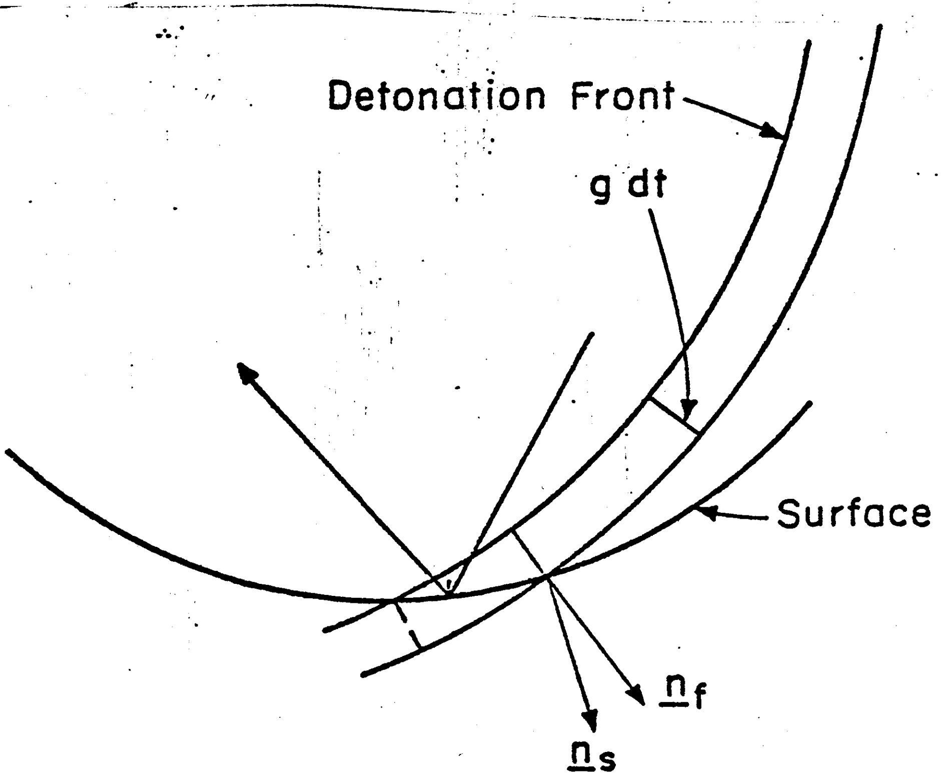


Figure 6 Modeling the Impact of the Hydrogen Detonation Front on the Containment Surface



(viii) the model assumed elastic collisions between the steam molecules produced in the detonation and any surfaces they bombard with; and

(ix) it is assumed that the energy released per mole of steam produced is a constant value.

Under these assumptions, the model can be derived as follows. Since all of the energy released is assumed to be converted into the kinetic energy of the product steam:

$$K = 1/2 \ m \ v^{*2} \tag{20}$$

where $K$ = energy released per mole of steam produced;

$m$ = mass of mole of steam; and

$v^*$ = velocity of the steam molecules.

When the pressure front impacts upon a surface area dA, the momentum transferred in that collision to the surface within the time interval dt is by definition (see Fig. 6):

$$2HDg \ dt \ dA(mv^*/4)(\underline{n}_2 \cdot \underline{n}_f)\underline{n}_s \tag{21}$$

where $H$ = volume fraction of hydrogen consumed;

$D$ = density of gas in volume (moles per unit volume);

$g$ = velocity of the detonation front;

$\underline{n}_s$ = outward normal from the surface; and

$\underline{n}_f$ = outward normal from the detonation front.

The impulse of the front equals the change in momentum, and since the pressure P is a force per unit area:

$$P = 1/2 \ HDg \ mv^*(\underline{n}_s \cdot \underline{n}_f) \tag{22}$$

The time of impact of the pressure pulses at various points on the surface are not simultaneous and the front travels at supersonic velocities.

A second model was developed to predict the pressure rise due to a hydrogen explosion. The major difference between this model and the one described earlier is the way in which the impulse on a given surface area dA is calculated. In this model, the momentum of the product steam is not dissipated until after the first collision with the surface, whereas in model 1, if the steam does not collide immediately with the surface, the energy is assumed dissipated to the surrounding gas. This assumption affects the impulse calculation and the time scale involved. Assuming that all of the energy released in the explosion initially is transferred into kinetic energy K of the steam ($K = 0.5\ mv^{*2}$), the total impulse I on an area dA on the surface is given by (see Figure 7):

$$I = 2mv^* \int_V c(\underline{w})\,dA(4\pi|\underline{w} - \underline{u}|)^{-1}\underline{n}_s\ d\underline{w} \qquad (23)$$

where $c(\underline{w})$ = H·D for $\underline{w}$ in free volume; 0 otherwise;

$\underline{w}$ = position in volume V;

m = mass of mole of steam;

$\underline{u}$ = position on surface; and

$\underline{n}_s$ = outward normal from surface.

Since pressure is a force per unit area, or impulse per unit time and area, the pressure P in the surface produced by the explosion is:

$$P = \frac{2mv^*}{4\pi} \int c(\underline{w})\underline{n}_s(\underline{w}-\underline{u})(|\underline{w}-\underline{u}|)^{-3}(\Delta t)^{-1} \qquad (24)$$

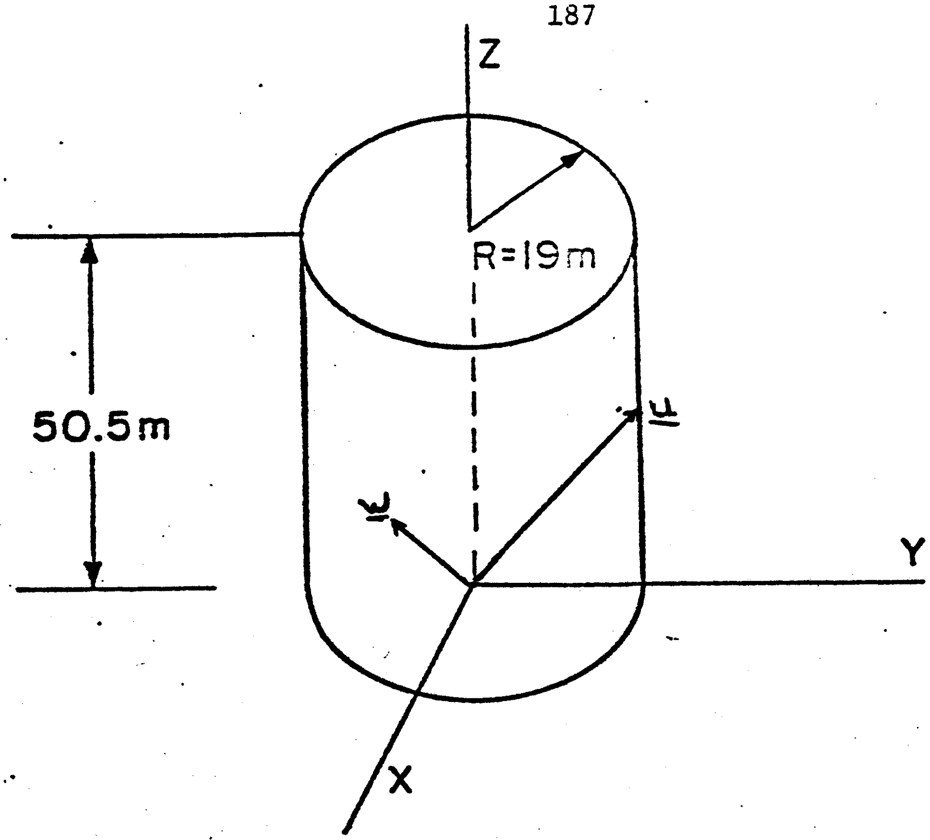


Figure 7    Approximation of Containment Structure

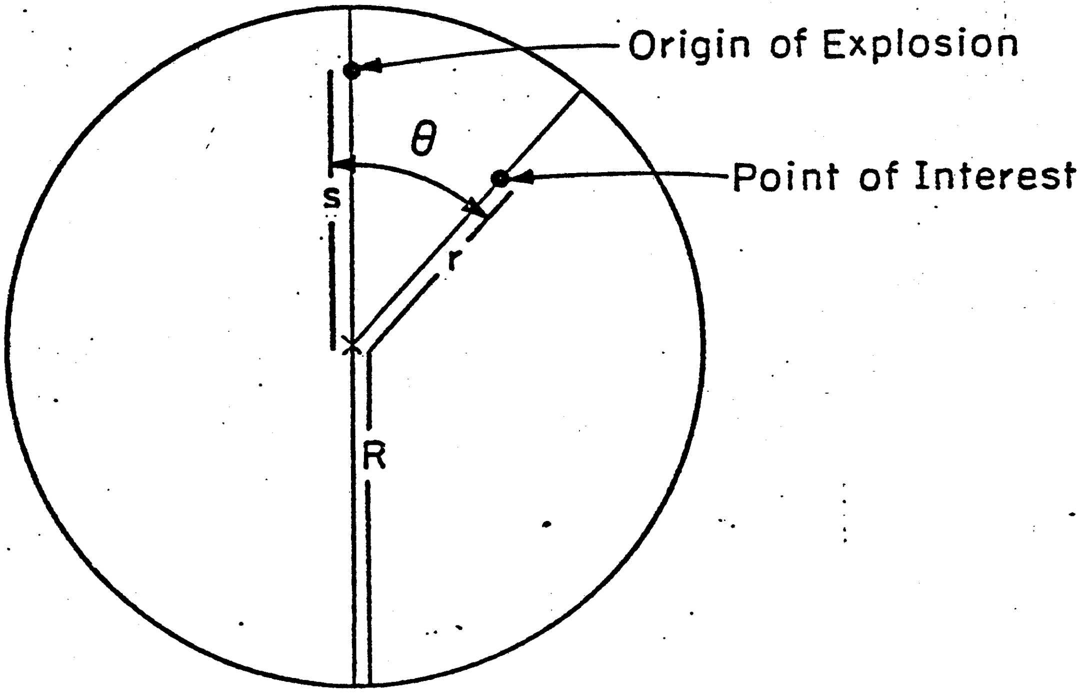


Figure 8    Geometry of Containment Cross-Section (Model 1)

where $\Delta t$ is the time duration of the spike. The duration of the spike is the same over all of the containment surface, but is not felt at all points at the same instant (in the sample calculations that follow, the duration of the pressure rise is ∿ 30 millisec and the maximum time lag ∿ 4 millisec).

### C.4.3 Sample Calculations

Sample calculations were performed using both models to estimate the pressure increases due to hydrogen explosions in a containment structure. The containment structure is approximated as a cylindrical volume with height 51 m and radius (R) 19 m (see Figure 7). The velocity of the detonation front is assumed constant at 1200 m/sec with a 20% $H_2$-80% air mixture at 18 psia and room temperature. In model 2, an assumption was made that all of the contents of the vessel are uniformly distributed throughout the volume. To account for this, c, the effective hydrogen concentration in the vessel is used, where

$c \equiv H \cdot D$ free volume/total volume.

Two cases were examined in calculating the pressure distribution in containment due to a hydrogen explosion: (i) at the lateral surface of the containment, and (ii) at the top of the structure. (These cases were defined in this way for ease in calculation.)

#### C.4.3.1 Case I: Lateral Surface of Containment

Model 1

The surface of interest is on the lateral surface of the containment ($r=R$, where R is the radius of the cylinder). In Cartesian coordinates, the explosion originates at s, 0, $z_s$) and the surface of interest is at ($r \cos \theta$, $r \sin \theta$, $z_r$) (Figure 8). The normal to the detonation front at the surface is:

$$\underline{n}_f = \frac{(r\ \cos\ \theta,\ r\ \sin\ \theta,\ z_r) - (s,\ \theta,\ z_s)}{|(r\ \cos\ \theta,\ r\ \sin\ \theta,\ z_r) - (s,\ 0,\ z_s)|} \tag{25}$$

$$= \frac{r\ \cos\ \theta - s,\ r\ \sin\ \theta,\ z_r - z_s)}{(r^2+s^2+\Delta z^2 - 2rs\ \cos\ \theta)^{1/2}} \tag{26}$$

The normal to the surface at $(r\ \cos\ \theta,\ r\ \sin\ \theta,\ z_r)$ is:

$$\underline{n}_s = \frac{(r\ \cos\ \theta,\ r\ \sin\ \theta,\ z_r) - (0,\ 0,\ z_r)}{|(r\ \cos\ \theta,\ r\ \sin\ \theta,\ z_r) - (0,\ 0,\ z_r)|} \tag{27}$$

$$= (\cos\ \theta,\ \sin\ \theta,\ 0) \tag{28}$$

Therefore:

$$\underline{n}_s \cdot \underline{n}_f = \frac{r - s\ \cos\ \theta}{(r^2+s^2+\ z^2-2sr\ \cos\ \theta)^{1/2}} \tag{29}$$

and

$$P = \frac{1}{2}\ \mathrm{HDg}\ mv^* \frac{(r - s\ \cos\ \theta)}{(r^2+s^2+(z_r-z_s)^2-2rs\ \cos\ \theta)^{1/2}} \tag{30}$$

For an explosion originating at $s = 0$, the magnitude of the pulse is a constand as a function of angle $\theta$ and is symmetric about the maximum at $\Delta z = 0$. For an explosion originating elsewhere, the maximum pulse is at $\Delta z = 0$, $\theta = 0$ or $\pi$, and is symmetric about $\Delta z = 0$.

Model 2

The impulse consists of two components - the impulse from points above the surface and below the surface. Referring to Figure 9, the impulse above or below the surface of interest is given as:

$$I = \sum_{i=1}^{2} dA\ 2cmv^* \int (4\pi s^2)-1\ (\cos \theta \cos \emptyset)\ dL\ Ld\theta\ L \cos \theta\ d\emptyset \tag{31}$$

where L = the distance from a point located in the volume to the surface

θ = the angle between the xy plane and the line between the point in the volume and the surface, and

∅ = the angle between the x-y component of the vector between the point in the volume and the surface of interest, and a radial vector to the surface of interest.

The limits of integration for ∅ are $[\emptyset_m, -\emptyset_m]$ where, using the law of sines (again r = R):

$$\sin \emptyset\ (r)^{-1} = \sin\ (\pi-2\ \emptyset_m)(L \cos \theta)^{-1} \tag{32}$$

which yields:

$$\cos \emptyset_m = L(2r)^{-1} \cos \theta \tag{33}$$

or

$$\sin \emptyset_m = [1 - L^2(2r)^{-2} \cos^2 \theta]^{1/2} \tag{34}$$

Thus:

$$I = \sum_{i=1}^{2} dA2cmv^* \int (2\pi)^{-1} dL \cos^2 \theta\ [(1-L^2(2r)^{-2} \cos^2 \theta)^{1/2}]\ d\theta \tag{35}$$

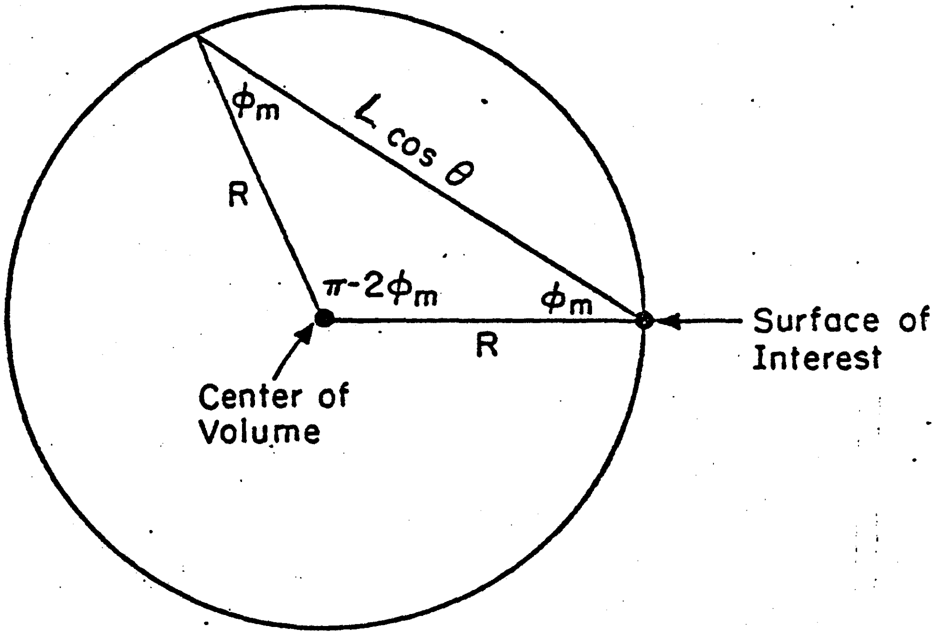


Figure 9 Geometry of Containment Cross-Section (Model 2)

Now, $z_1 = z_{max}-z_r$ and $z_2 = z_r$; $\theta_{max,i} = \sin^{-1} z_i/L$ for $L \geq z_i$, or $\pi/2$ for $L \leq z_i$; $\theta_{min} = \cos^{-1} 2r/L$ for $L \geq 2r$, or 0 for $L \geq 2r$; and $L^2_{max,i} = Z_i^2 + (2r)^2$. Thus:

$$I = \sum_{i=1}^{2} dA\ 2cmv* \int (2\pi)^{-1} dL \int_{\theta_{min}}^{\theta_{max,i}} \cos^2 \theta\ (1-L^2(2r)^{-2} \cos^2 \theta)^{1/2}\ dL \qquad (36)$$

Alternately, by reversing the order of integration, with $L\ max(\theta)_i = z_i \sin \theta^{-1}$ for $0 \geq 0^*_i$ and $2r \cos \theta^{-1}$ for $\theta \leq \theta^*_i$, and $\tan \theta^*_i = z_i(2r)^{-1}$,

$$I = \sum_{i=1}^{2} dA\ 2cmv* [\int_0^{\theta^*_i} (2\ )^{-1} \cos^2 \theta\ d\theta \int_0^{2r(\cos \theta)^{-1}} (1-L^2(2r)^{-2} \cos^2 \theta)^{1/2}\ dL$$

$$+ \int_{\theta^*_i}^{\pi/2} (2\ )^{-1} \cos^2 \theta\ d\theta \int_0^{z_i \sin \theta^{-1}} (1 - L^2(2r)^{-1} \cos^2 \theta)^{1/2}\ dL] \qquad (37)$$

or

$$I = \sum_{i=1}^{2} da\ 2cmv* [0.25r\ z_i z_i + (2r)^2)^{-1/2}$$

$$+ 0.5\pi^{-1}\ r\int_{\theta^*_1}^{\pi/2} \cos \theta\ (z(2r)^{-1} \cot \theta\ (1-z^2(2r)^2 \cot^2 \theta)^{1/2}$$

$$+ \sin^{-1} (z(2r)^{-1} \cot \theta))] \qquad (38)$$

This equation was evaluated by numerical methods to derive results. The maximum pressure rise is felt at $z = 0.5\ z_{max}$, and the pressure rise is symmetric about $z = 0.5\ z_{max}$. Keeping the volume fixed and $z/z_{max}$ fixed, the maximum pressure rise is felt at $R/z_{max}$ between $R/z_{max} = 0.8$ (for $z/z_{max} = 0$) and $R/z_{max} = 0.65$ (for $z/z_{max} = 0.5$).

### C.4.3.2 Case II: Top Surface of Containment

#### Model 1

The surface of interest is on the top of the cylinder (r = R). In Cartesian coordinates, the surface of interest is at $(r \cos \theta, r \sin \theta, z_r)$ where $z_r = 0$ or 51 m. The normal to the surface at these points is given by:

$$\underline{n}_s = (0,0,1),\ z_r = 51 \text{ m} \tag{39}$$

$$= (0,0,-1),\ z_r = 0 \tag{40}$$

The normal to the detonation front at the surface is analogous to case 1 (see equations 25 and 26), and

$$P = \frac{1}{2} \text{Hgmv*} \frac{|z_s - z_r|}{(r^2 + L^2 + (z_s - z_r)^2 - 2rL \cos \theta)^{1/2}} \tag{41}$$

The maximum pressure pulse is felt at $r = L\ \theta = 0$. The variation in the pulse magnitude increases with increasing s and decreasing $|z_s - z_r|$.

Model 2

The surface of interest is the end of the cylinder at a radius $r = R$. The distance L between the surface and a point in the volume is $L^2 = (\rho \cos \theta - r_L)^2 + ( \ \sin \theta)^2 + z^2$ where the fraction of the momentum in the z direction is $zL^{-1}$. Thus:

$$I = dA\ 2cmv^* \int_0^{2\pi} \rho\, d\theta \int_0^R d\rho \int_0^{z_{max}} dz\ (4\pi L^2)^{-1} zL^{-1} \tag{42}$$

$$= dA\ 2cmv^* \int_0^{2\pi} (4\pi)^{-1} d\theta\ \{(R^2+r^2-2R\ r \cos \theta)^{1/2} - (R^2+r^2-z_{max}^2-2R\ r \cos \theta)^{1/2}$$

$$- r + (r^2+z_{max}^2)^{1/2} + L\ r \cos \theta \log [((R^2+r^2-2R\ r \cos \theta)^{1/2} + R - r \cos \theta)$$

$$(r - r \cos \theta)^{-1}((r^2+z_{max}^2)^{1/2} - r \cos \theta)(R^2 + r^2 + z_{max}^2 - 2R\ r \cos \theta)^{1/2}$$

$$+ R - r \cos \theta)]\} \tag{43}$$

This integral was then evaluated numerically. The maximum pressure pulse for a given $R/z_{max}$ ratio is at $r = 0$. The maximum pulse is felt at $R/z_{max}$ between 0.55 (for $r = 0$) and 0.35 (for $r = R$).

Results of the model calculations are shown in Figure 10 for models 1 and 2, case I; and Figure 11 for models 1 and 2, case II. Since model 2 time averages the impulse on a surface to determine the pressure, and differences in the duration of the impulse to different surfaces is neglected, there is no angular dependence on the magnitude of the predicted pressure rise. (Model 1 does assume an angular dependence.) The impulse delivered to any surface is independent of the origin of the explosion. The duration, however, is not independent. The numbers shown in these figures are calculated for an

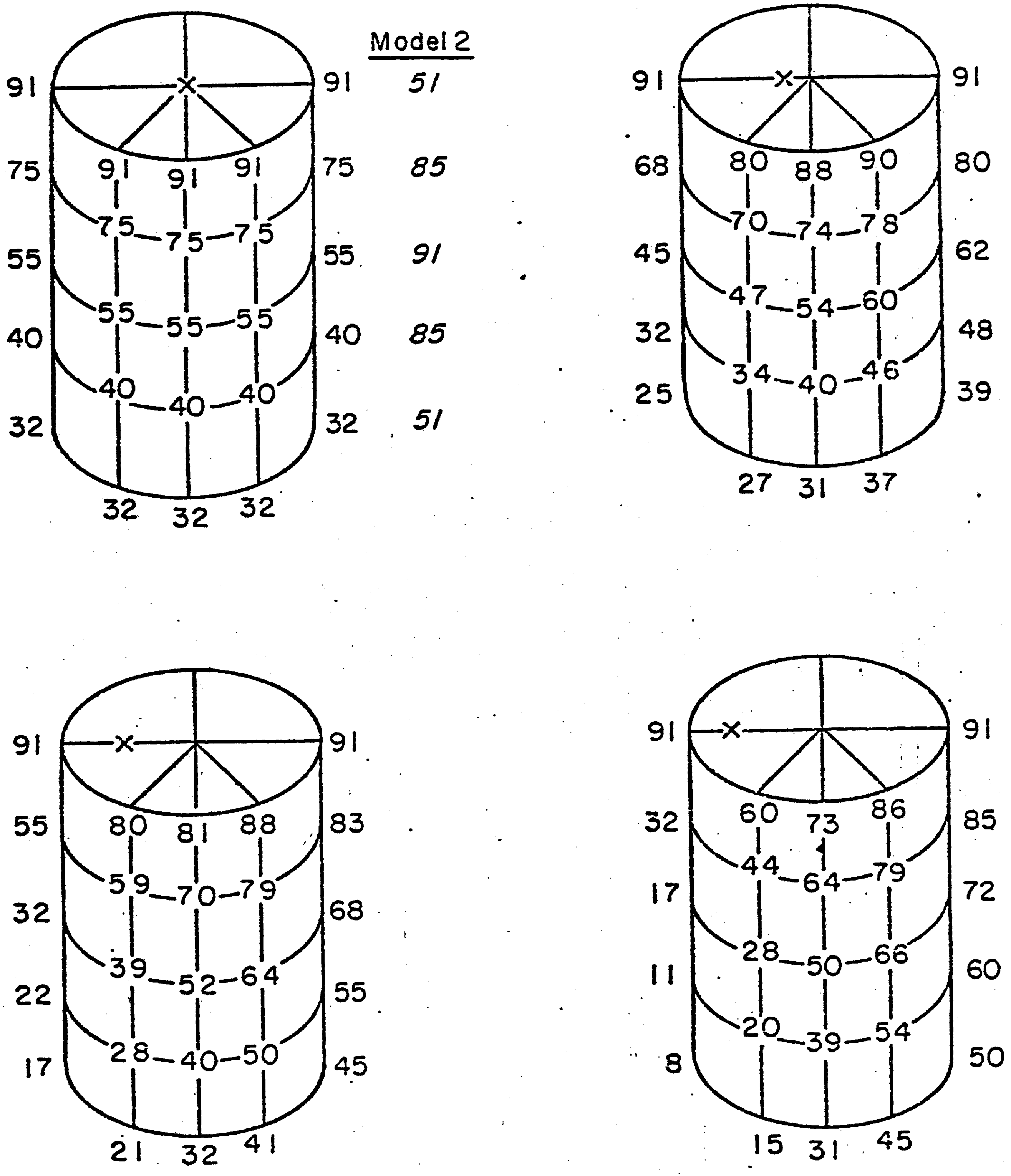


Figure 10 Results of Hydrogen Explosion Pressure Calculations for Case I (Lateral Surface of Containment)

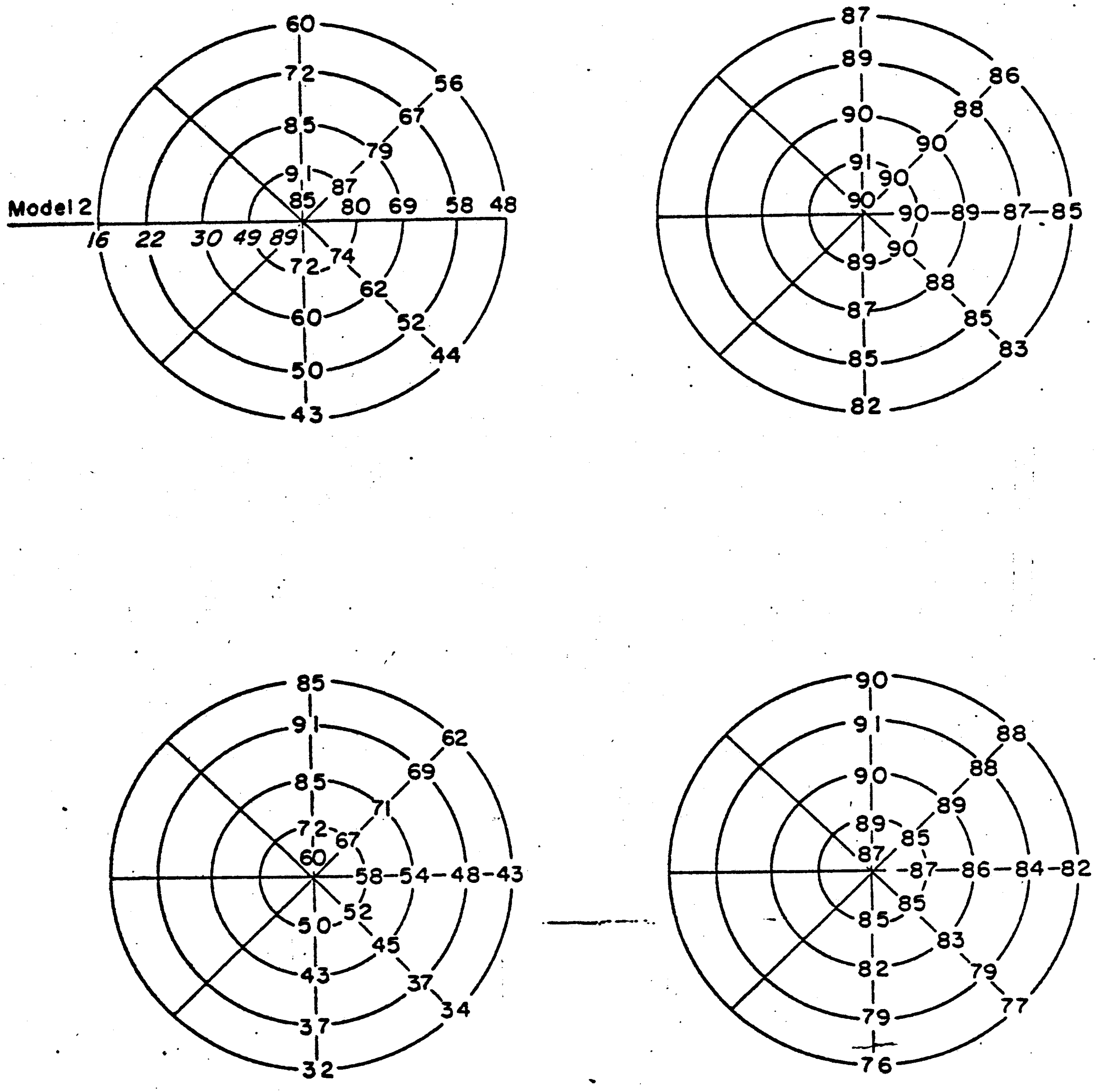


Figure 11 Results of Hydrogen Explosion Pressure Calculations for Case II (Top Surface of Containment)

explosion initiated at the center of the vessel. To determine the pressure response due to an explosion originating at a radius s and height z, the numbers shown here must be multiplied by $[(19+s)^2 + z_*^2]^{1/2}[19^2 + 25.25^2]^{-1/2}$, where $z_*$ is the maximum of either (50.5-z) or z. This factor varies between 0.5, for an explosion originating at a corner of the vessel, and 1.0, for an explosion originating at the center of the vessel.

## C.5 Summary and Further Discussion

A comparison was made of the maximum predicted pressure pulse due to a hydrogen detonation with that due to a hydrogen burn (Figure 12). In comparing the calculated values for the pressure rise, it is important to note that the pressure spike from the explosion would be added to the overall pressure rise in the vessel. In the calculations, the minimum value of the initial hydrogen concentration still within the detonation region was used along with a low value of 1200 m/sec for the detonation velocity. The calculated pressure spike for the explosion is thus 92 psia using the first model lasting for an infinitesimally small time; the second model calculates a pressure pulse of 91 psia lasting about 30 milliseconds (Figure 12).

It is informative to compare these results with the only truly relevant datum - the pressure spike experienced at Three Mile Island. The predictions are approximately three times higher than the actual spike. This seems to imply that both models are quite conservative in the upward direction, since higher pressures may be predicted than actually occur.

The ratio of the predictions of model 1 to model 2 is independent of the initial conditions. For a given geometry, the predictions of both of the models for the pressure rise varies as the product of the concentration of the hydrcgen and the velocity of detonation. At hydrogen concentrations

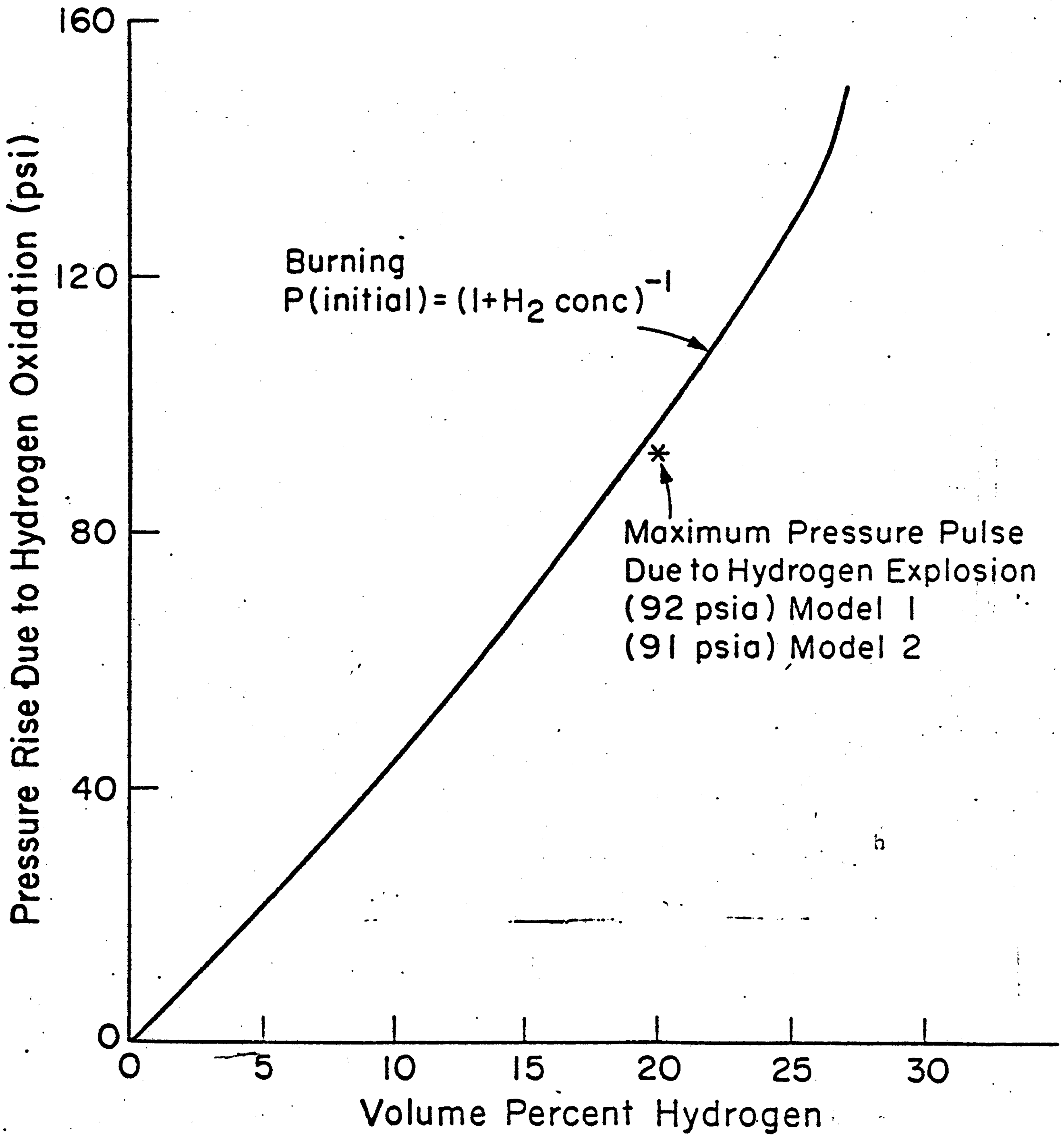


Figure 12 Comparison of Maximum Predicted Pressure Pulse from Hydrogen Explosion With Hydrogen Burn

between twenty and thirty percent by volume, the detonation velocity is greater than 1200 m/sec [6]. Therefore, in that region, the pressure rise increases faster than linear. The burning model predicts pressure rises roughly proportional to the consumed hydrogen concentration. Hence, at higher initial hydrogen concentrations, the pressure rise predicted by the burning model will not be so large relative to the predictions of the explosion models.

While both models 1 and 2 predict approximately the same maximum pressure spike, they do not predict the same momentum transfer. Model 2 is more intuitive and physically correct, although it involves substantially more computer time to calculate the numerical integration. (The time required to predict the pressure rise at one point of the surface using model 2 is ∿ 0.1 seconds of CPU time on the Honeywell MULTICS system.) The momentum transfer is a function of the entire volume of the containment. Model 1 neglects momentum, except from the steam that is produced immediately adjacent to the surface of interest. Model 2 includes the contribution of the momentum from the entire volume over a finite time while the transfer in model 1 is over an infinitely short time. By doubling all of the dimensions of the containment and keeping the same gas conditions, model 2 predicts an impulse per unit area that is two times as large over a duration that is also two times as long. The impulse varies as the cube of the length, the area goes as the square of the length, and the time goes as the length; hence, the impulse per unit area doubles as does the time, and since pressure = impulse/area-time, the pressure rise remains the same.

To conclude, hydrogen burn and detonation mechanisms and pressure response models have been reviewed in this article. Calculations were performed to calculate the expected pressure rise due to either a hydrogen burn or explosion in containment with the containment structure approximated as a cylinder of height 50.5 m and radius 19 m. As mentioned earlier, the assumption in the burning model that no energy is absorbed by the surroundings is very conservative. This fits in with the experimental results from General Electric [7]. We are still searching the literature for experimental data on hydrogen explosions in large vessels. Most of the experiments performed have been in narrow tubes with diameters of the order of centimeters, an order of magnitude narrower than the case at hand. Therefore, conclusions are difficult to draw from this data as the experimental volume is not comparable to that of an LWR containment.

## III.D Applying Bayes' Theorem to Update the Estimate of the Reactor Core Melt Frequency After TMI

### D.1 Summary of Study Results

A study was performed to investigate the limitations on the use of Bayes' theorem for updating probability estimates, particularly as applied to update estimates of the reactor core melt frequency. A Bayesian approach was taken in the earlier work of Apostolakis and Mosleh to assess the reactor core melt frequency, particularly with concern placed on the impact of critical judgment on RSS estimates [6]. This study examines the validity of this approach to probability updating using the experience at Three Mile Island as an additional data point by which past estimates can be modified. The specific numerical results of this study are representative only.

The main conclusions of the study are:

(1) Bayes' theorem is a concensus forming tool. It reduces uncertainty and therefore should not be used when there is disagreement about data validity;

(2) The relative importance of the prior and new evidence depends on the relative uncertainty of the distributions chosen to represent that data. The posterior is most influenced by the more peaked of either the prior or likelihood distributions and will result in less uncertainty than either of the two original distributions; and

(3) Operating experience apparently contributes less to the results than does engineering judgment.

These considerations combined with a desire to understand the applicability of a Bayesian approach toward assessing uncertainty has lead to the present work. By adopting a Bayesian or subjectivist approach [5], expert opinion and experiencial data can be combined to render useful and interesting results. Such an approach was taken earlier by Apostolakis and Mosleh to assess the reactor core melt frequency particularly with concern placed on the impact of critical judgment on RSS estimates [6].

This paper is divided into three sections: the first reviews Bayes' theorem and the results of the Apostolakis and Mosleh paper and relates these results to the present work. The main section deals with the impact of Three Mile Island and reactor operating experience on estimates of the reactor core melt frequency. Caveats concerning the application of Bayes' theorem are also discussed. Finally, overall conclusions are drawn.

## D.2 Introduction

The use of Bayes' Theorem to update estimates of the reactor core melt frequency was undertaken by Apostolakis and Mosleh. This paper is motivated by questions concerning Bayes' Theorem and numerical applications to problems. In particular, it is of interest to determine what data and information contributes the most in these applications, and how such applications should be used and interpreted, and what conclusions from such a practice are justified.

## D.3 A Review of Bayes Theorem

The use of Bayes theorem and its application to problems of risk assessment in the nuclear field has been expanded upon by several authors [6,7,8,9]. In this work, a special inferential notation is utilized following the work of Howard et al. at the Stanford Research Institute [10]. This notation defines a conditional state, ε, known as the prior information existing at the time the calculation is made. New evidence is noted here by the letter B and refers generally to real life experience expressed in terms of a model or probability distribution. The core melt frequency is treated as an uncertain quantity, denoted $\lambda_j$, where j refers to a particular interval falling in a range of possible values on λ (i.e., 0 to 1). With these definitions, Bayes theorem becomes:

$$P(\lambda_j|B,\varepsilon) = P(\lambda_j|\varepsilon)\,\frac{P(B|\lambda_j)}{\sum_j P(\lambda_j|\varepsilon)P(B|\lambda_j)} \qquad (1)$$

where $P(\lambda_j|B,\varepsilon) \equiv$ probability that the core melt frequency is in the range of $\lambda_j$ given new evidence B is applied against a prior estimate of the core melt frequency distribution, ε;

$P(\lambda_j|\varepsilon) \equiv$ probability that the core melt frequency is in the range of $\lambda_j$ given original prior information ε; and

$P(B|\lambda_j) \equiv$ probability of new evidence B occurring given that the actual core melt frequency is $\lambda_j$.

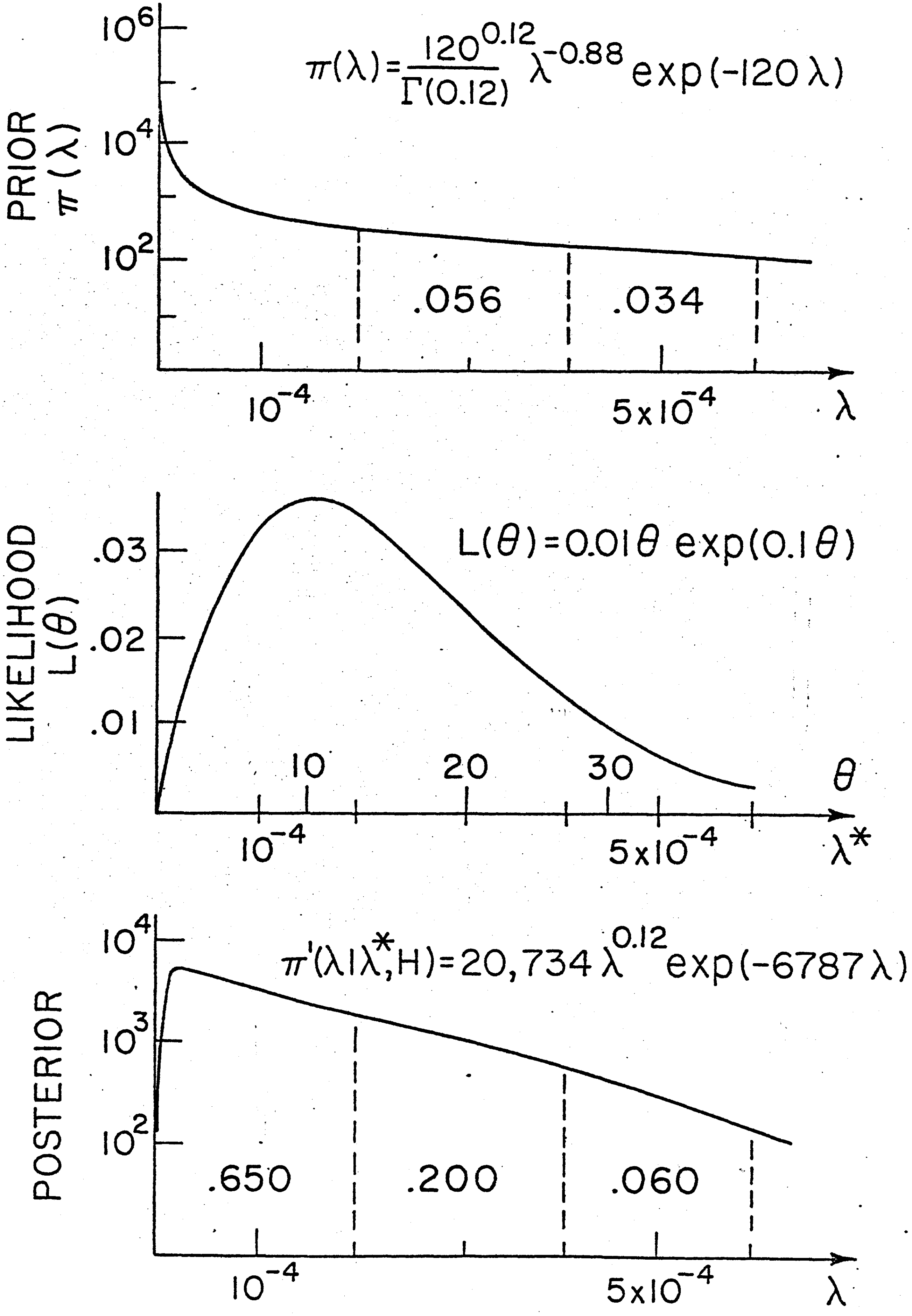
Bayes theorem can be used as a method for modifying an estimate based on new evidence. The prior information ε refers to a "state-of-information" based on some existing data, opinion or engineering judgment and therefore $P(\lambda_j|\varepsilon)$ is the prior estimate of the probability that the reactor core melt frequency $\lambda$ will be in the range specified by $\lambda$.

D.4 Apostolakis and Mosleh

The work by Apostolakis and Mosleh [6] also used conjugate distributions in applying Bayes theorem to assess a posterior distribution reflecting both expert and critical opinion concerning the results of the RSS. Reactor operating experience was used as the prior information and a Gamma distribution was applied to reflect this information. The probability of a core melt based on this information being greater than $1.5\times10^{-2}$ was found to be less than 1%; that is, an expected value of one in ∿67 reactor years. An estimate of the mean of $9.7\times10^{-5}$ was found based on .03 melts per 310 commercial reactor years of experience.

Using a Poisson distribution based on the RSS and its critics, Apostolakis and Mosleh determined that the likelihood distribution reflected an increase in the RSS estimate by a factor of ten such that the mode went from $1.5\times10^{-5}$/reactor-year to $1.5\times10^{-4}$/reactor-year. Then, a value for $\lambda$ the reactor core melt frequency was chosen such that the probability of $\lambda$ being greater than this value is no more than 5% (i.e., $\lambda = 7.1\times10^{-4}$/reactor-year). Using a transformation of variables to $\gamma$ and $\kappa$, the results shown in Figure 1 were derived, where $\alpha = \gamma\kappa + 1$; $\beta = \kappa/\lambda^* \rightarrow r^*/T^*$. The prior, likelihood and posterior distributions on $\lambda$. the core melt frequency per reactor-year are shown in Figure 1 as derived by Apostolakis and Mosleh. Controversy later arose [11,12,13] over how such distributions should be constructed and which set of data most correctly represents the prior

Figure 1 Estimates of Reactor Core Melt Frequency from Apostolakis and Mosleh [6].



information since building poor representations of the prior can render unreasonable results. The work of Apostolakis and Mosleh demonstrates an interesting approach and is modified and expanded upon in this work.

## D.5 Calculations

### D.5.1 Prior Distribution

In this work, to arrive at prior distributions reflecting existing knowledge with regard to the core melt frequency $\lambda$ estimates and uncertainty factors were assigned as shown in Table I. Five different distributions are shown broken into ten intervals falling between 0 and $\infty$ on the x axis. (Use of the ten interval notation facilitates later computations.) A log normal distribution was assigned to model the prior information, which consists of the reactor safety study and the composite of the critics noted in the work of Apostolakis and Mosleh [6]. Beginning with the RSS and assuming an uncertainty of a factor of ± 5 and the critics composite a weighted RSS + critics estimation for the prior was derived in such a way that the relative weight assigned to the validity of the RSS equals that of all critics combined (i.e., the weighting factors are normalized to sum to one). The uncertanity factors associated with the critics estimates are conjectural and represent the authors' best estimates only. A revised RSS + critics distribution was next derived (see fourth row in Table I) based on the authors' subjective assessment to produce a more realistic probabili~~ty~~-estimate at high values for $\lambda_j$. This revised prior is compared with the RSS estimate itself modified to include an uncertainty of ±10 (fifth row in Table I). The major difference

# Table I

## CORE MELT FREQUENCY

## PRIOR DISTRIBUTIONS

0 $5\text{x}10^{-6}$ $1\text{x}10^{-5}$ $5\text{x}10^{-5}$ $1\text{x}10^{-4}$ $2\text{x}10^{-4}$ $4\text{x}10^{-4}$ $8\text{x}10^{-4}$ $2\text{x}10^{-3}$ $4\text{x}10^{-3}$ ∞

| Interval | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| RSS: $5 \times 10^{-5}$ $\overset{x}{\div}$ factor of 5[a] | .009 | .040 | .451 | .261 | .161 | .061 | .014 | $2\text{x}10^{-4}$ | $1\text{x}10^{-5}$ | $6\text{x}10^{-6}$ |
| Critics Composite[b] | .005 | .011 | .094 | .088 | .117 | .135 | .143 | .167 | .096 | .143 |
| Weighted RSS + Critics[c] | .007 | .025 | .273 | .174 | .139 | .098 | .079 | .086 | .048 | .071 |
| Revised RSS + Critics[d] | .007 | .025 | .303 | .205 | .171 | .129 | .100 | .049 | .010 | .001 |
| RSS: $5 \times 10^{-5}$ $\overset{x}{\div}$ factor of 10[e] | .050 | .075 | .375 | .190 | .149 | .090 | .046 | .020 | .004 | .001 |

a) All factors are 90% confidence intervals.

b) Critics estimates from reference 6 --

Union of Concerned Scientists: $7.5 \times 10^{-4} \overset{x}{\div} 20$; Hsieh & Okrent: $6.4 \times 10^{-4} \overset{x}{\div} 10$; EPA: $1 \times 10^{-4} \overset{x}{\div} 10$; EPA: $1.5 \times 10^{-3} \overset{x}{\div} 20$. Averaged probabilities in each interval.

c) Weighted so Reactor Safety Study equals all critics combined.

d) Subjectively revised to produce more realistic probability at high $\lambda_j$.

e) Suggested as reasonable by Prof. N.C. Rasmussen, MIT.

between the RSS and the critics is in the estimate of the mean; the critics consistently place their estimates factors of 10-30 higher than the RSS. The revised RSS + critics estimate for the prior distribution on $\lambda$ reduces $\lambda_9$ and $\lambda_{10}$ spreading the likelihood over the $\lambda_4$-$\lambda_8$ intervals. This reflects, in our opinion, a more reasonable estimate of the prior distribution since even critical appraisal shows that $\lambda$ will not be as high as the unrevised estimate.

D.5.2 Likelihood Function

New evidence B defined as r* is a function of the number of "observed" melts in T* reactor years of commercial experience following Apostolakis and Mosleh [6]:

$$\lambda = \frac{r^*}{T^*} \tag{2}$$

A modified Poisson distribution was used to describe the likelihood function $P(B|\lambda_j)$ for four different combinations of values for r* and T* (Table II):

$$P(r^*|\lambda_j) = \frac{(\lambda_j T^*)^{r^*}}{\Gamma(r^*+1)} \exp(-\lambda_j T^*) \tag{3}$$

where $\Gamma(r^*+1) \equiv$ Gamma function ($\Gamma(1.06) = .96874$). Results of this procedure are shown in Table II. Note that the larger the background of experience (i.e., as $T \to \infty$), the more peaked becomes the Poisson distribution for the likelihood function about the ratio r*/T* (in our calculations, r*/T* is set at $\sim 9.7 \times 10^{-5}$ yr$^{-1}$).

## Table II

### CORE MELT EXPERIENCE DISTRIBUTIONS

$(\frac{r^*}{T^*} = 9.7 \times 10^{-5} yr^{-1})^*$

| Interval | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Core Melt Frequency $\lambda_j$ | $4x10^{-6}$ | $8x10^{-6}$ | $3x10^{-5}$ | $8x10^{-5}$ | $1.5x10^{-4}$ | $3x10^{-4}$ | $6x10^{-4}$ | $1.2x10^{-3}$ | $3x10^{-3}$ | $5x10^{-3}$ |
| $r^* = .03$<br>$T^* = 310$ yrs | .831 | .847 | .875 | .888 | .885 | .863 | .803 | .680 | .400 | .219 |
| $r^* = .06$<br>$T^* = 620$ yrs | .718 | .747 | .798 | .820 | .816 | .775 | .671 | .482 | .167 | .050 |
| $r^* = .12$<br>$T^* = 1240$ yrs | .558 | .603 | .688 | .727 | .719 | .649 | .486 | .251 | .030 | .003 |
| $r^* = .24$<br>$T^* = 2480$ yrs | .360 | .421 | .548 | .612 | .598 | .487 | .273 | .073 | .001 | $8x10^{-6}$ |

* $r^*$ = "observed" number of core melts

$T^*$ ≡ total reactor years of operation

$\Gamma(r^*+1)$ ≡ Gamma function ($\Gamma(1.06) = .96874$)

### D.5.3 Sample Calculation of Posterior

A typical calculation of the posterior distribution on $\lambda$ reflecting both RSS + critic prior information and commercial operating experience in the likelihood function is shown in Table III. This particular calculation also includes the impact of Three Mile Island in the experience base as reflected in the likelihood function. One calculation was made to answer the question what would be the posterior if the probability of a meltdown at Three Mile Island was about the same as at Browns Ferry when the fire incident occurred [14]; using Apostolakis and Mosleh's estimate for the Browns Ferry incident of .03, then $r^* = .06$ with $T^*$ the number of commercial years of experience as of 1979 of about 620 reactor-years (620 years was chosen because it doubles Apostolakis and Mosleh's estimate of reactor experience while retaining the same ratio for $r^*/T^*$. Also EPRI has used this number in their ATWS work (see section III.A)).

The procedure followed is also shown in Table III: (i) estimate the prior using the appropriate calculations and assumptions (i.e., here based on the RSS + critics viewpoints weighted for relative validity), (ii) calculate the likelihood of a core melt as reflected in the cumulative reactor experience to date placing subjective probability estimates on any events that may be construed to have come reasonably close to a core melt (i.e., Browns Ferry and/or Three Mile Island), (iii) multiply the prior with the likelihood $P(\lambda_j|\varepsilon)P(B|\lambda_j)$ for each range of $\lambda$ and sum, and (iv) divide $\sum_j P(\lambda_j|\varepsilon)P(B|\lambda_j)$ into $P(\lambda_j|\varepsilon)P(B|\lambda_j)$ to arrive at the posterior distribution $P(\lambda_j|B,\varepsilon)$.

## Table III

### EFFECT OF TMI - "INDUSTRY" ESTIMATE

($P_{TMI}$ = 0.03)

| Interval | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Σ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Core Melt Frequency $\lambda_j$ | $4x10^{-6}$ | $8x10^{-6}$ | $3x10^{-5}$ | $8x10^{-5}$ | $1.5x10^{-4}$ | $3x10^{-4}$ | $6x10^{-4}$ | $1.2x10^{-3}$ | $3x10^{-3}$ | $5x10^{-3}$ | |
| Weighted RSS+Critics $P(\lambda_j \mid \varepsilon)$ | .0073 | .025 | .273 | .174 | .139 | .098 | .079 | .086 | .048 | .071 | |
| $r^*$ = .06 <br> $T^*$ = 620 yr $P(B \mid \lambda_j)$ | .718 | .747 | .798 | .820 | .816 | .775 | .671 | .482 | .167 | .050 | |
| $P(\lambda_j \mid \varepsilon)P(B \mid \lambda_j)$ | .005 | .019 | .218 | .143 | .113 | .076 | .053 | .041 | .008 | .004 | .680 |
| $P(\lambda_j \mid B,\varepsilon)$ | .007 | .028 | .321 | .210 | .166 | .112 | .078 | .060 | .012 | .006 | |

## D.6 Results

### D.6.1 Impact of Three Mile Island

Two cases were examined in computing a posterior distribution on $\lambda$; use of a "reasonable" estimate for the probability of TMI having become a core melt accident of $P_{TMI} \sim 0.10$ such that $r^* = .03 + .10 = .13$, (ii) use of a critics estimate on $P_{TMI} = .75$ such that $r^* = .03 + .75 = .78$, and (iii) use of an "industry" estimate of $P_{TMI} = .03$ (discussed in II.C above).* Results of the calculations are shown in Tables IV and V for the "reasonable" and "critic's" estimate of $P_{TMI}$, and are compared to the "industry" result in Figure 2. (Note that in these calculations, the weighted RSS + critics estimates for the prior distribution is utilized.) The results show that the "industry" and "reasonable" estimates do not change the estimate on the core melt frequency much when compared with the prior estimate but that the "critic's" estimate does considerably. The median values of each of the resulting posterior distribution are shown in Figure 2 for the "industry" (I), "reasonable" (R) and "critic's" (C) estimates; an order of magnitude difference in $\lambda$ is seen between the industry and critic viewpoints.

### D.6.2 Impact of Reactor Operating Experience

The impact of the number of reactor years of commercial operating experience T* on the posterior estimate is shown in Figure 3 for T* = 310, 620, 1240, and 2480 reactor-years. The effect is to

*These values for $P_{TMI}$ are chosen more for example than on any more profound base of justification. Thus, results are representative only.

peak the distribution about $1x10^{-4}$ and to sharpen the cut off at the upper end of $\lambda$. This assumes $r^*/T^*$ stays constant at $9.7x10^{-5}hr^{-1}$ thus allowing for a proportionate increase in the number of events related to core melt.

### D.6.3 Bayesian Combination of RSS and Critics

When Reactor Safety Study estimated $\lambda_{median} = 5x10^{-5}$ with the critics estimate varying up to a factor of 30 higher. In part III.A of this paper, the RSS and critic estimates for $\lambda$ the core melt frequency were combined into a prior estimate on $\lambda$. It is also possible to apply Bayes theorem to arrive at a posterior distribution based on a combination of the RSS and critics distributions on $\lambda$. The result of such a calculation is shown in Figure 4. Note that the resulting posterior (i.e., RSS + critics composite distribution) exhibits less uncertainty than either the RSS or critics distribution on $\lambda$. Because of this seeming reduction in uncertainty, the use of Bayes theorem as a method for arriving at a composite distribution to be used as a representation for the prior distribution does not seem warranted. Details of the Bayesian calculation for arriving at a composite of the RSS + critics are given in Table VI.

### D.6.4 Caveats in Applications of Bayes Theorem

The preceding example serves to illustrate the care that must be taken in applying Bayes theorem for purposes of probabilistic estimation. Careful interpretation of results using the Bayesian approach can eliminate many possible pitfalls. In applying Bayes theorem, it is important to note that the theorem itself treats all existing data and expert opinion equally as valid and that in many cases the resulting posterior will exhibit a lesser degree of uncertainty than either the prior or likelihood functions. That is why the composite RSS + critics distribution derived above using the Bayesian approach exhibited less uncertainty when in fact the actual controversial nature of the validity of either the RSS or critics estimates would imply a wider spread for the composite distribution.

To illustrate this result a simple example is now given. Suppose an uncertain variable $\theta$ is estimated by both subject A and subject B. Suppose that A estimates $\theta$ to fall between 1 and 4 and B estimates $\theta$ to fall between 4 and 7. If A and B are both equally legitimate sources of information (i.e., A and B's estimates are of equal validity), then the resulting narrow posterior distribution on $\theta$ as shown in Figure 5 is a proper composite of the two distributions. However, if the interpretation of A and B is that either estimate could be wrong, then a more proper composite might be a distribution that peaks between 4 and 5 but includes the possibility that $\theta$ can still fall between 0 and 7. The point of this exercise is to caution against applications of Bayes theorem when A and B's estimates are not totally independent unbiased estimates. In the case of the reactor core melt frequency controversy this observation may hold especially valid since the critics estimates are simple multiples of the RSS results and are clearly dependent estimates.

## D.7 Conclusions/Further Discussion

In applying Bayes theorem to estimation problems the following points should be noted: (i) the posterior distribution will likely exhibit a lesser degree of uncertainty than either the prior or likelihood distributions, (ii) because of (i), Bayes theorem may not be useful for arriving at composites of distributions that reflect controversial opinions as the resulting composites represent concensus, and (iii) the relative importance of the prior and likelihood functions on the posterior is reflected in the spread or variance of the respective distributions. In the particular application addressed here, specifically the impact of TMI on the reactor core melt frequency $\lambda$, we find that estimates on the probability that TMI approached a core melt ($P_{TMI}$) of between .03-.10 did not shift the RSS estimate significantly [15]. On the other hand, if one perceives TMI as a "near miss" (i.e., $P_{TMI} \geq .75$), the core melt frequency is shifted upward. Bayes theorem can be a useful tool for providing a mathematical framework to update probabilistic estimates in the light of new experience and experimental data. However, it must be used with common sense.

Figure 2 Effect of TMI on Posterior Distribution for Core Melt Frequency.

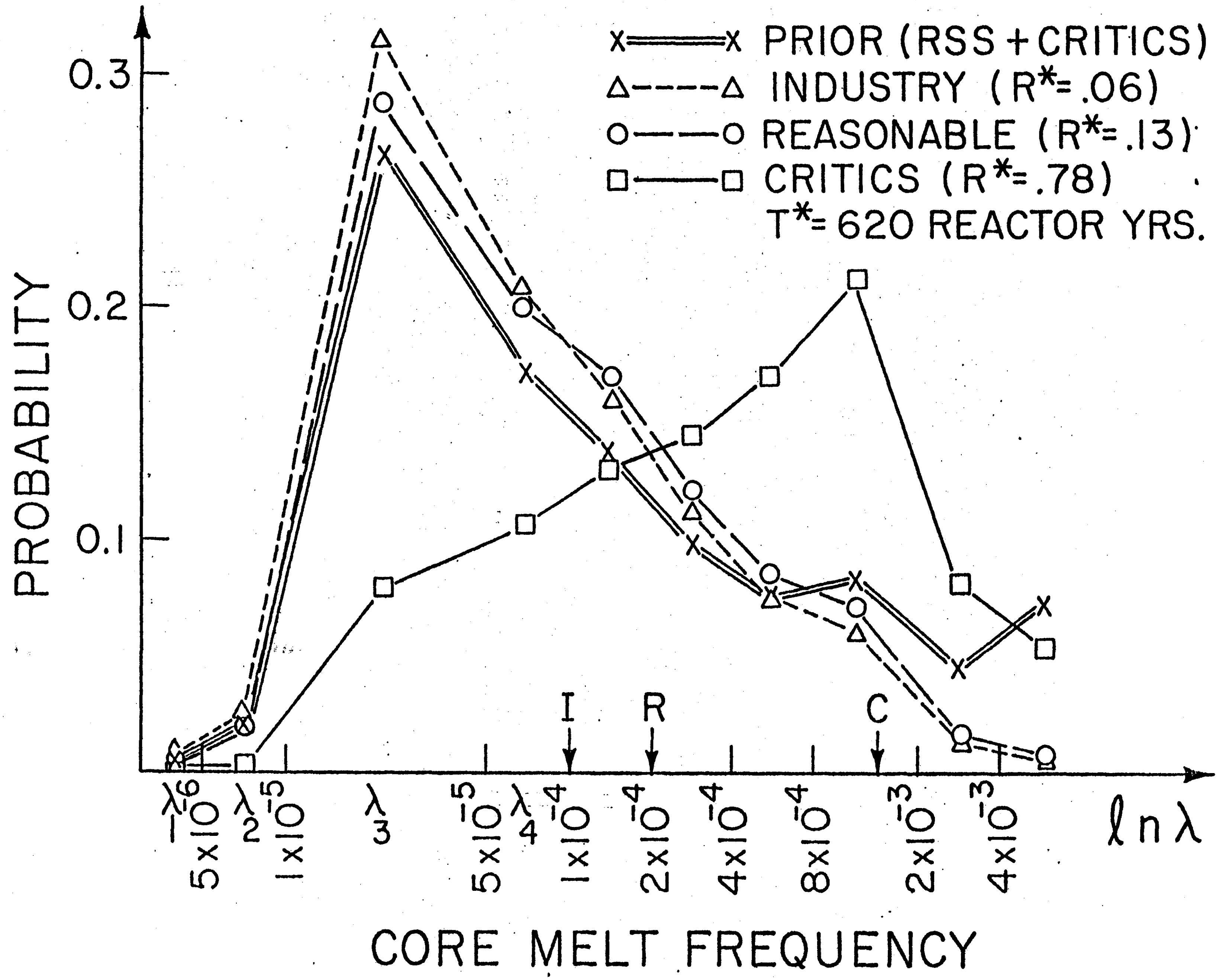


Figure 3 Effect of Operating Experience on the Core Melt Frequency Estimate.

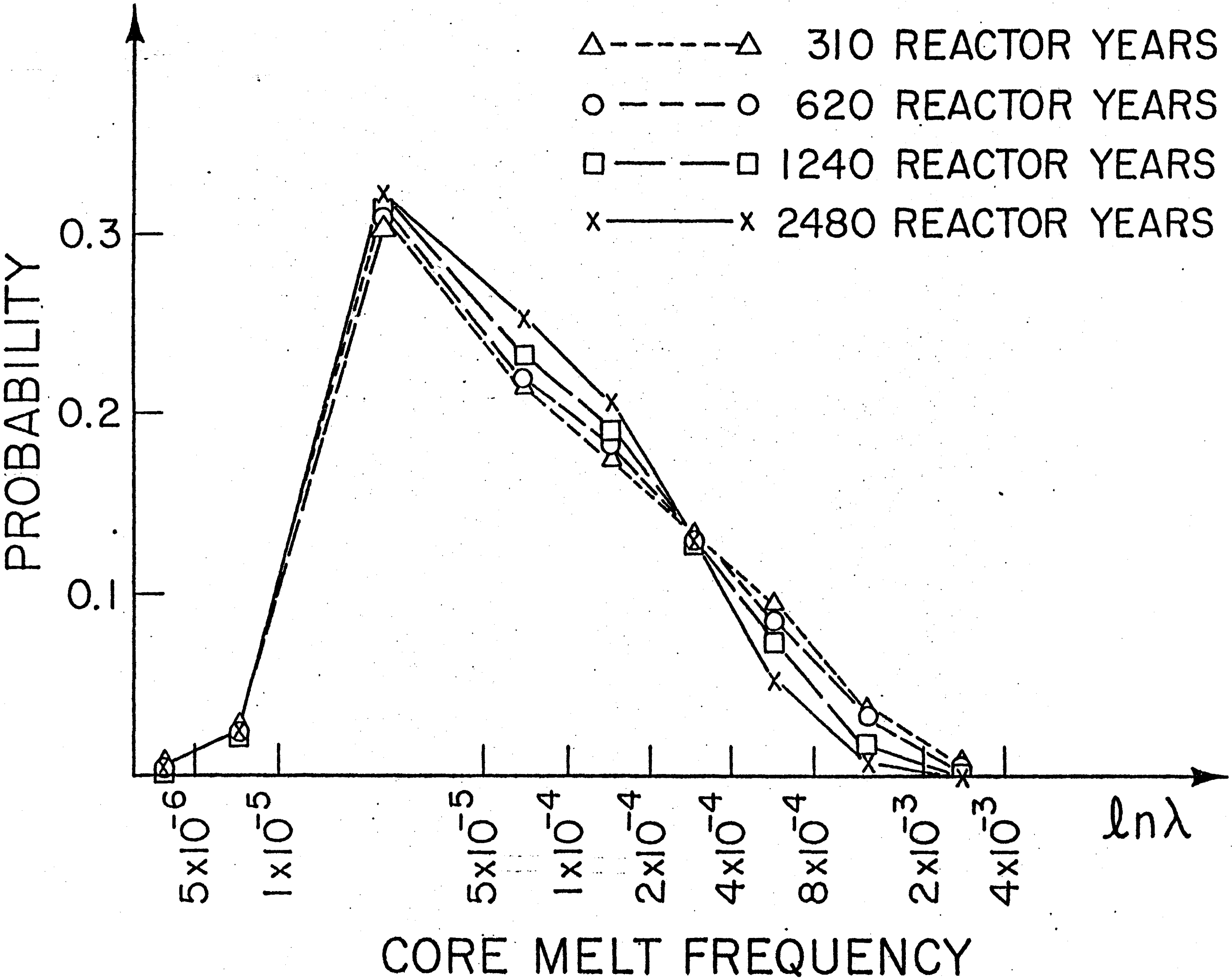


Figure 4 Bayesian Calculation of the RSS and Critics Composite Distribution.

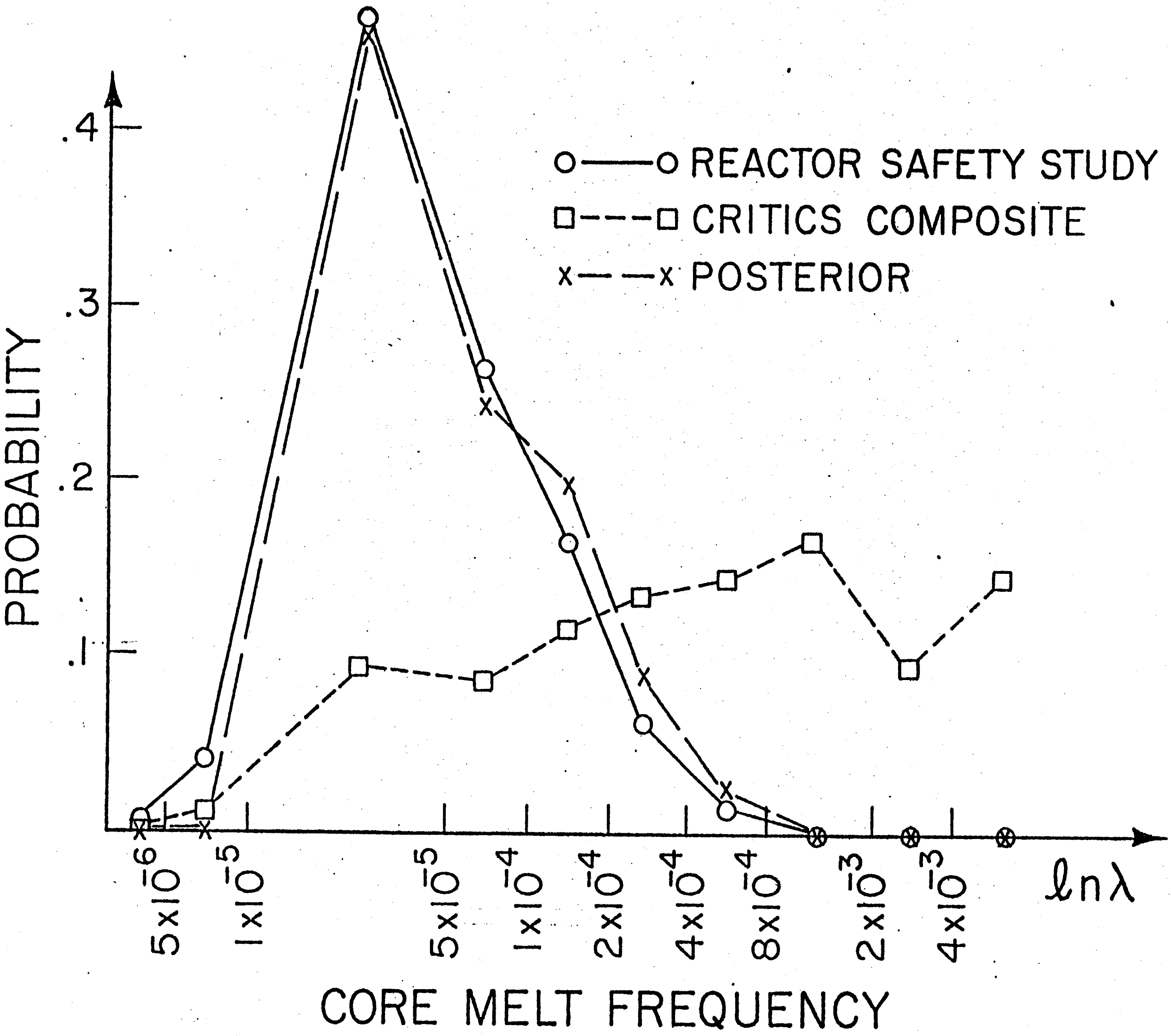
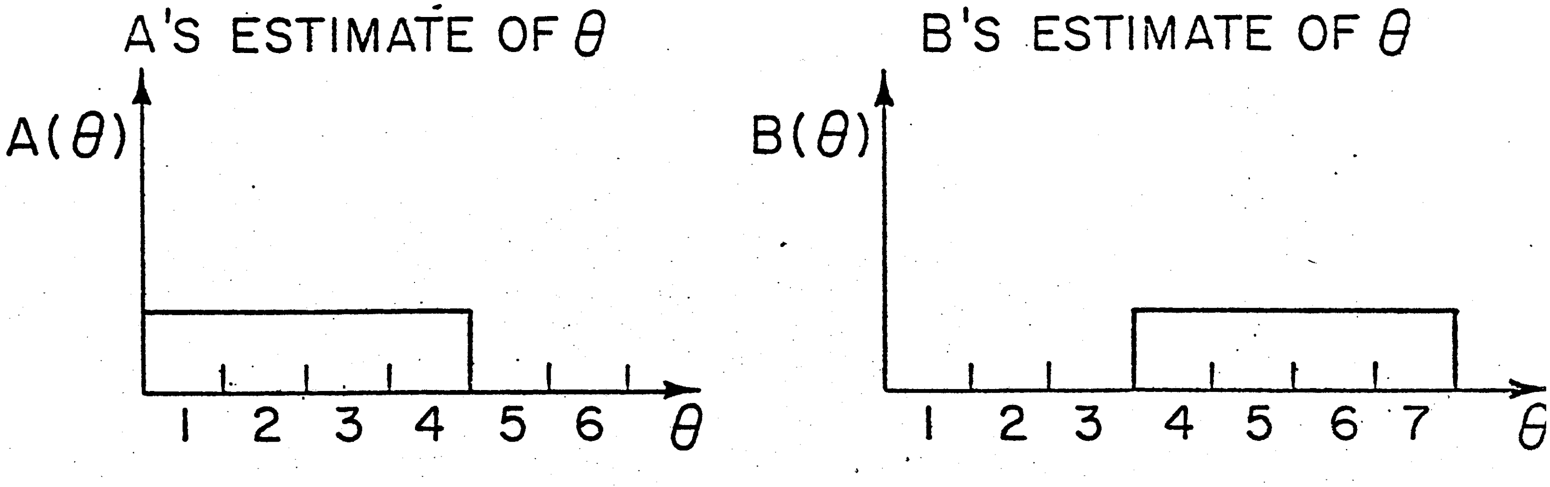
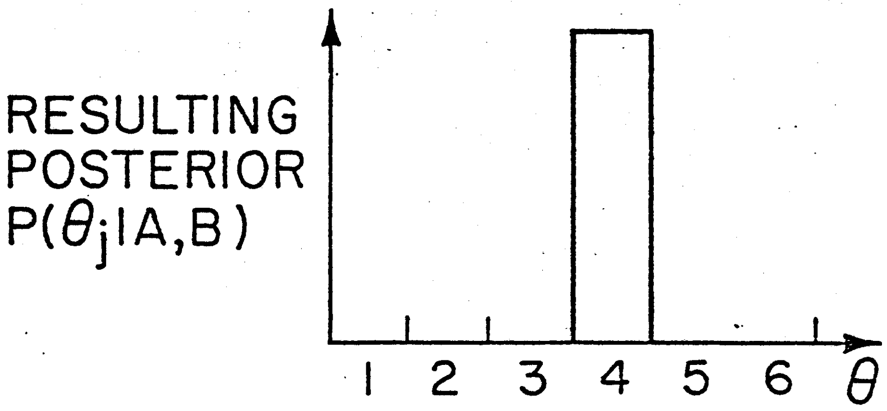


Figure 5 Caveats in Applying Bayes Theorem: A Simple Example.



| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $P(\theta_j \vert A)$ | 1/4 | 1/4 | 1/4 | 1/4 | 0 | 0 | 0 |
| $P(B \vert \theta_j)$ | 0 | 0 | 0 | 1/4 | 1/4 | 1/4 | 1/4 |
| $P(\theta_j \vert A)P(B \vert \theta_j)$ | 0 | 0 | 0 | 1/16 | 0 | 0 | 0 |
| $P(\theta_j \vert A,B)$ | 0 | 0 | 0 | 1 | 0 | 0 | 0 |



## Table IV

### EFFECT OF TMI - "REASONABLE" ESTIMATE

$(P_{TMI} = 0.10)$

| Interval | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Σ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Core Melt Frequency $\lambda_j$ | $4x10^{-6}$ | $8x10^{-6}$ | $3x10^{-5}$ | $8x10^{-5}$ | $1.5x10^{-4}$ | $3x10^{-4}$ | $6x10^{-4}$ | $1.2x10^{-3}$ | $3x10^{-3}$ | $5x10^{-3}$ | |
| Weighted RSS+Critics $P(\lambda_j\|\varepsilon)$ | .0073 | .025 | .273 | .174 | .139 | .098 | .079 | .086 | .048 | .071 | |
| $r^* = .13$<br>$T^* = 620$ yr $P(B\|\lambda_j)$ | .487 | .531 | .622 | .685 | .712 | .710 | .645 | .487 | .180 | .056 | |
| $P(\lambda_j\|\varepsilon)P(B\|\lambda_j)$ | .004 | .013 | .170 | .119 | .099 | .070 | .051 | .042 | .0086 | .0040 | .5798 |
| $P(\lambda_j\|B,\varepsilon)$ | .007 | .022 | .293 | .205 | .171 | .121 | .088 | .072 | .015 | .007 | |

## Table V

### EFFECT OF TMI - "CRITICS" ESTIMATE

$(P_{TMI} = 0.75)$

| Interval | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Σ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Core Melt Frequency $\lambda_j$ | $4x10^{-6}$ | $8x10^{-6}$ | $3x10^{-5}$ | $8x10^{-5}$ | $1.5x10^{-4}$ | $3x10^{-4}$ | $6x10^{-4}$ | $1.2x10^{-3}$ | $3x10^{-3}$ | $5x10^{-3}$ | |
| Weighted RSS+Critics $P(\lambda_j \mid \varepsilon)$ | .0073 | .025 | .273 | .174 | .139 | .098 | .079 | .086 | .048 | .071 | |
| $r^* = .78$<br>$T^* = 620$ yr $P(B \mid \lambda_j)$ | .010 | .017 | .047 | .099 | .154 | .241 | .344 | .407 | .273 | .118 | |
| $P(\lambda_j \mid \varepsilon) P(B \mid \lambda_j)$ | $7x10^{-5}$ | $4x10^{-4}$ | .0130 | .0172 | .0214 | .0236 | .0272 | .0350 | .0131 | .0084 | .1592 |
| $P(\lambda_j \mid B, \varepsilon)$ | .0004 | .0025 | .0816 | .1080 | .1344 | .1482 | .1708 | .2198 | .0823 | .0528 | |

## Table VI

### CORE MELT FREQUENCY ESTIMATE:

### REACTOR SAFETY STUDY MODIFIED BY CRITICS COMPOSITE

| Interval | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Σ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Core Melt Frequency $\lambda_j$ | $4x10^{-6}$ | $8x10^{-6}$ | $3x10^{-5}$ | $8x10^{-5}$ | $1.5x10^{-4}$ | $3x10^{-4}$ | $6x10^{-4}$ | $1.2x10^{-3}$ | $3x10^{-3}$ | $5x10^{-3}$ | |
| RSS: $5x10^{-5}$ $\overset{x}{\div}$ factor of 5 $P(\lambda_j\|E)$ | .009 | .040 | .451 | .261 | .161 | .061 | .014 | $2x10^{-4}$ | $1x10^{-5}$ | $6x10^{-6}$ | |
| Critics Composite $P(B\|\lambda_j)$ | .005 | .011 | .094 | .088 | .117 | .135 | .143 | .167 | .096 | .143 | |
| $P(\lambda_j\|\varepsilon)P(B\|\lambda_j)$ | $4.8x10^{-5}$ | $4.3x10^{-4}$ | .042 | .023 | .019 | .0083 | .0021 | $3.4x10^{-5}$ | $9.6x10^{-7}$ | $1.4x10^{-7}$ | .0950 |
| $P(\lambda_j\|B,\varepsilon)$ | .0005 | .0045 | .444 | .242 | .198 | .087 | .022 | .0004 | $1x10^{-5}$ | $1.5x10^{-6}$ | |

# REFERENCES

## Section I

1. Heising-Goodman, C.D., "Quantitative Methods in R&D Decision-Making", George Washington University, NSF-Sponsored Seminar Series, June 1980.

2. Lovins, A.B., "Cost-Risk-Benefit Assessments in Energy Policy", George Washington Law Review, Vol. 45, No. 5, August 1977, pp. 917-943.

3. Taylor, V., "Subjectivity and Science: A Correspondence About Belief", Technology Review, February 1979, pp. 49-57.

4. Kneese, A.V., "The Faustian Bargain", Resources, No. 44, September 1973, pp. 1-8.

5. Maxey, M.N., "Energy Needs: A Bioethical Perspective on Value-Conflicts", Address Given at American Nuclear Society Topical Meeting on Thermal Reactor Safety, Knoxville, Tennessee, April 1980.

6. Maxey, M.N., "Radiation Protection Philosophy: Bioethical Problems and Priorities", American Industrial Hygiene Association Journal, Vol. 39, September 1980, pp. 689-694.

7. Rose, D.J., "Energy - Some Unasked Questions - Continuity and Metanoia", The James R. Killian, Jr. Faculty Achievement Lectures, Massachusetts Institute of Technology, April 1980.

8. Rose, D.J., "On the Global $CO_2$ Problem", Testimony in Front of U.S. Senate Committee on Energy and Natural Resources, April 3, 1980.

9. O'Donnell, E.P., "The Need for a Cost-Benefit Perspective in the Nuclear Regulatory Process", Ebasco Services, Inc., American Nuclear Society Transactions, November 1978.

10. Hillier, F.S. and Lieberman, G.J., Operations Research, 2nd Edition, Holden-Day, Inc., San Francisco CA 1974.

11. Readings in Decision Analysis, Decision Analysis Group, Stanford Research Institute, Menlo Park CA, 1976.

12. Spetzler, C.S. and Staël von Holstein, C.S., "Probability Encoding in Decision Analysis", Presented at the ORSA-TIMS-AIEE 1972 Joint National Meeting, Atlantic City, New Jersey, November 8-10, 1972.

13. The Need for Change: The Legacy of TMI, Report of the President's Commission on the Accident at Three Mile Island, Pergamon Press, Washington DC, October 1979.

14. "Analysis of the Three Mile Island - Unit 2 Accident", Nuclear Safety Analysis Center, NSAC-1, July 1979.

15. "TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations", NUREG-0578, U.S. Nuclear Regulatory Commission, July 1979.

16. Lewis Report, Risk Assessment Review Group, U.S. Nuclear Regulatory Commission, November 1978.

17. Three Mile Island: A Report to the Commissioners and to the Public, Nuclear Regulatory Commission Special Interest Group, Volume I, April 1979.

18. Owen, D., The Concept of Influence and Its Use in Structuring Complex Decision Problems, Stanford University, Doctoral Dissertation, Engineering-Economics Department, Stanford CA, November 1978.

## Section II

1. Rasmussen, N.C., Reliability Analysis Class Notes: 22.38, Spring, 1980.

2. Burdick, G.R. and Fussel, J.B., "On the Adaptation of Cause-Consequence Analysis to U.S. Nuclear Power Systems Reliability and Risk Assessment", Report V: A Collection of Methods for Reliability and Safety Engineering, Idaho National Engineering Laboratory ANCR-1273, UC-79h, April 1976.

3. Lambert, H., "Fault Tree Analysis: An Overview", UCRL-75904, Lawrence Livermore Laboratory, August 6, 1974.

4. Lambert, H., "Systems Safety Analysis and Fault Tree Analysis", UCID-16238, Lawrence Livermore Laboratory, May 9, 1973.

5. Apostolakis, G., "Probability and Risk Assessment: The Subjectivist Viewpoint and Some Suggestions", Nuclear Safety, Vol. 19, No. 3, May-June 1978, pp. 305-315.

6. General Principles for Reliability Analysis of Nuclear Power Generating Station Protection Systems, IEEE Trial-Use Guide, IEEE Std. 352-1972, ANSI N41.4, 1972.

7. Litai, D., A Risk Comparison Methodology for the Assessment of Acceptable Risk, Ph.D. thesis, MIT, Nuclear Engineering Dept., Cambridge MA, January 1980.

8. Green, A.E. and Bourne, A.J., Reliability Technology, Wiley-Intersciences, New York, 1972.

9. Rowe, W.D., An Anatomy of Risk, Wiley-Intersciences, New York, 1977.

10. Holt, P.G., Port, S.C., and Stone, C.J., Introduction to Probability Theory, Houghton Mifflin Co., Boston, 1971.

11. Efron, B., "Controversies in the Foundations of Statistics", Stanford University, Working Paper of the Statistics Dept., Stanford, 1976.

12. Howard, R.A., et al., Readings in Decision Analysis, Stanford Research Institute, Decision Analysis Group, Menlo Park CA 1976.

13. Bowker, A.H. and Lieberman, G.J., Engineering Statistics, Prentice-Hall, Inc., Englewood Cliffs NJ, 1972.

14. Spetzler, L.S. and Stael von Holstein, "Probability Encoding in Decision Analysis", Stanford Research Institute, Decision Analysis Group, Nov. 8-10, 1972.

15. Reactor Safety Study, WASH-1400, U.S. NRC, Washington DC 1975.

## Section III.A

1. Short-Term Lessons Learned, NUREG-0578, Nuclear Regulatory Commission, Washington DC, 1979.

2. Garrick, J.B., et al., Oyster Creek Probabilistic Safety Analysis, Main Report, August 1979: Section 5.2.2 "Reactor Protection System", pp.5-40 to 5-43; Section A.2.4.3 "A Prior Quantification", pp. A-201 to A-224.

3. Reactor Safety Study, WASH-1400, U.S. Nuclear Regulatory Commission, Washington DC, 1975.

4. "Anticipated Transients Without Scram for LWRs", NUREG-0460, Vol. 1, PB-279-384, U.S. Nuclear Regulatory Commission, Washington DC, April 1978.

5. Kimmins, A.D.C., "Anticipated Transients Without Scram: A Utilities Perspective", 25th Annual Winter Meeting, American Nuclear Society, San Francisco, November 1979.

6. Lellouche, G.S., "Anticipated Transients Without Scram", 25th Annual Winter Meeting, American Nuclear Society, San Francisco, November 1979.

7. Lellouche, G.S., "Anticipated Transients Without Scram", Nuclear Safety, Vol. 21, No. 4, July-August 1980.

8. "Failure of 76 of 185 Control Rods to Fully Insert During a Scram at a BWR", IE Bulletin No. 80-17, U.S. Nuclear Regulatory Commission, Office of Inspection and Enforcement, Washington DC, July 3, 1980.

9. Personal communication with Dresden plant personnel, August 1980.

10. Hanauer, Steven, Presentation on ATWS, Nuclear Safety Course, MIT, July 1980.

## Section III.B

1. "Analysis of the Three Mile Island-Unit 2 Accident", NSAC-1, Nuclear Safety Analysis Center, Palo Alto, California, July 1979.

2. Wooton, R.D., Denning, R.S., and Cybulkis, P., "Analysis of the Three Mile Island Accident and Alternative Sequences", NUREG/CR-1219, U.S. Nuclear Regulatory Commission, Washington, D.C., January 1980.

3. "TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations", NUREG-0578, U.S. Nuclear Regulatory Commission, Washington, D.C., July 1979.

4. Farrar, M.C., Buck, J.H., Quarles, L.R., "Memorandum and Order in the Matter of Vermont Yankee Nuclear Power Corporation", Docket-50271, Atomic Safety and Licensing Board, ALAB-217, U.S. Atomic Energy Commission, Bethesda, Maryland, July 11, 1974.

5. Slifer, B.C. and Peterson, T.G., "Hydrogen Flammability and Burning Characteristics in BWR Containments", NEDO-10812, General Electric, San Jose, California, April 1973.

6. Control of Combustible Gas Concentrations in Containment Following a LOCA, REG/G-1.7 (rev. 2), U.S. Nuclear Regulatory Commission, Washington, D.C., November 1978.

7. "Post Accident Venting", Procedure No. 5.4.6. (rev. 5), Pilgrim Nuclear Power Station, Boston Edison Company, Plymouth, Massachusetts, November 1979.

8. Wilson, R.M. and Slifer, B.C., "Hydrogen Generation and the General Electric Boiling Water Reactor", NEDO-10723, General Electric, San Jose, California, February 1973.

9. Vandenburgh, D.E., "CAD System Description", Letter to U.S. Nuclear Regulatory Commission, Vermont Yankee Nuclear Power Corporation, Rutland, Vermont, June 1, 1976.

10. "Hydrogen Generated in a Boiling Water Reactor", Docket No. 50249-89, Dresden Nuclear Power Station, Commonwealth Edison Company, Illinois, August 1970.

11. Keilholtz, C.W., "Hydrogen Considerations in Light-Water Reactors", ORNL-NSIC-120, Oak Ridge National Laboratory, Oak Ridge, Tennessee, February 1976.

12. Reactor Safety Study, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", Appendix VIII: Physical Processes in Reactor Meltdown Accidents, WASH-1400, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1975.

13. Helwig, D.R., "Peach Bottom Atomic Power Station Post-LOCA Combustible Gas Control", Letter to Carolyn Heising-Goodman, Philadelphia, Pennsylvania, March 19, 1980.

14. "Leaks Inside the Primary Containment", Procedure No. 2.4.14. (rev. 3), Pilgrim Nuclear Power Station, Boston Edison Company, Plymouth, Massachusetts, March 1979.

15. Personal Communication with Robert E. Sojka and Richard Branch, Vermont Yankee Nuclear Power Station, Vernon, Vermont, February 21, 1980.

16. "Technical Specifications", Final Safety Analysis Report, Vol. V, Docket No. 50271, Vermont Yankee Nuclear Power Corporation, Vernon, Vermont, March 1970.

17. "Technical Specifications", Docket No. 50293, Pilgrim Nuclear Power Station, Boston Edison Company, Plymouth, Massachusetts, March 1970.

18. Thomas, G., "Testimony at Hearings Before the Atomic Energy Commission on Containment Inerting in the Matter of Vermont Yankee Nuclear Power Corporation", Docket No. 50271, Bethesda, Maryland, July 1974.

19. "BWR Decay Heat Removal System Appraisal", EPRI-NP-81, Electric Power Research Institute, Palo Alto, California, August 1978.

20. Personal communication with Mr. David Musolf, Northern States Power Co., June 5, 1980.

21. Personal communication with Mr. Steven Rosen, Institute for Nuclear Power Operations, June 5, 1980.

22. Personal communication between Prof. N.C. Rasmussen and personnel at Northeast Utilities, June 5, 1980.

23. Personal communication with Mr. Kevin Holtzclaw, General Electric Co. Licensing Staff, June 9, 1980.

24. Personal communication with Mr. Edward Sawyer, Yankee Atomic Electric Co., June 5, 1980.

25. Apostolakis, G. and Kazarians, M., "The Frequency of Fires in Light Water Reactor Compartments", ANS/ENS Thermal Reactor Safety Meeting, Knoxville, TN, April 7-11, 1980.

Section III.C

1. Wooten, R.D., Denning, R.S. and Cybulkis, P., "Analysis of the Three Mile Island Accident and Alternative Sequences", NUREG/CR-1219, U.S. Nuclear Regulatory Commission, Washington, D.C., January 1980.

2. Nitti, D.A., "B&W Hydrogen Bubble Calculations", Babcock and Wilcox, Lynchburg, Virginia, March 29, 1979.

3. "Analysis of the Three Mile Island - Unit Two Accident", NSAC-1, Nuclear Safety Analysis Center, Palo Alto, California, July 1979.

4. "The Need for Change: The Legacy of TMI", Report of the President's Commission on the Accident at Three Mile Island, Washington, D.C., October 1979.

5. TMI-2 Lessions Learned Task Force Status Report and Short-Term Rècommendations, NUREG-0578, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1979.

6. Bone, W.A., Flame and Combustion in Gases, Longmans, Breen and Co., Ltd., London, 1927.

7. Slifer, B.C. and Peterson, T.G., "Hydrogen Flammability and Burning Characteristics in BWR Containments", NEDO-10812, General Electric, San Jose, California, April 1973.

8. Keilholtz, C.W., "Hydrogen Considerations in Light-Water Reactors", ORNL-NSIC-120, Oak Ridge National Laboratory, Oak Ridge, Tennessee, February 1976.

9. Shapiro, Z.M. and Moffette, T.R., "Hydrogen Flammability Data and Applications to PWR Loss-of-Coolant-Accidents", WAPD-SC-545, Bettis Plant, Pittsburgh, Pennsylvania, September 1957.

10. Sokolik, A.S., Self-Ignition Flame and Detonation in Gases, Israel Program for Scientific Translations, Jerusalem, Israel, 1963.

11. Strehlow, R.A., Fundamentals of Combustion, International Textbook Co., Scranton, Pennsylvania, 1968.

12. Shchelkin, K.I. and Troshin, Y.K., Gasdynamics of Combustion, Mono-Book Corp., Baltimore, Maryland 1965.

13. Moyle, M.P. and Churchill, S.W., Impact Pressures Developed in Hydrogen-Oxygen Detonations, Symposium on Shock Waves in Process Equipment, Chicago, December 8-11, 1957.

14. Lewis, L. and von Elbe, G., Combustion, Flames and Explosions of Gases, Academic Press Inc., New York, 1961.

15. Minkoff, G.J. and Tipper, C.F.H., Chemistry of Combustion Reactions, Butterworth and Co., London, 1962.

16. Reactor Safety Study, Appendix VIII: Physical Processes in Reactor Meltdown Accidents, WASH-1400, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1979.

17. Wooten, R.O., "Comparison of BWR Core Heatup Calculations", Batelle Memorial Institute, Columbus, Ohio, May, 1968.

18. Personal communication with Mr. B. Slifer, Yankee Atomic Electric Co., July 31, 1980.

19. Henry, A.F., Nuclear Reactor Analysis, MIT Press, Cambridge, MA, 1975.

Section III.D

1. Reactor Safety Study, WASH-1400 (NUREG-75/014), U.S. Nuclear Regulatory Commission (1975).

2. Personal communication with Prof. N. C. Rasmussen, MIT, March 1980.

3. Analysis of the Three-Mile Island Accident and Alternative Sequences, NUREG/CR-1219, Battelle Columbus Laboratories (1979).

4. Mitigation of Small-Break LOCAs in Pressurized Water Reactor Systems, NSAC-2, Nuclear Safety Analysis Center (1980).

5. Howard, R.A., Proc. of Fourth International Conf. on Op. Res., Wiley-Intersciences, New York (1966).

6. Apostolakis, G. and Mosleh, A., Nucl. Sci. and Engineering, 70, 135-149(1979).

7. Apostolakis, G., Kaplan, S., Garrick, B.J., and Duphily, R.J., Nucl. Eng. and Design, 56, 321-329 (1980).

8. Kaplan, S. and Garrick, B.J., Nucl. Tech., 44, 231-245 (1979).

9. North, D.W., Judd, B.R., and Pezier, J.P., "New Methodology for Assessing the Probability of Contaminating Mars", Stanford Research Institute, Palo Alto (1973).

10. Howard, R.A., Proc. of IEEE, 58, 5, 632-643 (1970).

11. Martz, H.F., Jr., Nucl. Sci. Eng., 72, 368 (1979).

12. Martz, H.F., Jr., Nucl. Sci. Eng., 74, 158 (1980).

13. Apostolakis, G. and Mosleh, A., "Reply to Comments on the Bayesian Method for Estimating Reactor Core Melt Frequencies", Manuscript No. 19-802, UCLA (1980).

14. This represents, we believe, a fairly "pro-industry" estimate of the likelihood of core melt aversion at TMI; others may argue this value for $P_{TMI}$ is too high.

15. In the authors' opinion, TMI was not a "near-miss" and perhaps can be categorized with the Brown's Ferry incident such that estimates of $P_{TMI}$ = .03-.10 seem reasonable.