NUREG/CR–5477

An Evaluation of the Reliability and Usefulness of External-Initiator PRA Methodologies

Prepared by R. J. Budnitz, H. E. Lambert

Future Resources Associates, Inc.

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW, Lower Level, Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Information Resources Management, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

DISCLAIMER NOTICE

NUREG/CR-5477

An Evaluation of the Reliability and Usefulness of External-Initiator PRA Methodologies

Manuscript Completed: May 1989
Date Published: January 1990

Prepared by
R. J. Budnitz, H. E. Lambert

Future Resources Associates, Inc.
2000 Center Street
Berkeley, CA 94704

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN D2506

TABLE OF CONTENTS

I. INTRODUCTION

I.A Need for This Project

The need that this project addresses can be succinctly stated as follows:

> This report, prepared to assist policy-level decision-makers, evaluates the extent to which each category of external-initiators PRA methodology produces reliable and useful results and insights, at its current state-of-the-art level.

I.B Background

The discipline of probabilistic risk analysis (PRA) has become so mature in recent years that it is now being used routinely to assist decision-making throughout the nuclear industry. This includes decision-making that affects design, construction, operation, maintenance, and regulation. Unfortunately, not all sub-areas within the larger discipline of PRA are equally "mature", and therefore the many different types of engineering insights from PRA are not all equally reliable.

In particular, the sub-discipline of external-initiator PRA analysis is relatively less mature and less reliable than the corresponding internal-initiators analysis. This is due predominantly to four causes:

- first, external-initiator analysis began in a serious way only about 1980, more than a half-decade after the first internal-initiators analysis of WASH-1400, and there are fewer full-scope external-initiator PRAs available, especially for external flooding and extreme winds --- as a consequence the methods are less mature;
- second, large uncertainties in certain aspects of external-initiators analysis lead to poorer numerical accuracy in the "bottom-line" core-damage and risk results;

- third, compared to internal-initiator analysis the number of practitioners is fewer, and the number of full-scope PRAs that include external initiators also fewer, so there is less opportunity for a broader community to have digested and re-digested the methods, models, data, and results --- this is true for both the hazard analysis methods and the fragility-analysis methods;

- fourth, problems continue to exist with some components of the methodologies used. These problems occur in analysis of every area, including analysis of earthquakes, internal fires, extreme winds, external floods, and transportation accidents.

Up until the last couple of years, these relative weaknesses in external-initiator PRA made many decision-makers, in both industry and the NRC, reluctant to use external-initiator PRA results. This was true despite several papers and reports pointing out that many features of the methodology were reasonably mature (Ref. NRC, 1983; Budnitz, 1984; NRC, 1984; Budnitz, 1986; Budnitz, 1987). The external-initiator analyses had developed a "bad reputation" in some quarters --- they were considered too uncertain, or too conservative, or supported by too little solid data to be of much use.

Recently, however, this picture has begun to change. There are several signs of this change:

- Almost all new full-scope PRAs accomplished with utility support in recent years have included external-initiators as an integral part.

- The draft of NUREG-1150 (Ref. NRC, 1987) was criticized for omitting external-initiators (Ref. Kastenberg, 1988; LeSage, 1988), and to address this criticism the final version of NUREG-1150 includes external-initiator analysis of two plants.

- Even though the IPEs (Individual Plant Evaluations) for external initiators will only be required at a later stage (Ref NRC/IPE GL, 1988), the NRC's proposed approach to resolving the "severe accident" issue for existing plants recognizes that external initiators must have an equal footing with internal initiators (Ref. NRC/SECY-88-147, 1988).

- The NRC's evolving policy for the regulation of advanced designs seems to be headed toward recognizing that external initiators should be considered on an equal footing (Ref. NRC Public Meeting on Future Reactors, 1988).

Despite this evolving change in how external-initiators PRAs are viewed, the fact is that all too many decision-makers continue to believe that external-initiator PRA results are too uncertain to be of much use. This opinion is prominent even among decision-makers who have now broadly accepted the usefulness of PRA methods more generally --- meaning PRAs based on internal-initiator analysis.

This project will assist decision-makers in understanding both the benefits and the limitations of external-initiator PRA. The project objective, stated next, addresses this point directly.

I.C Objective

The project's objective is, for each external-initiator category separately, to evaluate the reliability and usefulness of the insights available. Specifically, the evaluation addresses whether the results and insights emerging from current analyses are reliable and useful, and why --- and if not, why not.

I.D Categories of External Initiators

The five categories of 'external initiators' examined here are the following:

- earthquakes
- internal fires
- external floods
- extreme winds
- transportation accidents.

Internal fires are probably mis-categorized as "external initiators", since unlike the other categories of initiators that arise outside the plant, internal fires begin within the plant. Their mis-categorization is strictly an artifact of the history of PRA --- specifically, the "external initiators" category seems to have arisen historically to describe the class of common-cause initiators not considered in WASH-1400, the first PRA.

I.E The Audience for This Report

The audience for this report is policy-level decision-makers in the nuclear industry, the government (NRC, DOE, Congress, OMB, etc.), and the general public.

Unfortunately, the limitations that continue to exist in the external-initiator methodologies have convinced many safety

decision-makers that the insights available are not reliable and therefore not useful. Often, these decision-makers decide to give little or no weight to the results obtained, even though externally-initiated accident sequences typically account for 10% to 30% of the total core-damage frequency in most recent full-scope PRAs. A few recent items attest to this strong negative attitude:

- At a recent (August, 1987) NRC-sponsored symposium in Annapolis on the subject of external initiators, the IDCOR representative stated that external-initiators analysis of existing plants, in the context of the IPE, was not necessary, or at least of sufficiently low priority to justify being left out of the IPEs all together (Ref. LLNL/Annapolis, 1987). This opinion is apparently shared by many in the industry, although a gradual shift is underway.

- The recent NRC IPE (Individual Plant Evaluations) generic letter (Ref/ NRC/IPE GL, 1988) requires examining only internal initiators, and states that external-initiator IPE evaluations will be required only sometime later.

- The number of papers on external initiators at the recent PSA'89 international conference in Pittsburgh (Ref. PSA'89/Pittsburgh, 1989) was only about 4% of the total, all in only one session.

- In the key opening session of PSA'87 in Zurich (Ref. PSA'87/Zurich, 1987), in which top regulators from all of the principal countries spoke, there was no mention of external initiators. In the question-and-answer period, in response to a direct question from Dr. Budnitz, one top regulator stated that in his opinion the concern for external-initiator accidents was overstated, and the other top regulators on the panel seemed to agree fully.*

Recently, NRC has increased its attention to the overall issue of how external initiators should be regulated. The most visible manifestation of this is the appointment (December, 1987) of the

---

* That particular regulator stated that in his opinion, if someone walked in the back door of the lecture hall with the news that a core-damage accident had just occurred somewhere in the world, the last thing that would come to his mind would be that it might have been caused by an external initiator! If external initiators truly represent from 10% to 30% of core-damage frequencies at large LWRs, this opinion is ill-founded indeed.

"External Events Steering Group", whose charter includes providing an integrated approach to resolving a wide variety of current regulatory issues related to external initiators (Ref. NRC/EESG, 1987). The establishment of the EESG is a major step forward for NRC: if a set of integrated approaches to resolving the various issues can be developed it will surely be a major accomplishment.

Unfortunately, the underlying problem remains: all too many utility decision-makers, and all too many NRC regulatory staffers and other key decision-makers, still don't understand that these initiators can be very important, and still discount the insights available from PRA-type analysis.

I.F Technical Approach of this Study

It is important to note that this paper is not intended to be an in-depth technical review of the subject matter, but rather an in-depth evaluation of the reliability and usefulness of the results and insights from external-initiator PRA.

The technical approach builds on recent work accomplished under NRC support at Lawrence Livermore National Laboratory. LLNL Report NUREG/CR-5042, by C.Y. Kimura, R.J. Budnitz, and P.G. Prassinos (Ref. Kimura et al., 1987), provided a brief examination of each of the important external initiator categories from the perspective of their risk significance and what has been learned about them from various PRAs. The initiator categories covered in NUREG/CR-5042 are the same five that are evaluated in this project: earthquakes, internal fires, external flooding, extreme winds, and transportation accidents. This LLNL work provides the basis for the current project, along with Sandia's recently completed "Fire Risk Scoping Study" (Ref. Sandia/Fire Risk Scoping Study, 1988).

The technical approach here is to perform a more in-depth evaluation of what is known about external initiators. Each initiator is examined separately. The thrust is to identify and describe the principal aspects of the current state-of-the-art PRA methodology, what aspects are more robust and therefore provide the most reliable insights, what aspects are less robust and therefore provide less reliable insights, and why.

The product of the study is intended to be an evaluation of the PRA methodology for each external-initiator category. The evaluation concentrates on the sub-methodologies for each initiator (for example, for earthquakes these would be the hazard methodology, the response methodology, and the systems methodology), and on how these sub-methodologies are combined together to provide overall PRA results and insights.

Although the various sub-methodologies are all being used today

to perform PRA analyses, the evaluation reveals important limitations in aspects of many of them. Some of those limitations can be reduced or eliminated through performing trial analyses and sensitivity studies to gain further understanding. In other cases, reducing the limitations will require physical experimentation, extensive data-gathering, the building and testing of a complex computer-based phenomenological model, and so on.

I.G Definition of Terms

The terms "reliability", "usefulness", and "uncertainty" are used often in this report. These are all different, as follows:

The reliability of a PRA result describes how robust it is in the face of methodological approximations and incomplete underlying data. The concept is that a decision-maker can "rely" on the validity of the result if it is robust despite the shortcomings.

The usefulness of a PRA result describes how much use a safety decision-maker can make of it. In plain English, some results are simply more useful than others. Thus, it might be only moderately useful to identify a particular vulnerability per se, but much more useful to identify an easy remedy within the PRA analysis --- for example, a remedy involving a minor procedural change that, through PRA methods, can be shown to reduce one component of the core-damage frequency by several orders of magnitude. In this sense, intermediate PRA results (such as the results of an extreme-wind hazard analysis) tend to be less useful than final or bottom-line results, or of identified vulnerabilities in components or system configurations.

The uncertainty in a PRA result usually describes the numerical uncertainty in the result, but it could also describe a modeling uncertainty (such as an "either-or" uncertainty about whether a phenomenon actually occurs) or an applicability uncertainty (such as whether the underlying data used actually apply to the case being studied). One example of applicability uncertainty would be the common situation that no site-specific data for extreme flooding may exist, and the applicability of similar data at a different site may be suspect.

I.H References

Budnitz, 1984: R.J. Budnitz, "External Initiators in Probabilistic Reactor Analysis ---- Earthquakes, Fires, Floods, Winds", Risk Analysis 4, 323 (1984)

Budnitz, 1986: R.J. Budnitz, "Recent Developments in Methodology and Findings From Seismic PSA", paper presented at the meeting of the IAEA Technical Committee on Advances in Nuclear Power Plant Risk Analysis With Emphasis on External Events, Vienna (1986)

Budnitz, 1987: R.J. Budnitz, "Recent Developments in Methodology and Applications for Seismic PRA", paper published in proceedings of PSA'87 Symposium (see Ref. PSA'87/Zurich, 1987)

Kastenberg, 1988: W.E. Kastenberg et al., "Findings of the Peer Review Panel on the Draft Reactor Risk Reference Document, NUREG-1150", Lawrence Livermore National Laboratory, Report NUREG/CR-5113 (1988)

Kimura et al., 1987: C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", Report NUREG/CR-5042, Lawrence Livermore Laboratory (1987); Supplement 1 to same NUREG report, same title, by P.G. Prassinos (1988)

LeSage et al., 1988: L. LeSage et al., American Nuclear Society Special Committee on Reactor Risk Reference Document (NUREG-1150), "Initial Report of the Special Committee" (April 1988)

LLNL/Annapolis, 1987: Lawrence Livermore National Laboratory, "Severe Accident Policy Implementation External Events Workshop", sponsored by U.S. Nuclear Regulatory Commission, Annapolis, Maryland (August 1987)

NRC, 1983: J. Hickman et al., "PRA Procedures Guide": A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", Report NUREG/CR-2300, American Nuclear Society, Institute of Electrical and Electronic Engineers, and U.S. Nuclear Regulatory Commission (1983)

NRC, 1984: U.S. Nuclear Regulatory Commission, "PRA Reference Document", Report NUREG-1050 (1984)

NRC, 1987: U.S. Nuclear Regulatory Commission, "Reactor Risk Reference Document", Report NUREG-1150 (draft, 1987)

NRC/EESG, 1987: Two Memoranda, E.S. Beckjord (Director, RES) to L.C. Shao (EST, NRR), "External Events Steering Group", December 21, 1987 and May 31, 1988

NRC Public Meeting on Future Reactors, 1988: T.L. King, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, "Public Meeting to Discuss Plans to Develop Guidance for Implementation of Severe Accident Policy for Future Reactors", held in Rockville, Maryland (June 9, 1988)

NRC/SECY-88-147, 1988: U.S. Nuclear Regulatory Commission, Policy Paper, SECY-88-147, V. Stello to Commissioners, "Integration Plan for Closure of Severe Accident Issues" (May 25, 1988)

NRC/IPE GL, 1988: U.S. Nuclear Regulatory Commission, Generic Letter No. 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50.54(f)" (November 23, 1988)

PSA'87/Zurich, 1987: International Topical Conference on PSA and Risk Management, sponsored by European Nuclear Society and American Nuclear Society, Zurich (August, 1987)

PSA'89/Pittsburgh, 1989: International Topical Meeting on Probability, Reliability, and Safety Assessment, sponsored by American Nuclear Society and European Nuclear Society, Pittsburgh (April, 1989)

Sandia/Fire Risk Scoping Study, 1988: J.A. Lambright, S.P. Nowlen, V.F. Nicolette, and M.P. Bohn, "Fire Risk Scoping Study: Investigation of Nuclear Power Plant Fire Risk, Including Previously Unaddressed Issues", Report NUREG/CR-5088, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (1988)

II. INTERNAL FIRES

II.A Summary Evaluation

Because nuclear power plant PRAs have often identified accident sequences initiated by internal fires as among the important contributors to core-damage frequency, the analysis of fires cannot be neglected as a part of external-initiators PRA. Fortunately, the PRA analysis can be accomplished in stages, beginning with a screening stage to reduce the scope to a few critical locations for which a full-scope analysis is required.

This summary will provide an overview evaluation of the reliability and usefulness of the PRA methodology for studying internal fires. The main text below will support its summary statements.

1) How reliable and useful is the methodology for identifying and screening potential fire locations?

This initial identification and screening methodology can be competently accomplished using guidance that is routinely available in the fire PRA literature. Generally, uncertainties arising from this aspect are not a major contributor to overall uncertainty in the analysis. This is especially true insofar as this step tends to be accomplished using conservative screening criteria.

2) How reliable and useful is the methodology for analyzing the frequency of fire initiation in each fire location?

The existing nuclear-plant fire data base provides a good starting point for the determination of these fire-initiation frequencies. Because of the nature of the data base, the analyst must adapt or modify it for each specific configuration. There are different approaches to deal with this aspect. Often, considerable expert judgment is involved.

Even though expert judgment is an important element, this aspect of the fire PRA methodology is now mature, variations of it having been used in over two dozen individual analyses. Of course, numerical uncertainties continue to exist, and these can amount to factors of, say, plus-or-minus three or sometimes more for an individual initiation frequency. Nevertheless, when the uncertainties are accounted for properly, the reliability and usefulness of the results of this sub-methodology are high.

3) How reliable and useful is the methodology for analyzing fire growth and spread and barrier adequacy?

Fire growth calculations: The analytical capabilities used in modern PRAs are limited to only a few configurations. In almost all fire PRAs to date, the COMPBRN code has been used. The original code has been modified twice, the most recent version being COMPBRN III. The code was developed to calculate scenarios involving an oil fire beneath cable trays. The objective is to predict the time elapsed before the fire will damage or ignite the cabling or other critical equipment. The COMPBRN algorithms were selected originally for simplicity of use, and they employ approximations that are known to be adequate in only some configurations.

Several technical issues are still not analyzed as well as is needed, however. Sandia's recent Fire Risk Scoping Study discusses these thoroughly. Even though COMPBRN seems to have several limitations, the code has been of major benefit to analysts in understanding fire growth as a function of time for several crucial configurations (in particular for cabling). Although new and better codes are definitely needed to address some of the issues not well covered, it is fair to conclude that the available COMPBRN code can provide reasonable quantitative results on the time for fire growth, spread, and damage in a number of key analysis situations, provided uncertainties (often large) are accounted for and the results not taken too literally.

Barrier adequacy: The usual assumption made in PRA analysis is that fire barriers with a specific code rating (such as a 3-hour barrier) will live up to their time rating fully. The Sandia Fire Risk Scoping Study discusses some test evidence to the contrary but the situation is inconclusive, so the report recommends research to investigate this issue. This issue is still open. Significant barrier failure probability would have a major impact on calculated core-damage frequencies. The probability of barrier failure needs to be kept down in the 1% range or lower for the core-damage frequency to be acceptably small from this issue.

It is concluded that at present the assumption of full barrier adequacy is in partial doubt, although most barriers are undoubtedly adequate for their ratings. Concerning the PRA methodology, we conclude that it is fully capable of dealing with an assumed non-zero barrier failure probability.

4) How reliable and useful is the methodology for analyzing the effectiveness of fire detection and suppression?

Three individual issues will be evaluated separately here:

Detection and Alarm: Analysts often utilize the judgment of an experienced fire engineer to quantify the distribution of detection and alarm times for each specific scenario; the judgments, in turn,

are based on a data base for both automatic and human detection capabilities. As a rule, the time distribution for detection is known quite well for spaces equipped with automatic detectors, while the distribution is broader (known less well) for human detection except for continuously occupied rooms such as the main control room. Although the process is usually heavily judgmental, the analysis itself can be quite reliable.

Automatic Suppression: The data base supporting this part of the analysis is excellent, and an experienced analyst's results for this aspect should be very reliable.

Manual Suppression: Manual suppression can be either by an individual who is already occupying the room of fire origin, or by a fire brigade (formal or informal) responding to an alarm. There are several time durations involved, to be assessed individually and added up: the time from the alarm to the arrival of personnel in the room of fire origin, followed by the time duration to find the fire, the time duration to apply fire-suppression agents, and finally the time duration until the fire is controlled or extinguished. In a full-scope analysis each time duration is represented by a distribution. Some PRAs have used a fault tree to work out the failure of manual suppression.

In general the time durations can each be determined reasonably well. However, the distribution of the overall assessed duration from alarm to suppression can be quite broad because it is a convolution of several intermediate durations taken together.

5) How reliable and useful is the methodology for assessing component fragility and the probability of "failure"?

The definition of "failure" differs from component to component. Usually, this definition is embedded in the fire-growth-and-spread code.

For cabling, separate temperature thresholds for insulation burning and damage are usually used, although they are not known very well. For smaller fires or fires at some distance from the cabling, the sensitivity can be great. A time-at-temperature model for cable damage would in principle be an improvement, but has not often been used, in part because the added precision is thought not to be worth the extra effort in light of other unknowns in the analysis. For electrical cabinets, the entirely reasonable assumption is usually made that a cabinet fire will destroy all equipment within it unless promptly extinguished.

A few issues are not well enough understood, and therefore not well enough treated, in current fire PRAs. Among these are indirect or secondary effects such as the effects of smoke, low-level thermal exposures, and interactions among smoke, corrosive gases, water, and steam.

In general, and despite the above, the methodological problems with assessing component fragility and the probability of component "failure" are generally within the capability of fire analysts.

6) How reliable and useful is the methodology for identifying fire initiating events ?

The basic task here is to identify how each postulated fire can cause an "initiating event" (using the standard PRA definition of that term). The effort involves coupling the fire analysis with event trees similar to those used in the traditional PRA systems analysis. Generally, this part of the analysis is straightforward and quite reliable.

Conclusions about two other issues will be summarized here:

- Seismic-initiated fires: This issue is covered in more detail in the section on seismic-initiated accident analysis. A summary of the finding in the other section is that methods to identify seismic-initiated fires do exist and should be reasonably robust. This type of analysis has not been attempted in any full-scope PRA, but it seems to be a straightforward extension of existing methodologies and should not be difficult to accomplish.

- Accidents arising from inadvertent actuation of fire suppression equipment: This issue has never been studied in detail, and there is no existing methodology, so it is not known whether its contributions to overall plant risk are minor, or major, or in-between. Presumably, an analysis would require data on how suppression agents (water, various gases) affect equipment, especially electrical equipment.

7) How reliable and useful is the PRA systems-analysis methodology for fires?

The objective of the systems-analysis methodology is to calculate, for various scenarios, the probability of core damage. The fire systems-analysis methodology is, in its basic outline, a variant of the type of systems analysis that is now a well-developed, mature PRA discipline. While certain issues must be specially treated, including especially the issue of control-systems interactions, every aspect of the methodology is fully within the routine capability of PRA analysts. Therefore, we conclude that any competent PRA systems analyst can perform this work, with little special training and only the minimal guidance that is readily available and easily learned.

The issue of control-system interactions involves the possibility that a fire might damage control systems, including possibly a fire in a single electrical cabinet, and thereby prevent control of safe-

shutdown equipment from both the main control room and the remote shutdown panel. While the basic systems-analysis methodology for performing such a calculation exists, no thorough analysis has been done and the potential significance of this issue remains unclear.

8) How reliable and useful is the methodology for analyzing plant response and offsite releases and consequences for fires?

The methodology is, in its basic outline, identical to the type of level-2 and level-3 analysis that is now a well-developed, mature PRA discipline. The methods and data used are similar or identical. We conclude that any competent PRA level-2/level-3 analysis team can perform this work, with no special training. Given a postulated core-damage accident, the conditional probability of radioactive releases can be reliably determined and the consequences calculated.

9) How reliable and useful are "bottom-line numbers" for core-damage frequency and offsite risk, and the key risk insights?

The numerical uncertainties in the bottom-line results can be large (plus-or-minus an order of magnitude or more would not be uncommon). This is due to several factors in the various submethodologies, and the sources of uncertainty will differ from one plant to another. Despite the numerically large uncertainties, these uncertainties should generally not invalidate the key insights concerning potential fire-related vulnerabilities. These insights involve the identification of specific locations where fire initiation is likely, specific equipment that is susceptible to damage, fire barriers whose effectiveness needs reevaluation, fire-brigade training and access improvements, automatic or manual suppression capabilities, and so on.

One of the major lessons from fire PRAs is that an integrated examination of the plant, by a team including both fire engineers and systems engineers, can be of major benefit in identifying issues that neither type of expert could find alone. Another major benefit is that an integrated examination of fire in the context of the rest of the plant's safety functions and systems is crucial --- and PRA analysis can accomplish this integrated examination very well.

II.B Introduction

Small internal fires are a common occurrence at nuclear power stations: several occur each year, and it is widely recognized that there is always the potential for a minor fire to grow, spread, and damage crucial safety equipment. Fortunately, up to now the design and operational practices have been sufficient to keep the potential from becoming a reality. Also, significant research work has occurred in recent years, so that today there is a widely-used methodology for probabilistically analyzing potential fire-initiated accident sequences at nuclear power plants.

As discussed in the introductory chapter, this paper is not intended to be an in-depth technical review of the subject matter, but rather an in-depth evaluation of the reliability and usefulness of the results and insights from these analyses.

The technical approach here, which builds on recent work accomplished under NRC support at Lawrence Livermore National Laboratory (Ref. Kimura & Budnitz, 1987), is to perform a more in-depth evaluation. The thrust is to identify and describe the principal aspects of the current state-of-the-art PRA methodology, what aspects are more robust and therefore provide the most reliable insights, what aspects are less robust and therefore provide less reliable insights, and why.

This study will concentrate on the sub-methodologies and on how these sub-methodologies are combined together to provide overall PRA results and insights. There is a significant amount of guidance in the literature on the methods for performing fire PRAs, which can be referred to for more details (Ref. Fleming, 1979; Gallucci, 1980; Kazarians & Apostolakis, 1981; NRC, 1983; Brookhaven, 1985; Kazarians, Siu, & Apostolakis, 1985; Bohn & Lambright, 1988; Sandia, 1988).

II.C Description of the Methodology

The overall methodology for probabilistic evaluation of internal fires consists of eight sub-methodologies, which are combined together. (Of course, the division into these eight sub-methodologies is quite arbitrary. Some analysts use a different division.) The eight sub-methodologies to be discussed here are:

- the methodology for identifying and screening potential fire locations
- the methodology for analyzing the frequency of fire initiation in each fire location

- the methodology for analyzing fire growth and spread, including barrier adequacy
- the methodology for analyzing the effectiveness of detection and suppression
- the methodology for assessing component fragility and the probability of component "failure"
- the methodology for identifying fire initiating events
- the PRA systems-analysis methodology
- the PRA methodology for analyzing plant response and offsite releases and consequences.

No fire at any nuclear power plant has been sufficiently damaging to cause a core-damage accident, although the Browns Ferry fire in 1975 was a very serious event, possibly a "near miss" depending on how one defines that term. Even including the event at Browns Ferry, the experience with fire-initiated accidents taken as a whole is not sufficient to provide information for the analysis discussed here. The frequency of fire-initiated core damage can only be determined from calculations using data and tests coupled with models of what might occur in extremely unlikely situations.

II.D Evaluation of the Various Sub-Methodologies

In the next sub-sections, we will discuss and evaluate each of the eight sub-methodologies in turn.

II.D.1 Evaluation of the methodology for identifying and screening potential fire locations

Description of the Methodology: The purpose of this initial step is to develop an inclusive list of all the fire locations in the plant, and then to screen out those for which the potential for a fire to cause a core-damage event is considered minor. Usually, this step begins with the fire areas and fire zones delineated in the plant's safety analysis report, but often these zones and areas must be modified and/or subdivided, since fire zone boundaries in the SAR may not be suited for this analysis. In practice, this sub-methodology begins with paper screening, uses a plant walkdown to gather information, and ends with a list of locations carried forward for further analysis.

There are eight types of areas normally considered in this type of analysis: the control room, cable spreading rooms, diesel-generator rooms, the reactor building, the turbine building, the

auxiliary building, electrical switchgear rooms, and battery rooms. Of course, some plants do not have separate buildings or rooms that fit each of these categories.

The identification and screening work usually employs a screening criterion that narrows the emphasis to locations where multiple equipment could be compromised by a single fire, in particular several trains of redundant equipment. Usually, all equipment related to electrical distribution and power conversion are included, since these support functions are so important. A key aspect of this initial step is examination of cable routing for control, instrumentation, and power cables. Sometimes this can be very time consuming, especially for support-system cabling.

Because of the possible adverse effects of suppression systems, such as water damage, in the initial screening step these adverse effects are assumed as given. In the later systems analysis, it is necessary to examine each specific item of equipment in the affected room for this issue.

For each location not screened out, it is necessary to identify one or more fire scenarios to be carried forward for further analysis. The scenarios involve specific equipment possibly threatened, and including adjacent locations to which the fire might spread. Because further analysis will be done, this aspect of the fire methodology tends to be conservative and inclusive in its screening.

Evaluation of the Methodology: This identification and screening methodology can be competently accomplished using guidance that is routinely available in the fire PRA literature. Today, automated screening methods are available, using computer coding by location, to identify rapidly and easily the co-location of various equipment items by zone.

The key element in this work is the plant walkdown, which is one of the most important parts of the entire fire-PRA analysis. The walkdown provides specific information about configuration details, spatial relationships, fire-spreading openings and passageways, barriers, the transient-fuel situation, and so on. The walkdown also identifies those few situations where zone-to-zone barriers need to be given special attention by the analyst. Sometimes, the walkdown reveals that the original delineation into zones and areas is not appropriate for the subsequent analysis, so these must be modified.

Generally, this methodology is reliable, and uncertainties arising from it are not a major contributor to overall uncertainty in the analysis. This is especially true insofar as this step is accomplished using conservative screening criteria.

II.D.2 Evaluation of the methodology for analyzing the frequency of fire initiation in each fire location

Description of the Methodology: The objective of this aspect is to determine the frequency per year of fires for each important fire location carried forward from the initial identification/screening step. The data base used as a starting point is usually taken from actual fires in nuclear power plants, and today there are several data compilations available (Ref. Kazarians & Apostolakis, 1982; Dungan & Lorenz, 1983; Wheelis, 1986). The principal fire types are in cabling, in electrical cabinets, in lubricating oil within equipment, welding fires, and fires from transient fuels such as trash and cleaning compounds.

Of course, there are different ways to compile and display this data base, but this isn't the central difficulty, which is that the data base taken as a whole is often not directly applicable to a specific fire location being studied, even when scaled by floor area, which is one common approach to plant-specific adaptation. As an example, while the data base contains several fires in or near, say, turbine-generators, the layout of the individual turbine-generator at a given plant may not be represented well. Another example is control room fires, which the data base shows occur almost exclusively in electrical cabinets, so that the floor area of a control room is not the correct variable.

Based on the above, we see that the analyst must adapt or modify the numerical initiation frequency taken from the data base for the specific configuration. Different approaches exist to deal with this aspect. Bayesian updating of the generic data base with plant-specific information can be useful in some applications (Ref. Iman & Hora, 1989). Sometimes, area-ratio methods are used for this partitioning, but often these must be adapted further, based partly on information gathered in the walkdown such as local fuel loading, whether the specific site is controlled for fires, and how often it is occupied. If stringent administrative controls are in place --- for example, limiting acetone to 1/2-liter quantities in spill-proof safety cans, with sign-in and sign-out procedures --- this should be accounted for.

Inevitably, uncertainties arise in the numerical values used, and these will propagate through to uncertainties in the bottom-line results of the full analysis. Often, considerable expert judgment is involved, which requires review by others to assure its validity.

Evaluation of the Methodology: The existing data base provides a good starting point for the determination of fire-initiation frequencies. The adaptation of that data base to each individual configuration involves using an analytical approach, plus expert judgment, to account for individual location-specific issues.

This aspect of the fire PRA methodology is now mature, variations of it having been used in over two dozen individual analyses. Of course, numerical uncertainties continue to exist, and these can amount to factors of, say, plus-or-minus three or sometimes more for an individual initiation frequency. Nevertheless, when the uncertainties are accounted for properly, the reliability and usefulness of the results of this sub-methodology are high.

II.D.3 Evaluation of the methodology for analyzing fire growth and spread and barrier adequacy

Two different aspects (analysis of fire growth-and-spread and barrier adequacy) will be discussed separately in the paragraphs below.

Fire growth calculations: In principal, it is feasible to calculate (at least approximately) the phenomena accompanying the growth of any fire. In practice, the analytical capabilities used in modern PRAs are limited to only a few configurations.

Typically, the analyst may postulate only a very small number of types of fires --- sometimes only two, such as a one-gallon and a ten-gallon oil fire on the floor of a compartment --- as surrogates for all fires. Also, because fires that damage electrical and control cabling are usually found to be the most serious type, the code-development effort has concentrated on modeling how cable fires ignite, burn, spread, and cause damage.

In almost all fire PRAs to date, the COMPBRN code (Ref. COMPBRN, 1983) has been used. The original code has been modified twice, and the most recent version, which removes many of the conservatisms and corrects some of the known errors in the earlier versions, is called COMPBRN III (Ref. COMPBRN III, 1985). The code was developed to calculate scenarios involving an oil fire beneath cable trays. It uses a zone model with three zones: the flame and plume, a hot gas layer, and the ambient surroundings. Models predict the growth of the fire and the thermal environment at various locations around the fire as a function of time.

The objective is to predict the time elapsed before the fire will damage or ignite the cabling (or other critical equipment which can also be modeled). The COMPBRN algorithms were selected originally for simplicity of use, and they employ approximations that are known to be adequate in only some configurations. Furthermore, the original models used were purposely conservative in some ways, although recent versions have attempted to improve the code by removing some of these conservatisms.

Because fire PRAs have used COMPBRN or its derivatives almost exclusively, we will concentrate here on that code. However, a

detailed discussion of COMPBRN --- indeed, of any fire-growth code --- will not be attempted here, since the recent widely-available critique by Sandia has done a thorough job in this regard (Ref. Sandia, 1988). Instead, a summary evaluation of the state of fire-growth code capability will be offered, as follows:

While COMPBRN seems to have limitations in a number of aspects, the code has been of major benefit to analysts in understanding fire growth as a function of time for several crucial configurations (in particular for cabling). If exercised carefully, COMPBRN can provide many insights into fire growth phenomena, such as how sensitive the growth time is to various assumptions concerning pilot-fire fuel amount, location, and area extent; assumed damage threshold models for cabling or other equipment; the role of hot gas layers in spreading heat within a zone or between connected zones; the sensitivity of the results to fire locations adjacent to walls or ceilings; the spread of fires or hot gases down passageways and ducting; and the like.

COMPBRN is a very valuable piece of the overall fire-PRA methodology, despite its limitations. New and better codes are definitely needed to address some of the issues not well covered. However, it is fair to conclude that the available COMPBRN code can provide reasonable quantitative results on the time for fire growth, spread, and damage in a number of key analysis situations, provided uncertainties (often large) are accounted for and the results not taken too literally. To put this point another way, while the code does have limitations, these need not invalidate the insights obtained, in the hands of a competent analyst aware of the code's limitations.

Several technical issues are still not analyzed as well as is needed, however: Sandia's report discusses these thoroughly. Examples include whether cable ignition and damage depend not only on a temperature threshold but also on a parameter related to critical heat flux or critical energy flux; the mass burning rate correlation; and how flame height is treated.

Barrier adequacy: The usual assumption made in PRA analysis is that fire barriers with a specific code rating (such as a 3-hour barrier) will live up to their time rating fully. This seems to be a reasonable assumption on its face, assuming that the barrier is intact at the time of the fire. (If not --- if, for example, a fire door is left open or a fire damper fails with a certain non-zero probability --- the assumption is invalid. The PRA methodology can treat this case properly by assuming that the two separated compartments are linked, and this case can be treated properly in fire PRAs.)

In Sandia's Fire Risk Scoping Study (Ref. Sandia, 1988), the issue of barrier adequacy is addressed in some detail. It is

pointed out that the US fire-code test for barriers is usually performed with equal pressures on both sides of the barrier, or sometimes with a slight negative pressure on the fire side of the barrier, to aid in exhausting the combustion gases during the test. However, during actual fires the heat in a small compartment can build up to produce a slight positive pressure on the fire side. Whether the barriers used in nuclear plants will all remain fully adequate in this situation is not known. The Sandia report discusses some test evidence to the contrary but the situation is inconclusive, so the report recommends research to investigate this issue. The most likely area of concern cited by Sandia is wall penetration seal systems for cables, which can exhibit cracking.

This issue is still open. Sandia's report points out that if barrier failure occurs with 10% probability this would have a major impact on calculated core-damage frequencies, because all too often the failure would compromise two redundant trains in adjacent zones that must be separated to assure an effective safe-shutdown capability. The probability of barrier failure needs to be kept down in the 1% range or lower for the core-damage frequency to be acceptably small from this issue.

Based on this discussion, we conclude that at present the assumption of full barrier adequacy is in partial doubt, although most barriers are undoubtedly adequate for their ratings. Concerning the PRA methodology, we conclude that it is fully capable of dealing with an assumed non-zero barrier failure probability.

II.D.4 Evaluation of the methodology for analyzing the effectiveness of detection and suppression

It is useful to think about detection and suppression as processes that compete with fire growth and spread, in a race over short time periods after the fire starts. If suppression wins, the fire is put out without causing damage. If growth and spread win and suppression loses the race, the fire will lead to damage.

There are several individual issues here, which must be discussed and evaluated separately:

Detection and Alarm: For a given fire scenario, fire detection and alarm can be automatic (if detectors exist and operate), or local (by plant personnel directly observing the fire), or remote (using secondary indications such as off-normal indications on instruments). In PRAs, all three detection methods are analyzed as stochastic phenomena characterized by a probabilistic time distribution. Analysts often utilize the judgment of an experienced fire engineer to quantify the distribution of detection and alarm times for each specific scenario; the judgments, in

turn, are based on a data base for both automatic and human detection capabilities. For local human detection, the fraction of time that an area is occupied must be estimated. For remote detection, the analysis must usually rely heavily on judgment. As a rule, the time distribution for detection is known quite well for spaces equipped with automatic detectors, while the distribution is broader (known less well) for human detection except for continuously occupied rooms such as the main control room.

Because the analyst's knowledge of the various detection and alarm times is represented by several distributions, the times are treated probabilistically as weighted random variables. Mathematical methods exist for combining properly the various time distributions (Ref. Apostolakis, Arueti, Kazarians, and Siu, 1989). Developing the distributions is often done by starting with generic information and modifying it based on specific local issues.

Although the process of estimating detection and alarm times is usually heavily judgmental, the analysis itself can be quite reliable if care is taken and if the judgments are reviewed by other experts.

Automatic Suppression: Given activation of an automatic suppression system, the analyst must work out how quickly the fire will be suppressed. Considerations include the distance from the automatic system to the fire, the size and configuration of the room, the fire's character, and so on. Usually, the time from detection to automatic suppression will be very short, unless the automatic system fails to function on demand (a probability that must be worked out by the PRA systems analyst). The data base supporting this part of the analysis is excellent, and an experienced analyst's results for this aspect should be very reliable.

Manual Suppression: Manual suppression can be either by an individual who is already occupying the room of fire origin, or by a fire brigade (formal or informal) responding to an alarm. Because fire brigades differ significantly from one to the next power station (Ref. Sandia, 1988), it is necessary to perform a site-specific analysis. This will include consideration of the probability that the crew will be forced to abandon the main control room because of intense heat or smoke. In some recent PRAs this has been assumed to occur due to heat and smoke once in about every ten control-room fires that are not automatically suppressed (Ref. Sandia/1150 Ext. Events [draft], 1989; N-Reactor PRA [draft], 1989).

There are several time durations involved, to be assessed individually and added up. The first time duration is the time from alarm to the arrival of personnel in the room of fire

origin, followed by the time duration to find the fire, the time duration to apply fire-suppression agents, and finally the time duration until the fire is controlled or extinguished.

All of these time durations need to be determined, and in a full-scope analysis each is represented by a distribution. The set of time distributions is added up by a mathematical convolution, yielding the final result, the time duration from alarm to suppression (represented by a distribution).

The analysis of time duration from the alarm to the arrival of the fire brigade can be done quite well in most cases: the analyst must meet with the on-site fire-brigade and control-room personnel to learn how the specific alarm and response system operates. Finding the fire can be a problem if smoke and heat are dense, and especially if the fire brigade is constrained not to inundate the whole space because important safety equipment might be inadvertently damaged --- hence the time duration to find the fire can be difficult to assess. However, in general the time durations for finding the fire, applying the suppression agents, and controlling the fire can each be determined reasonably well.

Some PRAs have used a fault tree to work out the failure of manual suppression, to account systematically for the several factors, including failure of detectors and alarms, failure of personnel to suppress the fire with manual carbon-dioxide extinguishers or local water, and so on. This fault tree can provide an overall probability of complete failure to suppress the fire. Of course, complete failure is equivalent to the "time for suppression" being very long, and if for a given scenario this time duration is known to be much longer than the time it takes for the fire to grow, spread, and cause damage, the fault tree isn't worth developing.

Assuming successful execution of all suppression steps, the results of the analysis, in the form of distributions of time durations, should be reliable. However, the distribution of the <u>overall</u> assessed duration from alarm to suppression can be quite broad (meaning that our knowledge of it is sometimes not very precise) because it is a convolution of several intermediate durations taken together.

<u>II.D.5 Evaluation of the methodology for assessing component fragility and the probability of component "failure"</u>

<u>Description of the Methodology:</u> The definition of "failure" differs from component to component. Usually, this definition is embedded in the fire-growth-and-spread code, in the sense that a critical temperature or time-at-temperature relation is incorporated as the code works out the time elapsed for the fire to

grow to a defined "size".

For cabling, insulation and damage thresholds are usually used, although they are not known very well. For large cable fires, the thresholds are not as critical as for smaller fires, because the fire grows so rapidly that the time-to-threshold analysis is insensitive. For smaller fires or fires at some distance from the cabling, the sensitivity can be great: indeed for some cases the differences can be between a pilot fire that never ignites the cabling to one that ignites only after a very long time to one that ignites rather quickly.

A time-at-temperature model for cable damage would in principle be an improvement over a simple temperature-threshold model, but has not often been used, in part because the added precision is thought not to be worth the extra effort in light of other unknowns in the analysis, such as just how much pilot-fire fuel will exist, where the pilot fire is located, the combustion efficiency, the surface burning rate, and so on.

For electrical cabinets, the entirely reasonable assumption is usually made that a cabinet fire will destroy all equipment within it. Fire damage to such cabinets is usually considered to occur shortly after a fire begins, unless promptly extinguished by personnel immediately available. The methodology issue with cabinet fires is in a major way the problem of working out the likelihood that the fire will spread to involve more than one cabinet before it can be suppressed.

There are a few issues that are not well enough understood, and therefore not well enough treated, in current fire PRAs. Among these are indirect or secondary effects such as the effects of smoke, low-level thermal exposures, and interactions among smoke, corrosive gases, water, and steam. It is widely held that the principal effects of smoke will be on electronic circuits or electrical items containing exposed conductors such as motors. However, detailed effects are poorly understood. Insofar as any of these issues might significantly affect a given fire scenario, the current analysis methodology is to that extent inadequate.

In general, and despite the above, the methodological problems with assessing component fragility and the probability of component "failure" are generally within the capability of fire analysts, even though uncertainties continue to be significant for some types of fires, such as the smaller fires with slower growth times or the larger fires whose damage potential is partly from spreading hot gas layers and smoke.

II.D.6 Evaluating the methodology for identifying fire initiating events for the systems analysis

Description of the Methodology: The basic task here is to identify how each postulated fire can cause an "initiating event" (using the standard PRA definition of that term) with the potential for evolving into a core-damage accident sequence of concern. The effort involves coupling the fire analysis with event trees similar to those used in the traditional PRA systems analysis. The "initiating event" is typically a signal, either automatic or manual, that triggers a reactor scram due to one or another off-normal condition initiated by the fire.

Evaluation of the Methodology: Generally, this part of the analysis is straightforward, although in all fairness it inevitably involves certain assumptions about how the specific operator response (or automatic response) will evolve. Although these assumptions are uncertain in detail --- therefore, they can lead to uncertainties in the "bottom-line" core-damage-frequency results --- the overall impact of these uncertainties is usually not a key issue in fire PRA analysis, and this aspect of the methodology is generally quite reliable.

There are two issues only peripherally related to initiating-event identification that will be discussed here. They are placed here in part because it isn't clear just where else they might fit in this overall discussion about fire-initiated accidents:

- Seismic-initiated fires: There is a reasonable likelihood that very large earthquakes might initiate a fire that, combined with earthquake-caused damage, could compromise plant safety. This issue is covered in more detail in the section on seismic-initiated accident analysis. A summary of the finding in the other section is that methods to identify seismic-initiated fires do exist and should be reasonably robust. It would be necessary to combine the methods used in seismic-failure analysis with the methods for fire analysir to obtain an overall analysis of this type of event. This has not been attempted in any full-scope PRA, but the analysis seems to be a straightforward extension of existing methodologies and should not be difficult to accomplish.

- Accidents arising from inadvertent actuation of fire suppression equipment: If fire suppression equipment were to be actuated in the absence of a fire, this could damage equipment necessary for plant safety. (This problem could also arise if actuation because of a real fire were to damage other equipment outside the fire's influence.) Damage mechanisms are several and will not be discussed here. This issue has never been studied in detail, so it is

not known whether its contributions to overall plant risk are minor, or major, or in-between. Presumably, an analysis of the effects of this issue would require data on how suppression agents (water, various gases) affect equipment, especially electrical equipment. There is no existing methodology for studying this issue probabilistically, although the structure of the analysis approach seems straightforward to set down. However, the details of such an analysis seem difficult to work out.

II.D.7 Evaluation of the PRA systems-analysis methodology for fire-initiated accident sequences

The objective of the systems-analysis methodology is to calculate, for various scenarios, the probability of core damage.

Discussion of the Methodology: The systems-analysis work is very similar in broad outline to ordinary PRA systems analysis. It uses the same tools and types of data, and the same way of setting up the analysis and solving it numerically.

The approach involves developing event trees to follow postulated accident sequences through from initiating event to conclusion, and fault trees to establish quantified success-failure values for the branch points. One general consideration involves support systems: often, a major contributor to fire-initiated accident sequences is the damage to support systems (power, service water, instrument air, room cooling, and so on) that cause multiple subsequent failures of diverse equipment. If the support-system matrix has been developed previously, in the context of an internal-initiators PRA study, it can be used directly. Otherwise it must be worked out here. In any event, the analysis of support system dependencies is standard and very reliable and very useful.

Another general consideration involves the contributions of non-fire-caused failures. Such failures can be due to random failures-on-demand of needed equipment, equipment out-of-service for maintenance, operator errors, and the like. The quantification of these failure probabilities is accomplished using standard PRA methods, and is very robust.

PRAs often analyze and take credit for operator recovery actions to restore a failed piece of equipment or substitute another. While the methodology for this aspect is sound, in some fire scenarios recovery must be carefully analyzed because the fire can impede access to certain areas.

Control system interactions: One key issue in the systems analysis is control systems interactions, a subject that has recently been treated in detail in Sandia's Fire Risk Scoping

Study (Ref. Sandia, 1988). The issue is the possibility that a fire can damage control systems, and thereby prevent control of safe-shutdown equipment from both the main control room and the remote shutdown panel. Specifically, if multiple control and actuation functions in the main control room were to be damaged by a fire spreading through one or more control cabinets, it is possible that control from the remote panel might also not be feasible, depending on the damage.

One particular aspect of this issue is the possibility that a fire in a single cabinet might compromise safety, which would be an important vulnerability to identify. A thorough analysis of this topic would require working out the likelihood and time elapsed for a fire to cause the failures of concern, taking into account local suppression, any operator recovery actions available, and the probability of specific non-fire-related random failures.

The Sandia report's conclusions appear to be two-fold: First, it was found (Ref. Sandia, 1988, page 22.6) that "current fire protection criteria applied to US nuclear reactor plants require an extensive search for both simple and complex interactions between remote shutdown systems and the control room. Uncertainties still exist in that detailed analyses of specific hardware and human interactions have not been performed. A comparison between primary reliance on preventative control logic and manual actions is one area of potential risk significance, which requires further examination."

The second Sandia conclusion emerges from a trial study of the LaSalle reactor configuration* as a test case. Two critical control room cabinets were studied, the ECCS Panel and the Electrical Distribution Panel. Assuming that both panels would be totally consumed by a postulated fire and that all components within each panel would fail in the most undesired state, two potential accident sequences were identified. The scoping analysis found that the failure combinations leading to accident sequences always include a random (non-fire-related) failure in combination with fire-related failures. That is, fire-induced failures alone would not be enough. With various conservative assumptions, the core-damage-frequency calculated from these scenarios is in the significant range --- about comparable with core-damage-frequency results from sequences involving other initiators. Whether this scoping analysis at LaSalle has generic significance isn't known, of course, but on its face it does point out the need for additional attention in fire PRAs to the

---

* LaSalle is a modern two-unit station in Illinois with dual BWR/5 reactors with Mark-II containments, designed by General Electric Company and owned by Commonwealth Edison Company. Each unit generates 1100 MWe.

control-system-interaction issue. Fortunately, the basic systems-analysis methodology for performing such a calculation exists, although its application to a specific control-room configuration may require extensive effort.

Evaluation of the Methodology: The fire systems-analysis methodology is, in its basic outline, a variant of the type of systems analysis that is now a well-developed, mature PRA discipline. While certain issues must be specially treated, including especially the issue of control-systems interactions, every aspect of the methodology is fully within the routine capability of PRA analysts. Therefore, we conclude that any competent PRA systems analyst can perform this work, with little special training and only the minimal guidance that is readily available and easily learned.

II.D.8 Evaluation of the Consequence/Release Sub-Methodology

Discussion of the Methodology: The objective of the consequence/release methodology is to calculate, for various fire-initiated sequences associated with various probabilities of core damage, the conditional probability that the accident will evolve into a "radiological release" scenario.

Each scenario requires separate treatment, depending on which items of safety equipment have been damaged by the fire, which other equipment has failed from other causes, which operator actions have contributed to the damage or mitigated the situation, and so on. The probability of a radiological release, and its size, also obviously depend on how phenomena develop both within the primary system and in containment after core damage begins; how ex-plant radiological dispersion phenomena develop; and how sheltering and evacuation are accomplished.

Evaluation of the Methodology: The consequence/release methodology is, in its basic outline, identical to the type of level-2 and level-3 analysis that is now a well-developed, mature PRA discipline. The methods and data used are similar or identical, including the use of containment event trees (or accident-progression event trees, as they are now often called) and offsite consequence analysis codes. We conclude that any competent PRA level-2/level-3 analysis team can perform this work, with no special training.

II.E Evaluation of the "Bottom-Line" Results for Core-Damage Frequency and Offsite Risk, and the Key Risk Insights

As the discussion above has implied, the numerical uncertainties in the bottom-line results can be large (plus-or-minus an order of magnitude or more would not be uncommon). This is due to several factors covered in the preceding subsections.

The principal engineering insights depend in part on the numerical "bottom-line" results but not in a major way. These insights involve the identification of specific locations where fire initiation is likely, specific equipment that is susceptible to damage, fire barriers whose effectiveness needs reevaluation, fire-brigade training and access improvements, automatic or manual suppression capabilities, and so on. The configurations of interest can include contributions from non-fire-related failures and human errors, which can be identified using the full power of the PRA approach to do an integrated analysis.

Despite the numerically large uncertainties in the "bottom-line" numbers, these uncertainties should generally not invalidate the key insights concerning potential fire-related vulnerabilities. Conversely, if no vulnerabilities are identified and the plant is judged to be well designed against fire-initiated accidents, this conclusion should be quite robust despite any numerical uncertainties in the bottom-line numbers.

One of the major lessons from fire PRAs is that an integrated examination of the plant, by a team including both fire engineers and systems engineers, can be of major benefit in identifying issues that neither type of expert could find alone. Another major benefit is that an integrated examination of fire in the context of the rest of the plant's safety functions and systems is crucial --- and PRA analysis can accomplish this integrated examination very well.

II.F References

Apostolakis, Arueti, Kazarians, and Siu, 1989: G. Apostolakis, S. Arueti, M. Kazarians, and N. Siu, "Fire Risk Analysis", Contribution to IAEA "Manual for PSA and Its Application in Safety Decisions", International Atomic Energy Agency, Division of Nuclear Safety (to be published, 1989)

Bohn and Lambright, 1988: M.P. Bohn and J.A. Lambright, "Recommended Procedures for Simplified External Event Risk Analyses", Report NUREG/CR-4840, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (draft report, 1988)

Brookhaven, 1985: M. McCann, J. Reed, C. Ruger, K. Shiu, T. Teichmann, A. Unione, and R. Youngblood, "Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, Volume 2, Brookhaven National Laboratory and U.S. Nuclear Regulatory Commission (1985)

COMPBRN, 1983: N.O. Siu, "COMPBRN - A Computer Code for Modeling Compartment Fires", NUREG/CR-3239, University of California at Los Angeles and U.S. Nuclear Regulatory Commission (1983)

COMPBRN III, 1988: V. Ho, N. Siu, and G. Apostolakis, "COMPBRN III - A Fire Hazard Model for Risk Analysis", Fire Safety Journal 13, 137 (1988)

Duncan and Lorenz, 1983: K.W. Duncan and M.S. Lorenz, "Nuclear Power Plant Fire Loss Data", Report EPRI-NP-3179, Electric Power Research Institute (1983)

Fleming et al., 1979: K.N. Fleming, W.J. Houghton, and F.P. Scaletta, "A Methodology for Risk Assessment of Major FIres and its Application to an HTGR Plant", Report GA-A15402, General Atomic Company (1979)

Gallucci, 1980: R. Gallucci, "A Methodology for Evaluating the Probability for Fire Loss of Nuclear Power Plant Safety Functions", Rensselaer Polytechnic Institute, Ph.D. thesis (1980)

Iman and Hora, 1989: R.L. Iman and S.C. Hora, "Bayesian Methods for Modeling Recovery Times with an Application to the Loss of Offsite Power at Nuclear Power Plants", Risk Analysis 9, 25 (1989)

Kazarians and Apostolakis, 1981: M. Kazarians and G. Apostolakis, "Fire Risk Analysis for Nuclear Power Plants", Report NUREG/CR-2258, University of California at Los Angeles and U.S. Nuclear Regulatory Commission (1981)

Kazarians and Apostolakis, 1982: M. Kazarians and G. Apostolakis, "Modeling Rare Events: The Frequencies of Fires in Nuclear Power Plants", Society for Risk Analysis, "Workshop on Low-Probability/High-Consequence Risk Analysis", Arlington, Virginia, June 15-17, 1982, published by Plenum Press, New York (1984)

Kazarians, Siu, and Apostolakis, 1985: "Fire Risk Analysis for Nuclear Power Plants: Methodological Developments and Applications", Risk Analysis 5, 33 (1985)

Kimura and Budnitz, 1987: C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", Report NUREG/CR-5042, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1987). Supplement 1 to the same NUREG report, same title, covering seismic issues, is by P.G. Prassinos (1988)

N-Reactor PRA, 1989 (draft): M. P. Bohn et al., "N-Reactor External Events Probabilistic Risk Assessment" (draft version, no report number yet), Sandia National Laboratories and Westinghouse Hanford Company (1989)

NRC, 1983: J. Hickman et al., "PRA Procedures Guide": A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", Report NUREG/CR-2300, American Nuclear Society, Institute of Electrical and Electronic Engineers, and U.S. Nuclear Regulatory Commission (1983)

Sandia, 1988: J.A. Lambright, S.P. Nowlen, V.F. Nicolette, and M.P. Bohn, "Fire Risk Scoping Study: Investigation of Nuclear Power Plant Fire Risk, Including Previously Unaddressed Issues", Report NUREG/CR-5088, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (1988)

Sandia/1150 Ext. Events [draft], 1989: J.A. Lambright, M.P. Bohn, S.L. Daniel, J.J. Johnson, M.K. Ravindra, P.O. Hashimoto, M.J. Mraz, and W.H. Tong, "Analysis of Core Damage Frequency: Peach Bottom Unit 2 External Events", Report NUREG/CR-4550, Revision 1/Volume 3, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (draft version, 1989)

Wheelis, 1986: W. T. Wheelis, "Users Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base", Report NUREG/CR-4586, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (1986)

III. EARTHQUAKES

III.A Summary Evaluation

Almost every full-scope PRA that has examined earthquake-initiated accidents has found that this category represents one of the important initiator groups. Occasionally, one of the earthquake-initiated sequences is among the few largest contributors to core-damage frequency and/or to offsite risk. Usually the sequences identified are very plant-specific in character, such that the specific vulnerability would probably not exist at any other plant, even another similar plant. Sometimes the issue is site-related, and sometimes it is design-related.

Given this background, it is obvious that no full-scope PRA can be considered complete without an examination of earthquakes.

This summary will provide an overview evaluation of the reliability and usefulness of the PRA methodology for studying earthquakes. The full text below will support the summary statements in this opening evaluation.

1) How reliable and useful is the seismic hazard methodology?
The "hazard methodology" analyzes for the frequency of earthquakes of various sizes at a given site, and the spectral shapes of the motion from these earthquakes. The methodology has four steps (see Figure III-1). A fair characterization is that each of the steps is straightforward to describe, but difficult to implement.

The four-step approach begins with a seismicity assessment, to delineate and characterize the seismic sources. The second step involves determining the earthquake recurrence relationship, which is usually expressed in terms of an annual frequency as a function of magnitude for each source or source zone. For both of these two steps, because the historical earthquake record is at best incomplete, and because except for very recent events the earthquakes have not been properly measured by good instruments, much judgment is necessary.

The third step is associating a motion vs. distance relationship with each magnitude. Usually, acceleration (in terms of peak ground acceleration or local spectral acceleration) is chosen as the motion parameter, even though it is an imperfect measure --- in fact, no single parameter can be other than an imperfect measure. There are two principal issues here, choosing an attenuation model and a ground response spectral shape. For the eastern U.S. the strong-

motion attenuation information is usually absent, so theoretical models are often used, although based in part on western-U.S. data and insights which are not always applicable.

Selecting a ground response spectral shape is also uncertain. In PRAs for eastern-U.S. sites, a standard broad-band spectral shape normalized to the zero-period acceleration value has usually been used. However, if much soil amplification is present, a site-specific spectrum should be developed.

The ultimate product of the hazard assessment is the "hazard curves" themselves, typically in terms of the annual frequency of exceedance vs. a motion parameter like peak ground acceleration. It is important to note that embedded implicitly in the hazard-curve presentation is a specific spectral shape used in the earlier parts of the analysis.

All of the four above steps are easy to describe broadly. However, as mentioned, their implementation leads to major uncertainties. The crucial problem is that the data available are not sufficient to differentiate among a large number of reasonable models developed by experts approaching this analysis problem from different perspectives. That is, reasonable experts differ in their assessments, and selecting which expert is correct is difficult.

Both the NRC and EPRI hazard projects have used the approach of eliciting expert opinion in structured ways that attempt to account for the wide divergence of opinion without either suppressing minority views or overemphasizing them. How the elicitation of expert opinion has been accomplished apparently has some influence on the outcome of the assessments, although this issue is also not clearly understood. Suffice it to say that, from the perspective of a decision-maker, a legitimate and wide divergence of opinion among experts cannot but be taken on its face as genuine "uncertainty" in the best meaning of that term. The fact that different models can lead to PRA core-damage-frequency calculations differing by more than a factor of 10 is simply a manifestation of the current state-of-the-art in the discipline of seismic hazard assessment.

2) How reliable and useful is the local-ground-motion and building-motion methodology? This phase of the analysis is generally quite well developed, although when specific situations are being analyzed there do remain uncertainties due to random variability and incomplete knowledge.

The analyst usually starts with a family of earthquake motions, either time histories or another characterization, that are postulated to arrive at the local site from the source. As a set, the time histories are intended to capture variability in the source. Usually, several different earthquake "sizes" are calculated. The objective is to work out the local motion at the location of each

significant item (equipment items and structures) necessary for the safety of the power station.

For items located at different elevations, either above or below grade, it is necessary to develop what are known as floor spectra, using a structural model of the building. This part of the analysis begins with determining the ground response frequency spectrum at the site. Usually, generic broad-band spectra have been used in PRAs, and this should be acceptable, provided they are applicable to local soil conditions. If the local soil produces much amplification, the analyst should develop a site-specific response spectrum.

If structural foundations are on rock or stiff soil, their motions should be the same as for the free field. On soft soil, the soil-structure coupling can change both the frequencies and the amplitudes of the motion entering the building. In developing realistic floor spectra, it is typical to use linear dynamic analysis for the structure, and then to account for non-linear effects by estimating the inelastic energy absorption capacity of each component, so that the response for the equipment item represents the floor spectrum modified to account for how each equipment item responds in frequency space.

For all of these analyses, it is especially important for the analyst not to take as necessarily correct the models used in the design, since these may contain conservatisms or other errors which would not be a realistic representation of behavior in an actual earthquake.

As a summary of the state-of-the-art, it is a fair conclusion that while uncertainties are certainly present in this aspect of the analysis, from both variabilities and modeling approximations, the analytical approaches for the several topics are all generally well-developed and robust in the hands of experienced analysts.

3) How reliable and useful is the walkdown methodology? Among seismic-PRA analysts, the plant walkdown is considered to be almost the most crucial aspect. Among the most important benefits of the walkdown is the interaction that occurs among the systems analysis team, the seismic-capacity analysis team, and the utility staff. This is one of the major lessons learned in the past few years.

Another crucial benefit of the walkdown is that the seismic-capacity team can determine, for each important item (structure or equipment), whether that item is "typical" of its generic category, or somehow atypical or even unique. Still another benefit is the opportunity for the systems-analysis team to understand just how the operating crew has been trained to carry out its tasks, especially during emergencies.

The methodology for seismic-PRA walkdowns is now very mature.

be guidance is sufficiently detailed, and the number of teams that have accomplished an excellent walkdown is large enough, that a new team should have no difficulty in learning the approaches that work best. In summary, this aspect should be very reliable and very useful.

4) How reliable is the failure-mode and fragility methodology for earthquakes? The seismic fragility methodology calculates the capacity of individual structures and equipment items, and from that capacity the "fragility curve" for each item and the correlations among these.

Before capacity can be determined, "failure" must be defined, for both structures and equipment items. The definitions are highly individualized for specific equipment items, and the assignments must be made with the advice of a competent systems analyst. This aspect of the methodology is generally a robust and reliable part of the seismic-PRA methodology.

The fragility of a component is defined as the conditional frequency of its failure as a function of a response parameter, usually an acceleration parameter, such as peak ground acceleration or local spectral acceleration. A family of "fragility curves" is generated, typically characterized mathematically by lognormal expressions (for calculational convenience even though lognormals don't represent the data in the tails), anchored to median values and using various uncertainty parameters to capture both variability from randomness and uncertainty from lack of knowledge.

To develop a family of fragility curves, the analyst can use test data, data from real earthquake experience, and/or analysis. For a structure, analysis is usually used, since structures are all so individualized and since they are more amenable to calculation given a determination of the important failure mode(s). For equipment, reliance on test and experience data is the common approach, because there are now extensive data compilations in existence, including extensive experience data.

Some important items of equipment are now known to be generically quite rugged. This knowledge is embedded in a set of screening tables for seismic capacity that can be found in the NRC and EPRI seismic margin reports.

Despite major progress in our understanding, some uncertainties remain for many items of equipment. Specifically, there are still many unknowns, or differences among approaches, or different ways to interpret the underlying data --- so that different analysts will produce different capacities and fragility curves for the identical equipment item.

An illustration of this is the recent comparison among four expert analysts of their calculations for five specific items: a large storage

tank, a contactor for a motor starter, a starting air tank, a heat exchanger, and a block wall. The calculated median capacities differed, from the highest to the lowest of the experts, by factors in the range of about 1.5 for most of the components. (For a typical eastern-U.S. site, the hazard curve frequencies differ by factors of about 3 when the acceleration differs by a factor of about 1.5, so if a single component completely dominates a given sequence, core-damage frequency would vary by a factor of about 3). The lesson from this comparison is that the determination of seismic fragility curves, even by the most qualified experts, will still result in non-negligible differences.

We conclude that there is still some variability in the calculation of fragility parameters for items of equipment such as those cited in the test comparison study. This variability propagates through to modest uncertainties in the bottom-line risk results such as core-damage frequency. Therefore, while we conclude that the fragility estimates are reasonably good for many purposes, such as identifying the few important contributors at a plant, it is important not to take the numerical fragility values as implying too much accuracy.

5) How reliable and useful is the systems-analysis methodology? The objective of the systems-analysis methodology, given which equipment is damaged by the earthquake (typically with a probability distribution), is to determine which core-damage accident sequences may result, and the core-damage frequencies for each.

The systems-analysis work is broadly similar to traditional PRA systems analysis for internal initiators, and is within the technical capability of any competent PRA systems analyst, with no special training. It uses the same tools and types of data, and the same way of setting up the analysis and solving it numerically. There are only a few special issues: correlations among failures, relay chatter, design and construction errors, and operator response.

The problem of analyzing correlations among earthquake-induced failures can sometimes be difficult, especially for co-located equipment. Typically, the assumption is made of complete correlation in the response for nearby and similar equipment subject to the same floor motion. However, different equipment types, even if located in close proximity, are usually assigned only minor if any response correlation.

The problem for the analyst is that there is only very limited experimental information, from either testing or actual earthquakes, upon which to rely. Therefore, while the methodology for coping with correlations is well-developed, the underlying knowledge is typically inadequate. The usual fallback approach is to perform a sensitivity analysis, to obtain a measure of the uncertainty in the final results.

Whenever the accident sequences of concern involve components for which correlation might or might not be large, this issue is one of the important sources of uncertainty in the overall analysis.

The seismic-PRA methodology does not systematically take into account possible design and construction errors. The only consolation for the analyst (and the decision-maker) is that these omissions are directly parallel to possible similar omissions in the rest of PRA.

Recently, the relay-chatter issue has received significant attention. While the earliest seismic PRAs did not examine this issue, today an acceptable methodology does exist for treating it properly. Furthermore, the issue should not be ignored, because it certainly has a potential for contributing significantly to the overall seismic risk.

It seems likely that, during and after a strong-motion earthquake, operator response without error should be substantially degraded. However, this issue does not have as much effect on the results of PRAs as might be thought at first, principally because in PRAs no credit is usually allowed for operator control actions during the early minutes after a large earthquake. Based on this, the general consensus is that the operator-response aspect of the methodology, while not as strong as ultimately desired, is as robust (more-or-less) as the approach for operator error analysis used in internal-initiators PRA studies.

6) How reliable and useful is the consequence/release methodology? The objective of the seismic-PRA consequence/release methodology is to calculate, for various earthquake "sizes" associated with various probabilities of core damage, the conditional probability that the accident will evolve into a "radiological release" scenario. This conditional probability differs from one postulated core-damage accident sequence to the next. Therefore, each sequence requires separate treatment.

It is important that the analysis team consider a few special issues, such as the possibility that the earthquake may affect containment integrity, and the effect on emergency evacuation of possible extensive damage offsite, such as to roads, buildings, and bridges, or widespread panic among the public.

The consequence/release methodology is, in its basic outline, a variant of the type of level-2 and level-3 analysis that is now a widely used PRA discipline. While a few issues must be specially treated, we conclude that any competent PRA level-2/level-3 analysis team can perform this work, with no special training.

7) How reliable and useful are "bottom-line numbers" for core-damage frequency and offsite risk, and the key risk insights? The numerical uncertainties in the bottom-line results can certainly be large (plus-or-minus more than one order of magnitude or more is common). This is due to several factors in the various sub-methodologies, but dominantly due to the uncertainty in the hazard evaluation. The uncertainty in the fragility estimates per se contributes smaller amounts to the overall uncertainty. Perhaps the other major source of possible uncertainty would arise when several components must fail together to cause the accident sequence, and the correlations among them are not understood well --- the differences between assuming full correlation and zero correlation can also amount to about an order of magnitude difference in core-damage frequency in some cases.

Despite the numerically large uncertainties, these uncertainties should generally not invalidate the key insights concerning potential earthquake-related vulnerabilities. These insights include the identification of specific equipment and structural weaknesses, including weaknesses in components and systems not specifically designed or qualified against earthquakes, specific non-seismic-initiated failures and human errors that may contribute to a key sequence, the possible role of post-earthquake operator recovery actions, whether a given sequence would have major or only minor offsite-release consequences, and (almost most importantly) the places where support-system vulnerabilities can compromise different safety systems in subtle ways.

One of the major lessons from seismic PRAs is that an integrated examination of the plant, by a team including both seismic-capacity engineers and systems engineers, can be of major benefit in identifying issues that neither type of expert could find alone.

Another major benefit is that an integrated examination of seismic issues in the context of the rest of the plant's safety functions and systems is crucial --- and PRA analysis can accomplish this integrated examination very well.

III.B Introduction

There have been well over two dozen full-scope PRAs that have studied potential earthquake-initiated accidents at nuclear power stations. The methodology has been exercised by several different groups of practitioners and is considered mature. Nevertheless, and despite continuing research work to develop and improve the various parts of the methodology, some aspects remain difficult to accomplish well and introduce considerable numerical uncertainties into the bottom-line results.

As discussed in the introductory chapter, this paper is not intended to be an in-depth technical review of the subject matter, but rather an in-depth evaluation of the reliability and usefulness of the results and insights from these analyses. The reader who desires instruction on the methodology can find extensive guidance in the literature, including both full-scope PRA methods and so-called abbreviated methods (Ref. SSMRP, 1981; NRC, 1983; Bohn, 1984; Shieh, 1985; Brookhaven, 1985; Ravindra & Banon, 1985; Reed, 1985; SSMRP, 1986; RMIEP, 1987; Bohn & Lambright, 1988). In addition, guidance on seismic-margin methodologies is available from both NRC (Ref. Budnitz/Margins, 1985; Prassinos/Margins, 1986) and EPRI (Ref. EPRI/Margins, 1988). Some of this guidance on margins methods is directly applicable to PRA analysis.

The technical approach here, which builds on recent work accomplished under NRC support at Lawrence Livermore National Laboratory (Ref. Kimura, Budnitz & Prassinos, 1987) and recent reviews of the methodology (Ref. Budnitz, 1984; Ravindra, 1984; Ravindra, 1985; Budnitz, 1986; Budnitz, 1987), is to perform a more in-depth evaluation. The thrust is to identify and describe the principal aspects of the current state-of-the-art PRA methodology, what aspects are more robust and therefore provide the most reliable insights, what aspects are less robust and therefore provide less reliable insights, and why.

This study will concentrate on the sub-methodologies and on how these sub-methodologies are combined together to provide overall PRA results and insights. There is significant amount of guidance in the literature on the methods for performing seismic PRAs, which can be referred to for more details (Ref. NRC, 1983; Brookhaven, 1985; Bohn & Lambright, 1988).

II.C Description of the Methodology

The overall methodology for probabilistic evaluation of earthquake effects consists of six sub-methodologies, which are combined together. (Of course, the division into these six sub-methodologies is quite arbitrary. Some analysts use a different division.) The six sub-methodologies to be discussed here are:

- the seismic hazard methodology for calculating the frequency of earthquakes of various "sizes" at a given site and characterizing the motion parametrically
- the seismic local-ground-motion and building-motion methodology for working out the motion at a given location on the site or within buildings, given the incoming earthquake motion

- o the walkdown methodology that guides the essential plant walkdown that is at the heart of seismic PRA
- o the seismic failure mode and fragility methodology for calculating the capacity of individual equipment and structures, and from that capacity the "fragility curve" for each item and the correlations among these
- o the seismic-PRA systems analysis methodology
- o the seismic-PRA methodology for analyzing plant response and offsite releases and consequences.

There has never been an earthquake sufficiently damaging to any operating U.S. nuclear power station to cause safety concerns. By far the largest recent earthquake worldwide was the very destructive Armenian earthquake of November, 1988 which however produced only minor ground motion at an operating Soviet two-unit PWR reactor station near the strong-motion zone. However, preliminary and unpublished reports indicated that there was no significant damage (Ref. Yanev, 1989). While there are anecdotal reports of earthquakes near reactors in Japan, there is little published literature about any effects.

The published historical record is therefore not adequate for the analysis discussed here. The frequency of earthquake-initiated core-damage accidents can only be known from calculations, using a combination of real-earthquake data, test data, models of various phenomena, and systems analysis.

III.D Evaluation of the Various Sub-Methodologies

In the next sub-sections, we will discuss and evaluate each of the six sub-methodologies in turn.

III.D.1 Evaluation of the seismic hazard methodology

The "hazard methodology" is the methodology for analyzing for the frequency of earthquakes of various sizes at a given site, and the spectral shapes of the motion from these earthquakes. For most sites, outside of highly active regions like coastal California, very large earthquakes have never been experienced (or at least never been recorded). Therefore, it is necessary to develop the so-called hazard curves based on analysis of inferences, sometimes scarce and controversial, from the data that do exist.

Description of the Methodology: The methodology for developing the seismic hazard for a given site is well developed in outline, at least in principle, although as shall be seen below there is

still much uncertainty in the detailed results. The outline of the four-step approach is shown in Figure III-1, taken from the PRA Procedures Guide (Ref. NRC, 1983). Here, we will not discuss the four steps in detail, since the literature is so extensive, including a very clear description in the Brookhaven procedures guide (Ref. Brookhaven, 1985). However, a fair characterization is that each of the steps is straightforward to describe, but difficult to implement.

Two very large research projects have recently been completed to develop seismic hazard information for all of the various nuclear-reactor sites in the U.S., with emphasis on the regions east of the Rocky Mountains where well-known faults are not usually the principal source of seismicity. One research project has been supported by the NRC (Ref. Bernreuter, 1989) and the other by EPRI (Ref. EPRI/Hazard, 1989).

The four-step approach begins with a seismicity assessment, to delineate and characterize the seismic sources. The sources are typically either identified faults, or point sources, or areas called source zones in which it is assumed that the occurrence of earthquakes is spatially uniform. Usually, the different zones are assumed to be independent of each other. The assessment involves gathering and evaluating data about the various known sources near the site, for example from micro-seismicity records, geological and geotechnical information, surface topographic evidence, and so on.

Unfortunately, except in the western U.S. or other regions where well-characterized faulting dominates, the process that gives rise to earthquakes is not well understood, so it is necessary to postulate models, such as tectonic models coupled with other regional and local features. A model can then be transformed into a set of seismic sources for use in the subsequent analysis. Models range from the simple to the complex, and can incorporate factors such as possible interactions among sources, time dependence or independence of earthquake occurrence due to stress buildup, and inferences from similarity with other regions.

The second step is determining the earthquake recurrence relationship, which is usually expressed in terms of an annual frequency as a function of magnitude (as shown in stylized form in Figure III-1), for each source or source zone. Factors to be considered include the historical seismic activity rate, the lowest magnitude of concern for the given source, the upper-bound magnitude that can be generated, the distribution of earthquake magnitudes, the depth of the source, the spatial distribution of energy release (point, short plane, extended plane), and so on.

As with the seismicity assessment, models by different experts can range from the simple to the complex. Because the historical

earthquake record is at best incomplete, and because except for very recent events the earthquakes have not been properly measured by good instruments, much judgment is necessary. For example, what is known best about large earthquakes many years ago is the damage that they caused, which is not easily transformed into a more scientific parameter like magnitude (which, itself, is only a rough approach to categorizing earthquakes).

Also, many models would predict at least a finite chance of earthquakes of essentially infinite energy release, which is not physically correct, leading to the need for an upper-bound magnitude cutoff. Usually, various types of physical arguments are used, based on a variety of evidence, to determine this cutoff, and the evidence is usually difficult to interpret except in active areas like coastal California.

The next step (see Figure III-1) is associating a motion vs. distance relationship with each magnitude. Usually, acceleration (in terms of peak ground acceleration or local spectral acceleration) is chosen as the motion parameter, even though it is an imperfect measure --- in fact, no single parameter can be other than an imperfect measure.

There are two principal issues here, choosing an attenuation model and a ground response spectral shape. Sometimes, these two aspects are combined in a model that directly attenuates different frequencies differently. For some parts of the western U.S. the strong-motion earthquake records are extensive enough to provide actual data for attenuation modeling. For the eastern U.S. the strong-motion information is usually absent, so theoretical models are often used, although based in part on western-U.S. data and insights which are not always applicable. Issues to be considered include the effect of local transmission paths, fault rupture characteristics, and frequency dispersion.

Selecting a ground response spectral shape is also uncertain. In PRAs for eastern-U.S. sites, a standard broad-band spectral shape normalized to the zero-period acceleration value has usually been used in place of working out the spectral shape in a combined way with the attenuation model. However, if much soil amplification is present, a site-specific spectrum should be developed.

The final product of the hazard assessment, as shown in Figure III-1, is the "hazard curves" themselves, typically in terms of the annual frequency of exceedance vs. a motion parameter like peak ground acceleration. It is important to note that embedded implicitly in the hazard-curve presentation is a specific spectral shape used in the earlier parts of the analysis --- the results of the hazard methodology include both the hazard curves and the spectral shape(s).

In concluding this brief summary description of the hazard

methodology, it must be pointed out that a number of technical issues have not even been mentioned, because the summary has been intended mainly to introduce the various broad sources of information needed for seismic hazard analysis and why they are uncertain.

Evaluation: All of the above steps are easy to describe broadly. However, as mentioned, their implementation leads to major uncertainties. The crucial problem is that the data available are not sufficient to differentiate among a large number of reasonable models developed by experts approaching this analysis problem from different perspectives. The Brookhaven guide (Ref. Brookhaven, 1985) states the situation succinctly: "The development [of a seismic hazard model] is a product of scientific interpretation of uncertain and incomplete physical evidence on geological structures, tectonic processes, and seismicity." Therefore, reasonable experts differ in their assessments, and selecting which expert is correct is difficult.

Here we will not provide details on the specific issues on which the experts disagree --- the NRC and EPRI assessment reports should be referred to (Ref. Bernreuter,1989; EPRI/Hazard, 1989). Both the NRC and EPRI hazard projects have used the approach of eliciting expert opinion in structured ways that attempt to account for the wide divergence of opinion without either suppressing minority views or overemphasizing them. How the elicitation of expert opinion has been accomplished apparently has some influence on the outcome of the assessments, although this issue is also not clearly understood.

Suffice it to say that, from the perspective of a decision-maker, a legitimate and wide divergence of opinion among experts cannot but be taken on its face as genuine "uncertainty" in the best meaning of that term. The fact that different models can lead to PRA core-damage-frequency calculations differing by more than a factor of 10 is simply a manifestation of the current state-of-the-art in this discipline.

III.D.2 Evaluation of the seismic local-ground-motion and building-motion methodology

Discussion of the Methodology: This phase of the analysis is generally quite well developed, although when specific situations are being analyzed there do remain uncertainties due to random variability and incomplete knowledge.

In this phase, the analyst usually starts with a family of earthquake motions, either time histories or another characterization, that are postulated to arrive at the local site from afar (or, of course, perhaps from directly below the site). Usually, several different earthquake "sizes" are calculated, by

scaling the time histories up or down anchored to different zero-period accelerations. The objective is to work out the local motion at the location of each significant item (equipment items and structures) necessary for the safety of the power station.

Of course, some items are located on the ground at grade level, while others are at different elevations, either above or below grade. For these latter, it is necessary to develop what are known as floor spectra, for each elevation in each important building.

There are several individual issues here, each involving its own methodology. Because sites differ so much, not all of the issues will be relevant to every site. It is not the purpose of this discussion to cover the details of each aspect of the methodology: extensive discussion of the technical issues can be found elsewhere.

This part of the analysis begins with determining the ground response frequency spectrum at the site, which is a function of distance from the earthquake source, the size of the earthquake, and local subsurface (especially soil) conditions (Ref. Brookhaven, 1985). Usually, generic broad-band spectra have been used in PRAs, and this should be acceptable, provided they are applicable to local soil conditions. If the local soil produces much amplification, the analyst should develop a site-specific response spectrum (Ref. Bernreuter, 1987).

If structural foundations are on rock or stiff soil, their motions should be the same as for the free field. On soft soil, the soil-structure coupling can change both the frequencies and the amplitudes of the motion entering the building. For example, it is necessary to account for such factors as soil shear modulus and damping. Soil-structure interaction models (Ref. Johnson, Schewe, & Maslenikov, 1984; Shieh, 1985) are quite reliable if all of the relevant site factors have been considered. It is especially important for the analyst not to take as necessarily correct the models used in the design, since these may contain conservatisms or other errors which would not be a realistic representation of behavior in an actual earthquake.

Transmission of the motion within the structure must be determined, from the foundation to any given elevation and location. This entails the development of a structural model for the building, unless the analyst can rely on a model developed earlier, such as in the original design or for the safety analysis report. As elsewhere, it would not be correct for the analyst to use uncritically the floor response spectra found in the design analysis or safety report, since these will in all likelihood be highly conservative.

In developing realistic floor spectra, it is typical to use

linear dynamic analysis for the structure, and then to account for non-linear effects by estimating the inelastic energy absorption capacity of each component, so that the response for the equipment item represents the floor spectrum modified to account for how each equipment item responds in frequency space. The modifications account for several factors specific to each item such as damping and modal response combination --- all of which have variability which must be included in the analysis.

Earthquake variabilities are usually accounted for by using several time histories, each of which captures the correlations properly for itself; the set of time histories capture, as an ensemble, the variability from earthquake to earthquake. Guidance on carrying out this aspect can be found in several references (Ref. Bohn, 1984; Brookhaven, 1985; Kennedy, 1981), and discussion of a computer code specially developed for this analysis can be found in a Lawrence Livermore report that was part of their SSMRP project (Ref. Johnson/SMACS, 1981).

Evaluation: As a summary of the state-of-the-art, it is a fair conclusion that while uncertainties are certainly present in this aspect of the analysis, from both variabilities and modeling approximations, the analytical approaches for the several topics are all generally well-developed and robust in the hands of experienced analysts.

III.D.3 Evaluation of the walkdown methodology

Discussion of walkdown issues: Among seismic-PRA analysts, the plant walkdown is considered to be almost the most crucial aspect. A well planned and effectively executed walkdown can provide vital information about the plant configuration, specific spatial relationships, anchorages, and other features that cannot be found any other way --- and without which neither the seismic-capacity analyst nor the systems analyst can properly perform the required work.

Among the most important benefits of the walkdown is the interaction that occurs among the systems analysis team, the seismic-capacity analysis team, and the utility staff. These three groups should be working together throughout the seismic-PRA effort, but their interactions are most crucial during the walkdown, when each can assist the others in identifying the more important issues and screening out the less important. This is one of the major lessons learned in the past few years: the earliest seismic PRAs suffered because these interactions among analysts were insufficient, whereas today no seismic PRA would be considered competent without the significant analyst interaction that has become a central element of the walkdown.

Another crucial benefit of the walkdown is that the seismic-

capacity team can determine, for each important item (structure or equipment), whether that item is "typical" of its generic category, or somehow atypical or even unique. If it is judged to be "typical", then information from the broad class in which the item fits can often be used, eliminating the need for special analysis. If an "outlier" component or structure is identified, it can be given the special attention that it deserves.

Still another benefit of the walkdown is the opportunity for the systems-analysis team to understand just how the operating crew has been trained to carry out its tasks, especially during emergencies. This understanding is crucial to the development of correct event trees and fault trees.

The literature now contains excellent guidance on how to plan and carry out a walkdown (Ref. Brookhaven, 1985; Budnitz/Margins, 1985; Prassinos/Margins, 1986; EPRI/Margins, 1988). As an example, an extensive table in the Brookhaven guide (Table 9.3.5 in Brookhaven, 1985) is especially useful, since it provides a list, for almost every category of equipment, of what to look for and why.

Evaluation: The methodology for seismic-PRA walkdowns is now very mature. The guidance is sufficiently detailed, and the number of teams that have accomplished an excellent walkdown is large enough, that a new team should have no difficulty in learning the approaches that work best.

III.D.4 Evaluation of the seismic failure mode and fragility methodology

The seismic fragility methodology is the methodology for calculating the capacity of individual structures and equipment items, and from that capacity the "fragility curve" for each item and the correlations among these.

For each item, there are two different aspects of the analysis, the definition of "failure" and the determination of the fragility.

Discussion on determining "failure" modes: Before capacity can be determined, "failure" must be defined. For a structure it would usually be severe buckling or collapse that could compromise the safety equipment within, or collapse that could fall onto and damage equipment. "Failure" usually does not include minor structural damage. The decision about what constitutes "failure" must be made by the structural analyst on a case-by-case basis, with the advice of a competent systems analyst, and considering the specific safety equipment and safety functions that would be vulnerable. Sometimes more than one failure mode will be considered in the analysis. This aspect of the methodo-

logy, identifying structural failure modes, is quite reliable and useful. This is especially true if a conservative assignment of "failure" is adequate.

For an item of equipment, "failure" means the inability to perform its safety function --- inability of a valve to close or open, of a pump to pump, of a battery rack to provide DC power, and so on. Sometimes "failure" can involve a transient phenomenon with no lasting damage, such as relay chatter that affects other equipment functions. The definitions are highly individualized for specific equipment items, and as with structural failures must be assigned with the advice of a competent systems analyst.

Evaluation: Today, the assignment of failure definitions is generally a robust and reliable aspect of the seismic-PRA methodology. Guidance on this aspect can be found in the procedures guides.

Discussion on fragility analysis: The fragility of a component is usually defined as the conditional frequency of its failure as a function of a response parameter, which in seismic PRAs is usually an acceleration parameter, such as peak ground acceleration or local spectral acceleration. Usually, a family of "fragility curves" is generated, as described fully in the procedures guides (Ref. NRC, 1983; Brookhaven, 1985). These fragility curves are typically characterized mathematically by lognormal expressions, anchored to median values and using various uncertainty parameters to capture both variability from randomness and uncertainty from lack of knowledge (Ref. Kennedy, 1980; Kennedy & Ravindra, 1984).

A thorough discussion will not be presented here covering either the standard mathematical formulation or its pitfalls. Suffice it to say that the use of lognormal mathematics is known to be an erroneous approach in the tails of the lognormal distributions, even when the lognormal shape adequately describes the data in the main parts of the distribution. The lognormal is used mainly for its calculational convenience.

There are three sources of information that can be relied on to develop a family of fragility curves for an item: test data, data from real earthquake experience, and analysis. For a structure, analysis is usually used, since structures are all so individualized and since they are more amenable to calculation given a determination of the important failure mode(s).

For equipment, reliance on test and experience data is the common approach. There are extensive data compilations in existence now, too numerous even to list here as references. Good recent lists of data references are in the reference lists of the two NRC seismic margins reports (Ref. Budnitz/Margins, 1985; Pras-

sinos/Margins, 1986) and the EPRI margins report (Ref. EPRI/Margins, 1988).

Recently, the use of earthquake experience data to supplement test data has become common, and this has strengthened the ability of analysts to anchor their analyses to real-world experience. Also, there are enough practitioners doing this kind of analysis today that a variety of independent viewpoints are being brought to the analysis of equipment fragility.

One key outcome of this expanded activity is that some important items of equipment are now known to be generically quite rugged. This knowledge is embedded in a set of screening tables for seismic capacity, that can be found in the NRC and EPRI seismic margin reports (Ref. Prassinos/Margins, 1986; EPRI/Margins, 1988). Using these tables, analysts can screen out certain items as rugged provided that the various conditions are met for each individual item so that it qualifies as a member of the ensemble represented.

Despite the major progress, some uncertainties remain for many items of equipment. Specifically, there are still many unknowns, or differences among approaches, or different ways to interpret the underlying data --- so that different analysts will produce different capacities and fragility curves for the identical equipment item.

An illustration of this is the recent comparison (Ref. Kennedy, 1989) among four expert analysts of their calculations for five specific items: a flat-bottom vertical water storage tank, an auxiliary contactor for a motor starter in an older motor control center, a starting air tank, a component-cooling heat exchanger, and a cantilevered reinforced block wall. Specific design details and failure mode assumptions were provided as input. The approach was for the experts to do independent calculations first, then to compare and review the results to identify sources of differences, and finally to revise the calculations as appropriate. After the second round, the calculated median capacities differed, from the highest to the lowest of the experts, by factors in the range of about 1.5 for most of the components*. If the median of the four experts is considered as

---

* For the so-called "HCLPF (High-Confidence-of-Low-Probability-of-Failure) capacity" the ratio from highest to lowest among the experts was in the range of about 1.3 to 1.4. The HCLPF capacity is the capacity at the point on the fragility curve representing a 95% confidence of a 5% probability of failure, and is a figure-of-merit in seismic-margin reviews. Calculating HCLPF capacities is described in the seismic-margin-review literature (Ref. NRC/Margins, 1986; EPRI/Margins, 1988; and Kennedy, 1988).

a rough "best estimate", this means that the highest and lowest calculations by the experts differ by about ± 20% to ± 25%. (For a typical eastern-U.S. site, the hazard curve frequencies differ by factors of about 2 to 3 when the acceleration differs by factors of 1.3 to 1.5, so if a single component completely dominates a given sequence, core-damage frequency would vary by a factor of about 2 to 3.)

The lesson from this comparison is that the determination of seismic fragility curves, even by the most qualified experts, will still result in non-negligible differences, which can only be considered, for the purposes of overall PRA analysis, to be "uncertainty" in the best meaning of that term.

Evaluation: Based on the above discussion, we conclude that there is still some variability in the calculation of fragility parameters for items of equipment such as those cited in the test comparison study. This variability usually propagates through to modest uncertainties (but sometimes to significant uncertainties, especially where test data are limited) in the bottom-line risk results such as core-damage frequency.

Therefore, while we conclude that the fragility estimates are reasonably good for many purposes, such as identifying the few important contributors at a plant, it is important not to take the numerical fragility values as implying too much accuracy.

III.D.5 Evaluation of the seismic-PRA systems analysis methodology

The objective of the systems-analysis methodology is as follows: Given which equipment is damaged by the earthquake (typically with a probability distribution), the analyst must determine which core-damage accident sequences may result, and the core-damage frequencies for each.

Discussion of the Methodology: The systems-analysis work is broadly similar to traditional PRA systems analysis for internal initiators. It uses the same tools and types of data, and the same way of setting up the analysis and solving it numerically. The following paragraphs will point out a few special considerations.

Logically,* the analyst should begin with the results of the seismic fragility analysis, which will have determined which structures and equipment have been damaged by the postulated earthquake (as a function of earthquake "size" in terms of, say, peak ground acceleration, frequency, etc.). The systems analyst must then take into account issues such as the random (non-earthquake-caused) likelihood that other vital equipment might be out-of-service due to testing, maintenance, operator error, or failure; possible correlations among failures; and the procedures used by the operators, including their ability to recover certain earthquake-damaged or failed equipment, or to substitute other equipment, or to perform the needed function another way.

The systems analysis requires developing one or more accident sequence event trees, that include the various functions or systems needed for safe shutdown, possible operator prevention and recovery actions, and the like. The success-or-failure numerical values on the event-tree branch points are then worked out using either data or fault trees. If we assume that the analyst has access to a completed internal-initiators PRA, then direct use can be made of such vital information as the emergency procedures and the support-system matrix. (Support systems such as AC power, instrument air, service water, and so on support the vital front-line equipment.) Otherwise, the analyst must develop this information anew. If fault trees from an internal-initiator analysis are used, they must be modified somewhat to account for location correlations and to introduce different failure modes.

The outcome of the systems analysis is the numerical value of core-damage frequency (actually, a density function that captures uncertainties) for each of several (usually discrete) earthquake sizes.

There are four special issues to discuss here: correlations among failures, relay chatter, design and construction errors, and operator response.

Correlations among failures: The problem of analyzing correlations among earthquake-induced failures can sometimes be hard.

The usual assumption, which seems obviously appropriate, is that

---

* The term "logically" is used here because, in practice, the process is not quite as linear as described in this paragraph, but rather is much more iterative: the systems analysts and the seismic-capacity analysts will have been working together from the start to screen out certain potential issues, develop input information on others, and help each other to focus on the issues deemed important. There will have been several iterations in any well-designed seismic-PRA study.

the earthquake motion coming into the site will affect all buildings in a fully correlated way. However, at different locations in a building, and certainly in different buildings, this correlation is diluted by intervening factors. Typically, the assumption is made of complete correlation in the response for nearby and similar equipment subject to the same floor motion. However, different equipment types, even if located in close proximity, are usually assigned only minor if any response correlation. Furthermore, even high response correlation doesn't imply high capacity correlation, which would arise when, for example, two valves come from the same manufacturer and the same assembly line.

The problem for the analyst is that there is only very limited experimental information, from either testing or actual earthquakes, upon which to rely. Therefore, while the methodology for coping with correlations is well-developed (Ref. Ravindra, 1984; Reed, 1985), the underlying knowledge needed to perform the calculations is typically inadequate. The usual fallback approach is to perform a sensitivity analysis, for example assuming complete correlation and then complete independence and ascertaining what difference these two assumptions make. The difference is then taken as representing a measure of the uncertainty in the final results.

Care must be taken about correlations not only in the central values but in the uncertainties. If neither of two parameters is known well, but what little is known comes from the same data set, the correlation in the uncertainty can be high.

Whenever the accident sequences of concern involve components for which correlation might or might not be large, this issue is one of the important sources of uncertainty in the overall analysis. (Conversely, if a key sequence is dominated by a single failure, or by two failures of very different kinds --- a large yard tank together with a battery rack would be examples --- both response and capacity correlations should be minor and the sensitivity of the results also minor.)

To summarize, while the methodology for this aspect of the analysis certainly exists in an adequate form, the underlying data are often inadequate, so that uncertainties in the final PRA results can sometimes be important from the issue of correlation.

Relay chatter: The issue of relay chatter was not analyzed at all in the first several seismic PRAs (early 1980s). Instead, the assumption was made that all relay chatter was recoverable by the operating crew, which assumption is tantamount to assuming no chatter. Recently, however, this issue has received significant attention. An NRC-sponsored study of chatter at two power plants (Ref. Budnitz, Lambert, & Hill, 1987) demonstrated that if there is no operator recovery the chattering of relays could lead to

core-damage accident sequences with high annual frequencies. This study also developed and used a methodology for examining relay-chatter issues in the context of a full-scope PRA. The recent Diablo Canyon PRA (Ref. PG&E, 1988) included a thorough examination of relay chatter, which was found to be a significant issue in the study. Also, the currently ongoing seismic margin review at Plant Hatch, jointly undertaken by EPRI, NRC, and the utility has examined this issue thoroughly (Ref. Moore, Wooten, & Kassawara, 1988). Furthermore, the test data base on seismic capacities for relay chatter has become more and more extensive.

A summary of the relay-chatter issue as of today is that (1) an acceptable methodology does exist for treating it properly; and that (2) the issue should not be ignored, because it certainly has a potential for contributing significantly to the overall seismic risk.

Design and construction errors: The seismic-PRA methodology does not systematically take into account possible design and construction errors, except in the rare case that such an error may be identified during the walkdowns or the study of design drawings. This may seem like a serious flaw in the methodology. In actual fact, there is no way to know whether or not it is! The only consolation for the analyst (and the decision-maker) is that these omissions are directly parallel to possible omissions in the rest of PRA, such as in the analysis of internally-initiated accidents, where possible design errors affecting the configuration of systems are also not accounted for properly either. This is not an excuse, but rather a generic weakness of all PRAs. Of course, a rigorous pre-operational testing program should identify most of these errors.

Operator response: It seems likely that, during and after a strong-motion earthquake, the ability of control-room operators to perform their assigned tasks without error should be substantially degraded, due to high levels of stress and confusion. This issue has been examined recently (Ref. Budnitz, Lambert, & Hill, 1987), and a model has been proposed to account more effectively for possible high operator stress. However, this issue does not have as much effect on the results of PRAs as might be thought at first, principally because in PRAs the assumption is commonly made that no credit is allowed for operator control actions during the early minutes --- often for as long as a half-hour --- after a large earthquake. By that time, things should have settled down (literally and figuratively), so that the normal PRA methodology for analyzing operator errors should apply. Based on this, the general consensus is that the operator-response aspect of the methodology, while of not as strong as ultimately desired, is as robust (more-or-less) as the approach for operator error analysis used in internal-initiators PRA studies.

Evaluation of the Systems-Analysis Methodology: As mentioned briefly above, the seismic systems sub-methodology is, in its basic outline, a variant of the type of systems analysis that is now a well-developed, mature PRA discipline. While certain issues must be specially treated, every aspect of the methodology, including correlations, relay chatter, and operator response, is fully within the routine capability of PRA analysts. Therefore, we conclude that any competent PRA systems analyst can perform this work, with no special training and only the minimal guidance that is readily available and easily learned.

III.D.6 Evaluation of the seismic-PRA consequence/release methodology

Discussion of the Methodology: The objective of the seismic-PRA consequence/release methodology is to calculate, for various earthquake "sizes" associated with various probabilities of core damage, the conditional probability that the accident will evolve into a "radiological release" scenario.

This conditional probability differs from one postulated core-damage accident sequence to the next. Therefore, each sequence requires separate treatment, depending on which items of safety equipment have been damaged by the postulated earthquake, which operator actions have contributed to the damage or mitigated the situation, which equipment has failed from other (non-seismic) causes, and so on. The size of the release also obviously depends on how phenomena develop both within the primary system and in containment after core damage begins; how ex-plant radiological dispersion phenomena develop; and how sheltering and evacuation are accomplished.

It is important that the analysis team consider a few special issues, such as the possibility that the earthquake may affect containment integrity, either for the structure itself or, more likely, for the penetrations or other ways in which integrity can be compromised.

Also, if the earthquake has caused extensive damage offsite, such as to roads, buildings, and bridges, or widespread panic among the public, the effect of these issues on emergency evacuation must be assessed.

Evaluation of the Methodology: The consequence/release methodology is, in its basic outline, a variant of the type of level-2 and level-3 analysis that is now a well-developed, mature PRA discipline. The methods and data used are similar or identical, including the use of containment event trees (or accident-progression event trees, as they are now often called) and offsite consequence codes. While a few issues must be specially treated, we conclude that any competent PRA level-2/level-3

analysis team can perform this work, with no special training.

Because some of the special issues --- such as offsite damage and panic and their effect on evacuation --- are difficult and highly uncertain, the reliability and usefulness of the results can be significantly compromised. This is not a fault of the methodology per se, but rather a potential for the analyst to be incomplete in developing all of the issues fully.

III.E Evaluation of the "Bottom-Line" Results for Core Damage Frequency and Offsite Risk, and the Key Risk Insights

The numerical uncertainties in the bottom-line results can certainly be large (plus-or-minus more than one order of magnitude or more is common). This is due to several factors in the various sub-methodologies, but dominantly due to the uncertainty in the hazard evaluation. The uncertainty in the fragility estimates per se contributes smaller amounts to the overall uncertainty. Perhaps the other major source of possible uncertainty would arise when several components must fail together to cause the accident sequence, and the correlations among them are not understood well --- the differences between assuming full correlation and zero correlation can also amount to about an order of magnitude difference in core-damage frequency in some cases.

Despite the numerically large uncertainties, these uncertainties should generally not invalidate the key insights concerning potential earthquake-related vulnerabilities. These insights include the identification of specific equipment and structural weaknesses, including weaknesses in components and systems not specifically designed or qualified against earthquakes, specific non-seismic-initiated failures and human errors that may contribute to a key sequence, the possible role of post-earthquake operator recovery actions, whether a given sequence would have major or only minor offsite-release consequences, and (almost most importantly) the places where support-system vulnerabilities can compromise different safety systems in subtle ways.

One of the major lessons from seismic PRAs is that an integrated examination of the plant, by a team including both seismic-capacity engineers and systems engineers, can be of major benefit in identifying issues that neither type of expert could find alone.

Another major benefit is that an integrated examination of seismic issues in the context of the rest of the plant's safety functions and systems is crucial --- and PRA analysis can accomplish this integrated examination very well.

III.F References

Bernreuter, 1987: D.L. Bernreuter, J.C. Chen, and J.B. Savy, "Development of Site Specific Response Spectra", Report NUREG/CR-4861, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1987)

Bernreuter, 1989: D.L. Bernreuter, J.B. Savy, R.W. Mensing, and J.C. Chen, "Seismic Hazard Characterization of 69 Nuclear Plant Sites East of the Rocky Mountains", Report NUREG/CR-5250, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1989)

Bohn and Lambright, 1988: M.P. Bohn and J.A. Lambright, "Recommended Procedures for Simplified External Event Risk Analyses", Report NUREG/CR-4840, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (draft report, 1988)

Bohn, 1984: M.P. Bohn et al., "Application of the SSMRP Methodology to the Seismic Risk at the Zion Nuclear Power Plant", Report NUREG/CR-3428, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1984)

Brookhaven, 1985: M. McCann, J. Reed, C. Ruger, K. Shiu, T. Teichmann, A. Unione, and R. Youngblood, "Probabilistic Safety Analysis Procedures Guide", Report NUREG/CR-2815, Volume 2, Brookhaven National Laboratory and U.S. Nuclear Regulatory Commission (1985)

Budnitz, 1984: R.J. Budnitz, "External Initiators in Probabilistic Reactor Analysis ---- Earthquakes, Fires, Floods, Winds", Risk Analysis 4, 323 (1984)

Budnitz/Margins, 1985: R.J. Budnitz, P.J. Amico, C.A. Cornell, W.J. Hall, R.P. Kennedy, J.W. Reed, and M. Shinozuka, "An Approach to the Quantification of Seismic Margins in Nuclear Power Plants", Report NUREG/CR-4334, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1985)

Budnitz, 1986: R.J. Budnitz, "Recent Developments in Methodology and Findings From Seismic PSA", paper presented at the meeting of the IAEA Technical Committee on Advances in Nuclear Power Plant Risk Analysis With Emphasis on External Events, Vienna (1986)

Budnitz, 1987: R.J. Budnitz, "Recent Developments in Methodology and Applications for Seismic PRA", paper published in proceedings of PSA'87 Symposium, sponsored by American Nuclear Society and European Nuclear Society, Zurich (1987)

Budnitz, Lambert, and Hill, 1987: R.J. Budnitz, H.E. Lambert, and E.E. Hill, "Relay Chatter and Operator Response After a Large Earthquake: An Improved PRA Methodology with Case Studies", Report NUREG/CR-4910, Future Resources Associates, Inc., Berkeley, California and U.S. Nuclear Regulatory Commission (1987)

EPRI/Hazard, 1989: Electric Power Research Institute, "Probabilistic Seismic Hazard Evaluations at Nuclear Plant Sites in the Central and Eastern United States: Resolution of the Charleston Earthquake Issue", Report EPRI-NP-6395D (1989)

EPRI/Margins, 1988: NTS Engineering, RPK Structural Mechanics Consulting, Pickard Lowe & Garrick, Woodward Clyde Consultants, and Duke Power Company, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin", Report EPRI-NP-6041, Electric Power Research Institute (1988)

Johnson/SMACS, 1981: J.J. Johnson, G.L. Goudreau, S.E. Bumpus, and O.R. Maslenikov, "Seismic Safety Margins Research Program -- Phase I Final Report, SMACS [Seismic Methodology Analysis Chain with Statistics] (Project VIII)", Report NUREG/CR-2015 (Volume 9), Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1981)

Johnson, Schewe, and Maslenikov, 1984: J.J. Johnson, E.C. Schewe, and O.R. Maslenikov, "Soil Structure Interaction Response of a Typical Shear Wall Structure", Report UCID-20122, Vol. 1 and 2, Lawrence Livermore National Laboratory (1984)

Kennedy, 1980: R.P. Kennedy et al., "Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant", Nuclear Engineering and Design, Vol. 59, No. 2, pp. 315-338 (1980)

Kennedy, 1981: R.P. Kennedy, R.D. Campbell, D.A. Wesley, H. Kamil, A. Gantayat, and R. Vasudevan, "Subsystem Response Review - Seismic Safety Margins Research Program", Report NUREG/CR-1706, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1981)

Kennedy, 1989: R.P. Kennedy, R.C. Murray, M.K. Ravindra, J.W. Reed, and J.D. Stevenson, "Assessment of Seismic Margin Calculation Methods", Report NUREG/CR-5270, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1989)

Kennedy and Ravindra, 1984: R.P. Kennedy and M.K. Ravindra, "Seismic Fragilities for Nuclear Power Plant Risk Studies", Nuclear Engineering and Design, Vol. 79, No. 1, pp. 347-68 (1984)

Kimura, Budnitz, and Prassinos 1987: C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", Report NUREG/CR-5042, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1987). Supplement 1 to the same NUREG report, same title, covering seismic issues, is by P.G. Prassinos (1988).

Lawrence Livermore, 1989: P.G. Prassinos, J.B. Savy, C.Y. Kimura, G.E. Cummings, R.C. Murray, R.J. Budnitz, and M.K. Ravindra, "Individual Plant Examinations for External Events: Guidance and Procedures", Report NUREG/CR-5259, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission, draft version (1989)

Moore, Wooten, and Kassawara, 1988: D.P. Moore, K.D. Wooten, and R.P. Kassawara, "Seismic Margin Assessment of Hatch Nuclear Power Plant", paper presented at "Second Symposium on Current Issues Related to Nuclear Power Plant Structures, Equipment, and Piping", Orlando, Florida, sponsored by Electric Power Research Institute (1988)

NRC, 1983: J. Hickman et al., "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", Report NUREG/CR-2300, American Nuclear Society, Institute of Electrical and Electronic Engineers, and U.S. Nuclear Regulatory Commission (1983)

PG&E, 1988: Pacific Gas and Electric Company, "Long Term Seismic Program Final Report --- Chapter 6, Probabilistic Risk Analysis", work also accomplished in part by Pickard Lowe & Garrick (1988)

Prassinos/Margins, 1986: P.G. Prassinos, M.K. Ravindra, and J.B. Savy, "Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margin Reviews of Nuclear Power Plants", Report NUREG/CR-4482, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1986)

Ravindra, 1984: M.K. Ravindra, H. Banon, R.H. Sues, and R.D. Thrasher, "Sensitivity Studies of Seismic Risk Models", Report EPRI-NP-3562, Electric Power Research Institute (1984)

Ravindra, 1985: M.K. Ravindra, R.P. Kennedy, and R.H. Sues, "Dominant Contributors to Seismic Risk: An Appraisal", Report EPRI-NP-4168, Electric Power Research Institute (1985)

Ravindra and Banon, 1985: M.K. Ravindra and H. Banon, "Scoping Quantification of External Events in PRA for Nuclear Power Plants", Report SMA 12605.02, Structural Mechanics Associates, Inc., prepared for Sandia National Laboratories (1985)

Reed, 1985: J.W. Reed, M.W. McCann, J. Ihara, and H. Hadidi-Tamjed, "Analytical Techniques for Performing Probabilistic Seismic Risk Assessment of Nuclear Power Plants", Proceedings of 4th International Conference on Structural Safety and Reliability, Kobe, Japan, Vol. III, p. 253 (1985)

RMIEP, 1987: J.E. Wells et al., "Seismic Analysis of the LaSalle Unit 2 Nuclear Power Plant -- Risk Methodology Integration Evaluation Program (RMIEP)", Report NUREG/CR-4832, Vol. 8, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (197)

Shieh, 1985: L.C. Shieh, J.J. Johnson, J.E. Wells, J.C. Chen, and P.D. Smith, "Simplified Seismic PRA: Procedures and Limitations", Report NUREG/CR-4331, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1985)

SSMRP, 1981: P. D. Smith et al., "Seismic Safety Margins Research Program, Phase I Final Report", Report NUREG/CR-2015, in 10 volumes, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1981)

SSMRP, 1986: G.E. Cummings, "Summary Report on the Seismic Safety Margins Research Program", Report NUREG/CR-4431, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1986)

Yanev, 1989: P. I. Yanev, "The December 7, 1988 Armenia USSR Earthquake", EQE Engineering, Inc. Summary Report (1989)

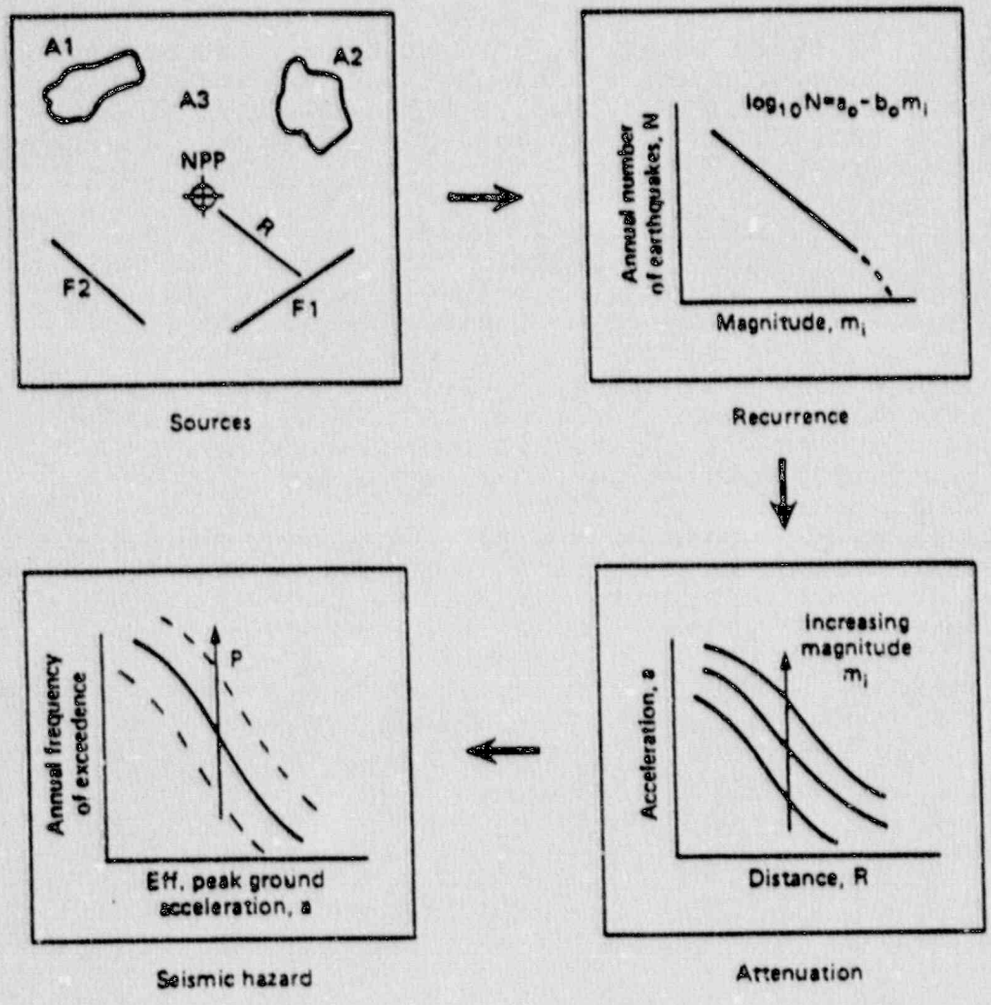


Figure III-1 *

Steps to Evaluate the Frequency
of Exceedance of Ground Motion from Earthquakes

* taken from the PRA Procedures Guide (Ref. NRC, 1983)

IV. EXTERNAL FLOODING*

IV.A Summary Evaluation

Because PRAs have occasionally identified core-damage accident sequences initiated by very high external flooding as among the important contributors at a few nuclear power plants, the analysis of flooding cannot be neglected as a part of external-initiators PRA. Fortunately, for most plants the analysis can be an abbreviated or screening analysis demonstrating that the plant layout and design are very well protected against flooding. For only a few plants will a more nearly full-scope analysis be required.

This summary will provide an overview evaluation of the reliability and usefulness of external-flooding PRA methods and results. Its summary statements are supported in the main text below.

1) How reliable is the flooding hazard methodology? The answer depends somewhat on the type of flooding phenomenon. For most of the phenomena, and for flooding heights up to or not too far above the historical record, the methodology can reliably provide site-specific answers to the question, "What is the annual frequency of flooding (F_F) up to flood level X?" Extrapolation methods much beyond the historical record at a given site possess diminished reliability. Because our historical record is usually on the order of about one century (often less, if records are poor), calculated values of F_F much below about 0.01/year become increasingly difficult to support. Modest extrapolations, of perhaps one order of magnitude to the range of 0.001/year, can be supported in some cases when the model for the flooding phenomenon is well understood.

In the above range (reliably down to F_F values near 0.01/year, less reliably down to about 0.001/year), the flood-hazard results are reliable. For F_F values much below about 0.001/year, the very broad uncertainties in the analytical models implies that the

---

The scope of this chapter covers external floods, meaning floods arising outside a nuclear power plant from external sources of water. The flooding phenomena under consideration mostly arise from "acts of god" such as high river or lake water, extreme precipitation, ocean flooding, tsunamis, seiche phenomena, and the like. A few man-made events can cause external flooding, principally due to the failure of dams, levees, and dikes.

reliability of these values is much poorer.

For a few phenomena, the situation is somewhat better. Specifically, in analyzing local precipitation it is often feasible to obtain more reliable extrapolations at a specific site by using regional information. For dam failures, use of the very large data base on dams can sometimes allow reliable extrapolations of F_F down to quite small values if similarity arguments can be supported soundly. At some sites, extrapolation of F_F for other phenomena may be supportable.

2) How reliable and useful are the flooding systems-analysis methodology and the consequence/release methodology? These aspects of the methodology, which are broadly similar to the systems-analysis methods of internal-initiators PRA, are highly reliable and useful. Specifically:

- Given a postulated flood large enough to breach a barrier and damage some key equipment, the methodology can reliably quantify the conditional probability (P_{CD}) of core damage, its principal contributors, and their interactive roles, including equipment issues, operator-error issues, and operator recovery issues.

- Given a postulated core-damage accident the conditional probability of radioactive releases (P_R) can be reliably determined and the results are highly useful.

- It is fully feasible to identify flood-related specific vulnerabilities at a nuclear plant using this methodology. When a vulnerability is identified, the analysis is robust and can be used to suggest alternative approaches to reducing the vulnerability, including approaches that rely on operator recovery actions.

3) How reliable and useful are "bottom-line numbers" for core-damage frequency and offsite risk and how reliable are the key engineering insights? Because the flood-hazard methodologies are reliable only in the range above, say, about F_F = 0.001/year, core-damage frequencies dependent on smaller F_F values will have large uncertainties. Since the frequency of core damage, F_{CD}, is roughly the product of F_F times P_{CD}, values of F_{CD} are reliable and useful only if they are constituted from F_F values above about 0.001/year.

Despite possibly large uncertainties in the bottom-line risk results, these uncertainties should not generally invalidate any insights that may be obtained about flooding vulnerabilities. That is, if the analysis reveals combinations of failures that can give rise to a safety concern, these should be robust despite uncertainties in the numerical results.

IV.B Introduction

Different types of sites are prone to different external-flooding phenomena. The following, taken from Kimura and Budnitz (Ref. Kimura & Budnitz, 1987), describes the wide range of flooding issues at different types of sites:

- all sites: flooding due to severe local precipitation and runoff effects on the site itself;
- river sites: flooding due to too much water in the river (from precipitation runoff, etc.)
- river sites: flooding due to a dam failure (which itself could be due to too much water in the river);
- ocean, estuarine sites: flooding due to combinations of high tides, wave effects, high wind-driven water levels, surges, seiches, etc.;
- ocean sites: flooding due to a tsunami;
- lake sites: flooding due to combinations of high lake water level, wave effects, high wind-driven water levels, surges, seiches, etc.;
- all sites: flooding due to earthquake-induced effects, such as landslides, dam failures, tsunami-type effects.

It is important to consider combinations of the above phenomena. At some sites, the very largest floods may not be due to an extremely unlikely occurrence of one of the phenomena, but rather to less extreme occurrences of more than one, in combination, at the same place and time. When considering the probabilities, the analyst and decision-maker must be cognizant of this issue.

As discussed in the introductory chapter, this paper is not intended to be an in-depth technical review of the subject matter, but rather an in-depth evaluation of the reliability and usefulness of the results and insights from external-initiator PRA.

The technical approach here, which builds on recent work accomplished under NRC support at Lawrence Livermore National Laboratory (Ref. Kimura & Budnitz, 1987), is to perform a more in-depth evaluation. The thrust is to identify and describe the principal aspects of the current state-of-the-art PRA methodology, what aspects are more robust and therefore provide the most reliable insights, what aspects are less robust and therefore provide less reliable insights, and why.

The product of the study is intended to be an evaluation of the PRA methodology for external flooding, concentrating on the sub-methodologies and on how these sub-methodologies are combined together to provide overall PRA results and insights. There is guidance in the literature about how to perform a flood PRA, which can be referred to for more details (Ref. NRC, 1983; Oconee PRA, 1984; Brookhaven, 1985).

IV.C Description of the Methodology

The overall methodology for probabilistic evaluation of external flooding consists of three sub-methodologies, which are combined together. The three are:

- the flood hazard methodology, which determines the frequency per year (F_F) of a flood large enough to cause damage to equipment at the nuclear power plant.
- the flood response methodology or systems analysis, which determines the probability (P_{CD}), given a flood large enough to cause more than minimal damage, that a core-damage accident will occur. P_{CD} is a conditional probability with values between 0 and 1.
- the flood consequence or release analysis, which determines the probability (P_R), given a core-damage accident from flooding, that the accident will evolve into a "radiological release" scenario. P_R is a conditional probability, and has different values for different accident sequences.

We will use the following definitions, following the notation used in Kimura and Budnitz (Ref. Kimura & Budnitz, 1987) --- here the parameter f represents the "size" (usually the high water level) of the flood:

$F_F(f)$ = frequency per year of a flood large enough to cause damage to the nuclear power plant, as a function of f;

$P_{CD}(f)$ = probability as a function of f that a core-damage accident will occur;

$P_R(f)$ = probability, given a core-damage accident from extreme flooding with size f, that the accident will evolve into a "radiological release" scenario. P_R is usually different from one accident sequence to the next.

We also define the following frequencies for reactor accidents:

F_{CD} = frequency per year of an accident involving core damage;

F_R = frequency per year of an accident involving a significant release of radioactivity.

Clearly, F_{CD} is obtained by an integration over flood sizes of $F_F(f)$ times $P_{CD}(f)$. Also, F_R is obtained by multiplying, sequence-by-sequence, the value of F_{CD} for a given sequence by P_R for that sequence, and then summing over similar sequences characterized by similar releases.

These multiplication operations are a simplification because they assume that there is no correlation or coupling between the three terms, F_F, P_{CD}, and P_R. The absence of coupling may not always be correct, although this simplification seems very reasonable, and is the approximation made in all flooding probabilistic analyses in the literature.

Of course, no large flood at any nuclear power plant has been sufficiently damaging to cause serious safety problems. That is, the floods that have occurred have been too small to cause trouble. Therefore, the empirical data base is not sufficient to provide information for the analysis discussed here. All three of the quantities (F_F, P_{CD}, and P_R) can only be determined from calculations using limited data coupled with models of what might occur in extremely unlikely situations.

In the next sub-sections, we will discuss and evaluate each of the three sub-methodologies in turn: the flood hazard methodology, the response methodology (systems analysis), and the consequence or release analysis.

IV.D Evaluation of Flood Hazard Sub-Methodologies

The task of the flood hazard methodology is to calculate F_F, whose definition was introduced above as the frequency per year of a flood large enough to be of concern to the nuclear power plant.

F_F is a function of flood "size", usually given in terms of flood water elevation. At any given site, the values of F_F will depend on which phenomenon (or combinations of phenomena) are considered. Also, for a given elevation of extreme flood water, the analyst's knowledge of F_F is never exact, so the analysis of F_F should provide a distribution rather than a point value to capture the uncertainty in the state of knowledge.

In the introduction, several different flooding phenomena were discussed, depending on the site (ocean, river, lake, etc.) and including extreme precipitation also. We shall evaluate each flooding phenomenon separately in turn.

Before discussing the individual phenomena, it is important to make five general observations.

The first and most important general observation was made in the introduction above. It is that no large flood at any operating nuclear power plant has ever caused a serious accident. While minor floods have occurred from time to time, and "major" flooding has affected a few sites, there have been no accidents. This attests, by-and-large, to the efficacy of the flood-protection criteria used in plant design, and tells us that in working out F_F the analyst is essentially always dealing with postulated floods larger than the historical record at a given site. What this means is that F_F can only be determined from <u>analysis</u>, based on limited historical data together with a model to extrapolate to the larger and much less probable floods of concern.

The second important observation involves the fact that, except for precipitation analysis, flooding analysis typically deals with a single parameter ---- floodwater height --- as its figure-of-merit. This height is then compared to the site features (river bank, dike height, ocean or lake shoreline, etc.). Once flooding reaches a certain undesired height, it is assumed that the waters will flow to all elevations at that height. It is then considered a trivial matter to determine which structures and equipment are flooded. The important observation worth noting here is that sometimes floodwater height alone may not be a sufficient endpoint for the hazard analysis. Sometimes, the <u>duration</u> of the event can be important, such as for wind-driven runup, wave effects, landslide-induced flooding, and so on. Also, sometimes the total water <u>volume</u> may be limited, such as for an upstream dam failure or a single-strike tsunami.

The third observation is that, while many of the types of flooding are mutually exclusive --- for example, one need not consider a tsunami together with a hurricane --- some of them are known to occur together, and due consideration must be taken of this issue where appropriate.

Fourth, on the units for F_F, we quote from Kimura and Budnitz (Ref. Kimura & Budnitz, 1987):

> "The value of F_F has units of frequency ("events per year"), but since large floods are so rare one often encounters discussions of the "100-year flood", "1000-year flood", and so on. The correct way to think about this terminology is as follows: although the "100-year flood" is popularly thought to be the river flood that

will recur every 100 years on the average, the correct logic is that it is the flood level with a 1/100th chance (1% chance) of occurring in any given year. Thus it should be assigned a frequency value of F_f = 0.01 per year."

Finally, because there are significant uncertainties in the flood hazard analysis, it is important that the methodology capture these. The flood hazard is generally expressed in terms of values of F_f as a function of flood height. The uncertainty is expressed as a distribution of F_f values at each given flood height, to capture the analyst's state of knowledge. Families of curves are often used to show the functional relationships, with different curves showing the 50th-percentile or median value of F_f, the 5th, 25th, 75th and 95th percentile values, the mean value, and so on.

IV.D.1 Flooding from Severe Local Rainfall

Discussion of the Methodology: The methodologies for this phenomenon depend on modelling of intense local rain over very short time periods (a few minutes up to, say, an hour), coupled with computer-based stochastic studies, such as Monte Carlo-type analysis, to generate the likelihood of several severe rains in a longer period, such as an 8-hour period. The limitations on these methods are principally that not enough is known about the correlations among severe short-duration storms. Attempts have been made to develop correlations, either spatial over short distances or temporal over a few hours, based on rain gauge data from several nearby stations. The notion is that one can develop understanding of how a severe storm might move (or not) in time. Another consideration sometimes used in the analysis is that there is a limit to the total rain available in any storm system, due to the finite size and content of the clouds. For a more detailed discussion the reader is referred to (Ref. Interagency Committee, 1986).

There does not seem to be any thorough analysis of flooding from severe local precipitation in any of the nuclear-power-plant PRAs examined. The phenomenon, if treated at all, is usually dismissed on the basis of deterministic calculations, typically in the Safety Analysis Report.

Evaluation: For extreme precipitation, there is a general consensus that some extrapolation beyond the site-specific historical record, using data from other sites, can be justified if the analysis method takes care to assure the comparability of the data used to the site being studied. The problem with determining F_f for the most extreme postulated rainfalls, say below about 0.001/year, is that the rarest events involve more than one extreme phenomenon in time correlation, and the correla-

tions are neither understood from empirical information nor modeled satisfactorily. No accepted model has yet been developed --- even more importantly, the technical basis for such a model is still not understood.

IV.D.2 River Flooding

Discussion of the Methodology: Numerous nuclear plants are sited along rivers, and in some cases the risk from flooding requires careful evaluation. (In other cases, the site is located so high above the river that major flooding is, for all intents and purposes, precluded).

The flooding design basis for most reactors is based on the Army Corps of Engineers "Probable Maximum Flood" (PMF). Although the method used for selecting the PMF is not directly linked to its annual frequency or return period, typical annual frequency (F_F) values for the PMF seem to be in the range from 0.01 to 0.001/year (Ref. Kimura & Budnitz, 1987). Two recent and prestigious studies have examined methods for assigning an annual frequency to the PMF. One study, by a US government Interagency Advisory Committee (Ref. Interagency Committee, 1986), was very pessimistic about developing annual probabilities for river flooding for recurrence intervals beyond a few hundred years, corresponding to F_F values in the range of, say, 0.003 to 0.001/year. The other study, under the auspices of a Committee of the National Academy of Sciences (Ref. National Academy of Sciences, 1988), was far more optimistic, believing that methods do exist for making estimates down to the range of 0.001/year or even lower, if appropriate watershed data can be obtained.

A discussion of the issues can be found in the recent Livermore study (Ref.Kimura & Budnitz, 1987). The fundamental problem is that, when extrapolations beyond the historical record must be made, there is a need to understand the correlations between weather phenomena, which correlations are not understood well theoretically nor known reliably from actual data in most areas.

Evaluation of the Methodology: Based on the available literature, it appears feasible to obtain values of F_F down to the range of about 0.001/year for at lest some river sites, where data and a good flooding model allow for extrapolation of the historical record. (F_F values near 0.001/year represent extrapolations of factors of 3 to 10 beyond the historical record.) For lower F_F values, the reliability of the extrapolation is probably poor, and the numerical values untrustworthy.

IV.D.3 Ocean (Coastal and Estuary) Flooding

Description of the Methodology: Numerous nuclear power plant sites are located adjacent to oceans and salt-water estuaries. While some coastal sites are located relatively high above the sea, others are low enough that storm-flooding issues can be important. For these sites, the flooding questions involve storm surges and waves running up onto the land. These usually occur in association with extreme tides, hurricanes and other storms, and possibly in association with very high rainfall.

For most coastal U.S. sites, the historical record, going back perhaps a century or sometimes two or more, provides a reasonable basis for limited extrapolations beyond the actual record. For example, historical data for a longer section of coastline (say, several hundred miles) can be used to strengthen the data base at the actual site itself. Of course, the use of these extended data requires developing a model of the specific site topography, both beneath the adjacent sea surface and on the land.

The largest coastal floods sometimes involve the coincident arrival of a large storm surge when the tides are also very high. Combining these two types of phenomena can be accomplished analytically using a joint probability distribution. It is necessary to know the extent of any correlations to perform a robust analysis. This is a major difficulty for analyses that attempt to push the extrapolations well beyond the historical record. Various extreme-value distributions have been used (Ref. St. Lucie PRA, 1987; Kimura & Budnitz, 1987).

Typically, estimates of flooding well beyond the historical record have large uncertainties, perhaps plus-or-minus a factor of 5 to 10, sometimes more. This is due to the absence of an accepted methodology for making the necessary extrapolations. These uncertainties are not as large when use of extended coastline data allows the analyst to extend his data base beyond the specific site to a longer section of coast. However, while use of this approach can "extend" the data base by a factor of, say, about one order of magnitude, going well beyond one order of magnitude inevitably involves modelling with its associated unknowns.

Evaluation of the Methodology: Based on the above brief discussion, the conclusions for coastal and estuarine flooding are similar to those for river flooding, for a similar although slightly different reason: if it is necessary to develop values of F_F well below the range of 1/100 to 1/300 per year, so that the historical data base is not directly usable, the F_F values becomes less and less valid and useful.

IV.D.4 Tsunamis

Discussion of the Methodology: The issue here is to calculate the frequency per year that a tsunami might occur large enough to threaten the reactor site. Usually, a bounding analysis will be sufficient.

Although a tsunami can occur along any of the world's coastlines, the threat to U.S. reactors is generally considered greatest for those few reactor sites near the Pacific Ocean, where tsunami events are much more frequent than elsewhere. (However, tsunamis are not unknown in the Atlantic: the major earthquake in 1755 in Lisbon, Portugal produced tsunami effects along the entire American Atlantic coast).

The historical data base for tsunamis extends for several hundred years in both Pacific and Atlantic basins, with less reliable data going back somewhat further. Given a distant tsunami arriving at a specific location, it is feasible to determine how large a tsunami-induced flood will be, by considering the local offshore subsurface topography. Usually, a deterministic analysis is sufficient to assure that tsunami effects will not be troublesome at a given site: that is, F_F is usually acceptably small based on conservative or deterministic analysis. If not, it would be necessary to perform a response analysis, determining which safety equipment and structures might be damaged and the consequences for overall safe shutdown.

Evaluation: There exists no full-scope probabilistic tsunami reactor analysis in the literature. However, such an analysis would require a straightforward adaptation of PRA methods that are well known and well within the capability of PRA analysts, and of tsunami-flood-height methods routine used in the engineering community. Therefore, such an analysis should be both reliable and useful.

IV.D.5 Lake Sites: High Water Level, Surges, Wave Effects

Discussion of the Methodology: In the U.S., this issue arises mostly for the several reactors located on the Great Lakes. The brief discussion here will therefore concentrate on Great Lake sites, for which the problem arises due to the possible (rare) combination of several effects such as storm-driven wave runup, wind-generated waves, and an unusually high lake level.

Of course, lake levels rise and fall over the years, for a variety of reasons both natural and man-made. For the Great Lakes, only slightly more than 100 years' data exist. While extrapolations out to a few hundred years are routinely done for

planning purposes, it is difficult to know how reliable these are, especially in light of the rise in Great Lake levels over the past decade or so that is not well explained (Ref. National Geographic, 1987).

Effects of extreme winds, including both wind-driven waves and wind setup along the shore, are often much larger than the variations in the lake levels themselves: for example, Lake Michigan data cited by Kimura and Budnitz (Ref. Kimura & Budnitz, 1987) show only about two feet difference between the 10-year (known) and 500-year (extrapolated) lake levels in comparison to 5-foot or even up to 10-foot effects from wind and wave phenomena at certain sites.

Analysis of a given site requires knowing the subsurface topography and local configuration. Theoretical understanding of wind-wave effects is reasonably well grounded, and reliable for modest extrapolations beyond the historical record.

Evaluation: The historical record can support F_f values down to the range of about 0.01/year. Extrapolations to another order of magnitude, to the range of about 0.001/year, can be made with modest confidence. Beyond that, uncertainties become so great that it would be difficult to rely heavily on analysis using such extrapolations.

IV.D.6 Dam Failures

Discussion of the Methodology: The issue here is to calculate the likelihood that a nearby dam might fail, thereby causing unacceptable flooding at the nuclear plant site. A generic data base exists on US dam failures, that categorizes dams into several different types such as earthfill dams, concrete gravity dams, and so on (Ref. Vanmarke & Bohnenblust, 1982; McCann & Hatem, 1985). Use of this generic data base can be useful in some circumstances, depending on how closely the specific dam fits into the data base.

The mean value for all dams is a failure rate in the range between about 10^{-4} and 10^{-5} per year (Ref. Oconee PRA, 1984; Kimura & Budnitz, 1987). However, for some modern dams that have been extensively engineered, values even in the range below about 10^{-6}/year range have been quoted (Ref. McCann & Boissonnade, 1988), while for some poorly constructed older dams, values near 10^{-3}/year could be more nearly correct, since the actual dam failures observed are mostly in this group.

Evaluation: There does not seem to be any generally accepted methodology for analyzing the dam-failure frequency for a

specific dam. Usually, a dam is considered as one of a class. Whenever a bounding-type estimate is sufficient, this method should be fully adequate based on a reasonable application of the data base. If a realistic analysis is needed as a function of extreme conditions, such as those leading to very low probabilities in the range below, say, 10^{-5}/year, the analysis must be site-specific (and river-specific, of course) and would require detailed engineering studies. There are a very few such analyses in the PRA literature (Ref. Oconee PRA, 1984; McCann & Boissonnade, 1988). Their reliability and usefulness is probably limited for failure frequencies in the range below, say, about 10^{-6}/year.

IV.E Evaluation of the Flood Response Sub-Methodology

Discussion of the Methodology: The objective of the flood response methodology is to calculate, for various floods, the probability of core damage, P_{CD}, which was defined in the introductory sub-section as the probability that a core-damage accident will occur.

P_{CD} is a true probability. It is obviously a function of the type and size of the flood. Hence, the response analysis proceeds by postulating floods of different types and "sizes", and calculating the value of P_{CD} for each such "size", to develop a functional relationship.

A brief summary of the analyst's task is as follows: the work is very similar in broad outline to ordinary PRA systems analysis. It uses the same tools, the same type of data, and the same way of setting up the analysis and solving it numerically. The following paragraphs will point out a few special considerations.

Typically, the flood-response analyst begins with the results of the flood hazard analysis, because from those results it becomes clear just which types and "sizes" of flooding are important, in terms of their annual probability of reaching whatever flood levels can cause damage. The analyst then chooses a few selected flooding scenarios of interest, and performs the response analysis for each scenario in turn.

As a hypothetical example, suppose that the result of the flood hazard analysis is as follows: flooding to elevation 303 feet has F_F = 0.01/year; to elevation 306 feet F_F = 0.003/year; and to elevation 309 feet F_F = 0.001/year.* The three elevations (303,

---

* Actually, the flood hazard analysis does not produce single point-estimate values of F_F, but a distribution for each flood level. Our hypothetical example here gives point estimate values only for simplicity.

306, 309 feet) are chosen because at 303 feet water would hypothetically submerge and damage equipment group X; at 306 feet equipment group Y as well as group X; and at 309 feet equipment group Z also. Typically, the analyst must deal with only a few discrete flood levels such as these.

Given the above, the analyst's task, assuming the flooding of each equipment group (X; X and Y; X and Y and Z), is to calculate P_{CD} for each discrete flood level. The analysis usually assumes that equipment submerged by the flood and not specially protected against water will "fail". In the systems analysis, the analyst must take into account issues such as the random (non-flood-caused) likelihood that other vital equipment might be out-of-service due to testing, maintenance, operator error, or failure; the warning time that can enable plant staff to secure certain equipment and to place the plant in a safer state; the ability of operators to recover certain flood-damaged or failed equipment, or to replace it with substitutes, or to find another way to accomplish the needed function; and so on.

Sometimes, warning times may be long enough that the plant can be confidently assumed to be shut down (hot or cold shutdown), so that only the maintenance of the shutdown state need be considered. Also, in the hypothetical example above there may be the possibility that other preventive actions (sandbagging, etc.) can effectively prevent the undesired flooding, at least at the lowest flood level (e.g., 303 feet for our example).

To accomplish the above, an event tree is needed, showing the various equipment needed for safe shutdown, possible operator prevention and recovery actions, and the like. The success-or-failure values on the event-tree branch points are then worked out using either data or fault trees. If we assume that the analyst has access to a completed internal-initiators PRA, then direct use can be made of such vital information as the emergency procedures and the support-system matrix (which support systems such as AC power, instrument air, service water, etc. support which front-line equipment). Otherwise, the analyst must develop this information anew.

The outcome of the analysis is the numerical value of P_{CD} (actually, a P_{CD} density function that captures uncertainties) for each (usually discrete) flood level of interest.

Evaluation of the Methodology: As mentioned briefly above, the flood-response sub-methodology is, in its basic outline, a variant of the type of systems analysis that is now a well-developed, mature PRA discipline. While certain issues must be specially treated, every aspect of the methodology is fully within the routine capability of PRA analysts. We conclude that

any competent PRA systems analyst can perform this work, with no special training and only the minimal guidance that is readily available and easily learned.

IV.F Evaluation of the Flood Consequence/Release Sub-Methodology

Discussion of the Methodology: The objective of the flood consequence/release methodology is to calculate, for various flood levels associated with various probabilities of core damage (P_{CD}), the probability P_R, which was defined in the introductory sub-section as the probability, given a core-damage accident sequence from flooding, that the accident will evolve into a "radiological release" scenario.

P_R is a true probability. It obviously differs for each different core-damage accident sequence. Each sequence requires separate treatment, depending on which pieces of safety equipment have been damaged by the flood, which other equipment has failed from other causes, which operator actions have contributed to the damage or mitigated the situation, and so on. P_R also obviously depends on how phenomena develop both within the primary system and in containment after core damage begins; how ex-plant radiological dispersion phenomena develop; and how sheltering and evacuation are accomplished.

Evaluation of the Methodology: The consequence/release methodology is, in its basic outline, a variant of the type of level-2 and level-3 analysis that is now a well-developed, mature PRA discipline. The methods and data used are identical, including the use of containment event trees (or accident-progression event trees, as they are now often called) and offsite consequence analysis codes. While a few issues must be specially treated, we conclude that any competent PRA level-2/level-3 analysis team can perform this work, with no special training.

Of course, it is important that the analysis team consider a few special issues, such as the possibility that the external flooding (especially if associated with other natural phenomena such as extreme winds or enormous rainfall) may affect containment integrity or ultimate heat-sink capability; may degrade the recoverability of lost offsite power; may alter access and assistance from off-site personnel; may modify ex-plant evacuation routes; may alter environmental transport or released radioactivity; and so on. Treating all of these issues is fully within the capability of PRA analysts today.

IV.G Evaluation of the "Bottom-Line" Results for Core-Damage Frequency and Offsite Risk, and of the Key Risk Insights

As the discussion above has indicated, there are limitations in the accuracy of realistic estimates of the frequency of very large and rare floods. Thus the "bottom-line" numerical results for core-damage frequency and offsite risks can have large numerical uncertainties to the extent that they rely on flood-hazard frequency estimates for the rarest floods.

However, the principal engineering insights depend only in part on the numerical bottom-line results, and often not in a major way. These insights involve the identification of specific structures and equipment that may be vulnerable to flood-caused damage, and of configurations of safety systems and functions that, taken together, might lead to a core-damage accident. The configurations of interest can include contributions from non-flood-related failures and human errors, which can be identified using the full power of the PRA approach to do an integrated analysis.

Therefore, we conclude that despite the numerically large uncertainties in the "bottom-line" numbers, these uncertainties should generally not invalidate the key insights concerning potential flood-related vulnerabilities.

IV.H References

Brookhaven, 1985: M. McCann, J. Reed, C. Ruger, K. Shiu, T. Teichmann, A. Unione, and R. Youngblood, "Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, Volume 2, Brookhaven National Laboratory and U.S. Nuclear Regulatory Commission (1985)

Interagency Committee, 1986: Work Group on Probable Maximum Flood Risk Assessment, under the direction of the Hydrology Subcommittee of the Interagency Advisory Committee on Water Data, "Feasibility of Assigning a Probability to the Probable Maximum Flood", Office of Water Data Coordination (1986)

Kimura and Budnitz, 1987: C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", Report NUREG/CR-5042, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1987). Supplement 1 to the same NUREG report, same title, covering seismic issues, is by P.G. Prassinos (1988)

McCann & Boissonnade, 1988: M.W. McCann, Jr. and A.C. Boissonnade, "Probabilistic Flood Hazard Assessment for the N Reactor, Hanford, Washington", Report UCRL-21069, Lawrence Livermore National Laboratory (1988)

McCann & Hatem, 1985: "M.W. McCann, Jr. and G. Hatem, "Progress on the Development of a Library and Data Center on Dam Incidents in the U.S.", Stanford University Department of Civil Engineering, Progress Report No. 2 to Federal Emergency Management Agency (1985)

National Academy of Sciences, 1988: Committee on Techniques for Estimating Probabilities of Extreme Floods, Water Science and Technology Board, "Estimating Probabilities of Extreme Floods, Methods and Recommended Research", National Academy of Sciences (1988)

National Geographic, 1987: C.E. Cobb, Jr., "The Great Lakes' Troubled Waters", National Geographic Magazine 172, p. 2-31 (July, 1987)

NRC, 1983: J. Hickman et al., "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", Report NUREG/CR-2300, American Nuclear Society, Institute of Electrical and Electronic Engineers, and U.S. Nuclear Regulatory Commission (1983)

N-Reactor PRA, 1989 (draft): M. P. Bohn et al., "N-Reactor External Events Probabilistic Risk Assessment" (draft version, no report number yet), Sandia National Laboratories and Westinghouse Hanford Company (1989)

Oconee PRA, 1984: Electric Power Research Institute/Nuclear Safety Analysis Center and Duke Power Company, Report NSAC-60, "Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3", in 4 volumes (1984)

St. Lucie PRA, 1987: G.A. Sanders, D.M. Ericson, Jr., and W.R. Cramond, "Shutdown Decay Heat Removal Analysis of a Combustion Engineering 2-Loop PWR --- Case Study", Report NUREG/CR-4710, Sandia National Laboratories and U.S. Nuclear Regulatory Commission (1987)

Vanmarke & Bohnenblust, 1982: E.H. Vanmarke and H. Bohnenblust, "Risk-Based Decision Analysis for Dam Safety", Research Report R82-11, Massachusetts Institute of Technology, Department of Civil Engineering (1982)

V. EXTREME WINDS

V.A Summary Evaluation

Because PRAs have identified core-damage accident sequences initiated by extreme winds as among the important contributors at a few nuclear power plants, the analysis of extreme winds cannot be neglected as a part of external-initiators PRA. Fortunately, for most plants the analysis can be an abbreviated or screening analysis demonstrating that the plant layout and design are very well protected against extreme winds. For only a few plants will a more nearly full-scope analysis be required.

This summary will provide an overview evaluation of the reliability and usefulness of PRA methods for studying extreme winds. The main text below will support its summary statements.

1) How reliable is the wind hazard methodology? Although the site-specific wind hazard curves used in PRAs have significant numerical uncertainties (up to about plus-or-minus one order of magnitude uncertainty in some cases), the methodology is mature and reasonably reliable.

2) How reliable is the fragility methodology for extreme winds? This methodology has several different aspects:

- For unprotected equipment and for structures having poor wind-resistant capacity, a thorough walkdown is a reliable way to identify and analyze these items.

- For structures with an excellent wind-resistant design basis, the methodology can reliably identify these structures and can often screen them out without detailed analysis.

- For those structures for which further analysis is needed, the definition of structural "failure" for PRA-analysis purposes can usually be properly determined by experienced engineers. However, if a realistic calculation of damage and failure probability as a function of wind speed and other extreme-wind parameters is needed, the analysis, although mature for many structures, is difficult for some other configurations, and there can sometimes be large uncertainties in the numerical results. Despite these occasional problems, developing fragility curves for structures in extreme wind loadings is probably a more robust discipline than the same analysis problem for large earthquakes.

- In analyzing the "failure" of equipment within structures, it is usually conservatively assumed that structural "failure", however carefully defined, implies failure of all equipment dependent on or within the structure. If more realistic analysis is needed, the conclusion will typically depend on the experienced judgment of the analyst, and is therefore subject to possible uncertainties surrounding this judgment.

- Tornado missiles have never been found to be important contributors in any PRA, so conservative screening methods have been adequate as an approach to the analysis. If these screening methods are not adequate, methods do exist that can be used for detailed analysis of individual structures and equipment, and these methods are reliable in the hands of an experienced analyst.

3) How reliable and useful are the wind systems-analysis methodology and the consequence/release methodology? These aspects of the methodology are broadly similar to the systems-analysis methodology for internal-initiators PRA, and are highly reliable and useful. Specifically:

- Given a postulated extreme wind large enough to breach a barrier and damage some key equipment, the methodology can reliably quantify the conditional probability (P_{CD}) of core damage, its principal contributors, and their interactive aspects, including equipment issues, operator-error issues, and operator recovery issues. The principal difficult issue is determining dependencies among nearby items of equipment damaged together: although the conservative assumption of full correlation is usually adequate for gross building failure or tornado-missile damage to outside equipment, if it is not adequate a more realistic analysis can sometimes be quite difficult.

- Given a postulated core-damage accident, the conditional probability of radioactive releases (P_R) can be reliably determined and the consequences calculated. Special consideration is needed for a few issues, such as possible hampering of emergency evacuation procedures in the presence of extensive wind-caused damage.

4) How reliable and useful are "bottom-line numbers" for core-damage frequency and offsite risk, and the key risk insights? Although the numerical uncertainties in the bottom-line results can be large (plus-or-minus one order of magnitude or slightly more would not be uncommon), these uncertainties should generally not invalidate the key insights concerning potential wind-related vulnerabilities. Conversely, if no vulnerabilities are identified and the plant is judged to be well designed against wind-initiated accidents, this conclusion should be quite robust despite the numerical uncertainties in the bottom-line numbers.

V.B Introduction

Different types of sites are prone to different extreme-wind phenomena, including hurricanes, tornadoes, and extra-tropical wind storms. Damage can be from the wind forces themselves, from pressure differentials, or from wind-generated missiles. Here, the characteristics of these different extreme-wind phenomena will not be discussed in detail, because these are covered well in several readily accessible documents (Ref. Kimura & Budnitz, 1983; NRC, 1983; Lawrence Livermore, 1989). Suffice it to point out that at any given site it is important to begin by deciding which of these potential wind hazards (perhaps all!) apply, and why.

As discussed in the introductory chapter, this paper is not intended to be an in-depth technical review of the subject matter, but rather an in-depth evaluation of the reliability and usefulness of the results and insights from external-initiator PRA.

The technical approach here, which builds on recent work accomplished under NRC support at Lawrence Livermore National Laboratory (Ref. Kimura & Budnitz, 1987), is to perform a more in-depth evaluation. The thrust is to identify and describe the principal aspects of the current state-of-the-art PRA methodology, what aspects are more robust and therefore provide the most reliable insights, what aspects are less robust and therefore provide less reliable insights, and why.

The study will concentrate on the sub-methodologies and on how these sub-methodologies are combined together to provide overall PRA results and insights. There is guidance in the literature about how to perform a PRA for extreme winds, which should be consulted for details (Ref. NRC, 1983; Brookhaven, 1985; Ravindra & Banon, 1985; Lawrence Livermore, 1989).

V.C Description of the Methodology

The overall methodology for probabilistic evaluation of extreme winds consists of four sub-methodologies, which are combined together. The four are:

- the wind hazard methodology, which determines the frequency per year (F_W) of a wind storm large enough to cause damage to equipment at the nuclear power plant.

- the wind response analysis, which determines the probability (P_{CD}), given a wind storm large enough to cause damage, that a core-damage accident will occur. P_{CD} is a conditional probability with values between 0 and 1. There are two sub-methodologies involved here,

the wind fragility methodology and the wind systems-analysis methodology.

- the wind consequence or release analysis, which determines the probability (P_R), given a core-damage accident from extreme winds, that the accident will evolve into a "radiological release" scenario. P_R is a conditional probability, and has different values for different accident sequences.

We will use the following definitions, following the notation used in Kimura and Budnitz for external flooding (Ref. Kimura & Budnitz, 1987) --- here the parameter w is the windspeed:

$F_W(w)$ = frequency per year of a wind storm large enough to cause damage to the nuclear power plant, as function of w;

$P_{CD}(w)$ = probability as a function of wind speed w that a core-damage accident will occur;

$P_R(w)$ = probability, given a core-damage accident from extreme winds with wind speed w, that the accident will evolve into a "radiological release" scenario. P_R is usually different from one accident sequence to the next.

We also define the following frequencies for reactor accidents:

F_{CD} = frequency per year of an accident involving core damage;

F_R = frequency per year of an accident involving a significant release of radioactivity.

Clearly, F_{CD} is obtained by an integration over windspeed of $F_W(w)$ times $P_{CD}(w)$. Also, F_R is obtained by multiplying, sequence-by-sequence, the value of F_{CD} for a given sequence by P_R for that sequence, and then summing over similar sequences characterized by similar releases.

These multiplication operations are a simplification because they assume that there is no correlation or coupling between the three terms, F_W, P_{CD}, and P_R. The absence of coupling may not always be correct, although this simplification seems very reasonable, and is the approximation made in all extreme-wind probabilistic analyses in the literature.

No wind storm at any nuclear power plant has been sufficiently damaging to cause serious safety problems. That is, the high winds that have occurred have always been too small to cause a

core-damage accident or even a "near miss" consisting of loss of key safety functions. Therefore, experience alone is not sufficient to provide information for the analysis discussed here. All three of the quantities (F_W, P_{CD}, and P_R) can only be determined from calculations using limited data coupled with models of what might occur in extremely unlikely situations.

In the next sub-sections, we will discuss and evaluate each of the four sub-methodologies in turn: the extreme-wind hazard methodology, the response methodology (including the fragility analysis and the systems analysis), and the consequence or release analysis.

V.D Evaluation of the Extreme-Wind Hazard Sub-Methodology

Description of the Methodology: The wind hazard is usually expressed in terms of the frequency per year of exceedance of various wind speeds. This is typically given in the form of a family of "hazard curves" expressing differing levels of confidence, such as a median hazard curve, a 10% curve, and 90% curve, and so on. The analyst should take care to account for the other characteristics of the wind hazard besides wind speed. For tornadoes this would include path width, path length, translational tornado speed, vertical velocity, and the like. For hurricanes it would include duration, distribution of the central pressure drop, radius of the maximum winds, storm attenuation across land, associated rain and flooding, and so on.

The hazard curves for hurricanes, tornadoes, and extra-tropical straight winds have different shapes. A stylized representation for a given hypothetical site is shown in Figure V-1 (taken from Ref. Kimura & Budnitz, 1987). Note that tornadoes produce the highest wind speeds, albeit at the very lowest annual frequencies.

There are several established methods for developing wind hazard curves, and they have been used in numerous PRAs. The data bases in the literature often require extrapolation for the specific site being studied, which means developing a model to incorporate site-specific information into a regional-scale model. While this can usually be accomplished reasonably well, the various models do have differences and uncertainties definitely remain an issue.

A detailed discussion of the various models will not be attempted here, since the literature on this subject is extensive and some recent NRC-sponsored summaries exist (Ref. Lawrence Livermore, 1989; McDonald, 1983; Coates & Murray, 1985; Kimura & Budnitz, 1987). Suffice it to point out that the analysis requires not only a model incorporating a regional data base on tornadoes or

hurricanes categorized by "size" (usually wind speed), but also a local site-strike model to account for topography and other site aspects. Issues continue to exist on how to use the observational data base for tornadoes, since it is incomplete; how to categorize the tornadoes' damage potential; and how to determine out their potential for picking up missiles. For hurricanes, land-crossing attenuation relations must be used, and local heavy precipitation issues need to be considered.

For these and a few other reasons, uncertainties continue to exist in extreme-winds hazard analysis, especially whenever it is necessary to develop realistic hazard curves because a conservative or screening analysis is not adequate. However, the methodologies involved are mature and reliable, having been used for many years at a variety of sites by numerous practitioners.

Evaluation of the Methodology: Sometimes, conservatively biased hazard curves can be successfully used in a screening analysis, and this is appropriate if the screening step is sufficient to eliminate the issue. However, it is often necessary to develop realistic site-specific hazard curves. Although these hazard curves can have significant uncertainties depending on the site (factors up to about plus-or-minus one order of magnitude uncertainty are not uncommon), the methodology is quite reliable provided the analyst has appropriately accounted for the uncertainties and captured them in the analysis.

V.E Evaluation of the Extreme-Wind Response Sub-Methodology

V.E.1 Introduction

The objective of the extreme-wind response methodology is to calculate, for various large wind storms, the quantity P_{CD}, which was defined in the introductory sub-section as the probability as a function of wind speed that a core-damage accident will occur.

P_{CD} is a conditional probability. It is clearly a function of the type and size of the wind storm. Hence, the response analysis proceeds by postulating wind storms of different types and "sizes", and calculating the value of P_{CD} for each such "size", to develop a functional relationship.

There are two sub-methodologies involved here, the wind fragility methodology and the wind systems analysis.

A brief summary of the analyst's typical approach is as follows (here the first two steps comprise the wind-fragility methodology while the third step is the systems analysis):

- First, for each wind "size" (usually, "size" is characterized by wind speed but other aspects must be considered, as discussed above), the probability of damage to structures and equipment must be calculated. The damage can occur from either the direct wind forces, the negative pressures associated with the winds, or missiles picked up by the wind that can strike and damage structures and equipment. Sometimes, water damage can occur from associated heavy rains.

- Second, given damage to specific structures, the analyst must figure out which safety-related equipment may be damaged. Usually, the assumption is made that a damaged structure implies damage and failure of all equipment housed within it or dependent on it.

- Third, given which equipment is damaged (typically with a probability distribution), the analyst must determine which core-damage accident sequences may result. This work is broadly similar to traditional PRA systems analysis for internal initiators.

In the following two subsections, we will point out a few special considerations.

V.E.2 Wind Fragility Methodology

Discussion and Evaluation of the Methodology: The winds of interest have very high speeds, of the order of 80 to 130 mph (miles per hour) or more for hurricanes and sometimes in excess of 200 mph for tornadoes. Also, missiles picked up by the wind (usually by tornadoes, less commonly by hurricanes) can harm structures and equipment.

The methodology therefore has several parts, which will be discussed and evaluated separately in the following individual paragraphs:

1) Outside Equipment and Weak Structures: Certain unprotected equipment and some structures have so little wind-resistant capacity that damage is almost inevitable given high enough winds. This category includes the electrical switchyard, small exhaust stacks, unprotected wall and roof openings, outside wiring and cabling, and the like. Also, some building features can be vulnerable, such as a wall or roof with inadequate strength or bracing. A thorough walkdown of the site is necessary so that the analyst can identify the vulnerable items, and can assign them high (often 100%) likelihood of failure in the wind storms of interest. The methodology for this aspect is sound, and the results reliable.

2) Well-Designed Structures: The key structures, such as the reactor building and auxiliary building, are usually well-designed with a specific design basis traceable to one or another design code. In these cases, the design basis can serve as a starting point for the analysis of the wind speed, or tornado-induced pressure drop, where failure might be expected.

One important point must be made up-front, as follows: There is a consensus (Ref. Lawrence Livermore, 1989) that well-designed buildings, such as those designed to the NRC's current standards like the ANSI A58.1 standard, can be confidently screened out for wind speeds with annual frequencies down to about 10^{-6}/year. The screening criteria have been documented recently (Ref. Lawrence Livermore, 1989). To the extent that this is true, it vastly simplifies the PRA analysis of wind-initiated accidents at nuclear power plants.

There are several technical issues involved in this aspect of the analysis, which apply for those structures that cannot be screened out using the criteria referenced above:

- First, "failure" must be defined --- usually it would be severe buckling or collapse that could compromise the safety equipment within, or collapse that could fall onto and damage important equipment. "Failure" usually does not include minor structural damage. The decision about what constitutes "failure" must be made by the structural analyst on a case-by-case basis, with the advice of a competent systems analyst, and considering the specific safety equipment and safety functions that would be vulnerable. This aspect of the methodology is quite reliable and useful. This is especially true if a conservative assignment of "failure" is adequate. If the analysis requires a realistic model of damage and failure, there will probably be larger uncertainties in the judgments made here, although in general the results should be reasonably reliable.

- Second, even if they are not screened out earlier, some structures will be screened out here up to quite high wind speeds as adequately strong. If the required extrapolations are within (or not too far above) the design basis wind speed for the structure, this aspect can probably be done well by competent engineers, and the results will be reliable.

- Third, for some structures it will be necessary to do specific analysis, to determine the "fragility curve" representing the likelihood of failure as a function of wind speed. Because the design codes have embedded conservatisms, this involves, in essence, determining how much margin actually exists above the design basis for the

specific structure. A realistic analysis must translate wind speed (or in some cases pressure drop) into forces, and must correlate forces with structural capacities. It should take into account responses beyond the elastic limit, and may require extensive calculations, coupled with tie-ins to test data that may exist for some configurations. This analysis, although mature for many structures, is difficult for some other configurations, and there can sometimes be large uncertainties in the numerical results. Despite these occasional problems, developing fragility curves vs. wind speed for structures in extreme wind loadings is probably a more robust discipline than the same analysis problem for large earthquakes, and the results can usually be considered quite reliable.

3) Equipment Within Structures: Most safety equipment is located inside buildings. For this equipment, it is necessary to figure out the circumstances under which structural "failure" would result in equipment "failure", meaning equipment unable to perform its safety function.

Even when the definition of structural "failure" has been carefully selected, the usual assumption made here is that building "failure" implies failure of all equipment within --- or at least of all equipment tied into whatever part of the structure is analyzed as "failing". This can be a highly conservative assumption in some cases. If it is necessary to do better, the analyst can examine the mode of structural failure (full or partial) and the location of individual equipment items to ascertain whether they will actually fail given structural failure. This aspect of the methodology can be quite reliable if the expert judgments are competent.

4) Tornado Missiles: Fortunately, the few PRAs that have addressed tornado missiles have found them not to be an important contributor. However, the potential for damage must still be addressed for each individual site.

There are two issues with tornado missiles. First is the question of the "missile spectrum". Second is an assessment of the damage that they might cause.

The subject of the missile spectrum (how many missiles of which types might be picked up, and their velocities) is difficult, in that there is a very wide variability in tornado-missile spectra from real tornadoes. The NRC's design requirements call for consideration of a standard set of tornado missiles, which set is usually used as a starting point in PRA analysis. If a given structure has been designed for this spectrum of missiles, that fact can be an acceptable basis for screening out the structure.

The damage-analysis problem arises for structures not so de-

signed, or for unprotected outside equipment. First, a thorough analysis can determine the site-specific missile spectrum by surveying the site -- the results are used as input to the damage analysis (Ref. Twisdale, 1988). Often, a conservative missile spectrum will be adequate for screening purposes.

If conservative screening is not adequate, the analyst can fall back on a resource-intensive study of a variety of classes of missiles and their damage potentials for specific structures or outside equipment. Missiles can penetrate, cause local spalling, or create an overall dynamic load, depending on the missile type, the object struck, and how the object is struck. The methodology exists and has been exercised in a few cases, but is by no means commonly done (Ref. Twisdale, 1988). This methodology should be quite reliable if care is taken.

V.E.3 Wind Systems Analysis

As mentioned above, the objective of the extreme-wind response methodology is to calculate, for various large wind storms, the probability of core damage, P_{CD}, which has previously been defined as the probability, given a wind storm large enough to cause more than minimal damage, that a core-damage accident will occur.

Discussion of the Methodology: The systems-analysis work is very similar in broad outline to ordinary PRA systems analysis. It uses the same tools and types of data, and the same way of setting up the analysis and solving it numerically. The following paragraphs will point out a few special considerations.

The analyst typically begins with the results of the wind fragility analysis, which will have determined which structures and equipment have suffered damage from the extreme wind (as a function of wind speed, etc.). The systems analyst must then take into account issues such as the random (non-wind-caused) likelihood that other vital equipment might be out-of-service due to testing, maintenance, operator error, or failure; the warning time that can enable plant staff to secure certain equipment and to place the plant in a safer state; and the ability of operators to recover certain wind-damaged or failed equipment, or to replace it with substitutes, or to find another way to accomplish the needed function.

There are two special issues to discuss here: warning time and correlated failures.

Sometimes, warning times may be long enough that the plant can be confidently assumed to be shut down (hot or cold shutdown), so that only maintaining the shutdown state need be considered. This is especially likely to be true for hurricanes, less likely

for tornadoes that can sometimes strike with little or no warning. There may also be the possibility that certain anticipatory actions can effectively prevent or mitigate the undesired damage. If this is the case (for example, when a hurricane strikes after more than, say, 24 hours' warning), the analysis is much simplified.

The problem of analyzing correlations among wind-induced failures can be difficult. Usually, the assumption of complete correlation for nearby equipment is made: for example, if a structure collapses the analyst usually assumes that all items of safety equipment within or dependent on the structure will be damaged and will all fail to perform their safety functions. A detailed numerical analysis of this issue that goes beyond this simplified assumption, while feasible is principle, is probably very difficult to accomplish in practice, and has therefore never been attempted in any PRA.

The systems analysis requires developing one or more accident sequence event trees, that include the various equipment needed for safe shutdown, possible operator prevention and recovery actions, and the like. The success-or-failure numerical values on the event-tree branch points are then worked out using either data or fault trees. If we assume that the analyst has access to a completed internal-initiators PRA, then direct use can be made of such vital information as the emergency procedures and the support-system matrix. (Support systems such as AC power, instrument air, service water, and so on support the vital front-line equipment.) Otherwise, the analyst must develop this information anew.

The outcome of the systems analysis is the numerical value of P_{CD} (actually, a P_{CD} density function that captures uncertainties) for each of several (usually discrete) wind speeds of interest.

Evaluation of the Methodology: As mentioned briefly above, the wind systems sub-methodology is, in its basic outline, a variant of the type of systems analysis that is now a well-developed, mature PRA discipline. While certain issues must be specially treated, every aspect of the methodology is fully within the routine capability of PRA analysts. Therefore, we conclude that any competent PRA systems analyst can perform this work, with no special training and only the minimal guidance that is readily available and easily learned.

V.F Evaluation of the Extreme-Wind Consequence/Release Sub-Methodology

Discussion of the Methodology: The objective of the extreme-wind consequence/release methodology is to calculate, for various wind storm "sizes" associated with various probabilities of core damage (P_{CD}), the probability P_R. P_R was defined in the introductory sub-section as follows:

> P_R = probability, given a core-damage accident from extreme winds, that the accident will evolve into a "radiological release" scenario.

P_R is a conditional probability. It usually differs from one core-damage accident sequence to the next. Each sequence requires separate treatment, depending on which items of safety equipment have been damaged by the wind storm, which other equipment has failed from other causes, which operator actions have contributed to the damage or mitigated the situation, and so on. P_R also obviously depends on how phenomena develop both within the primary system and in containment after core damage begins; how ex-plant radiological dispersion phenomena develop; and how sheltering and evacuation are accomplished.

It is important that the analysis team consider a few special issues, such as the possibility that the external wind storm (especially if associated with other natural phenomena such as enormous rainfall) may affect containment integrity, either for the structure itself or, more likely, for the penetrations or other ways in which integrity can be compromised.

Also, if the wind storm has caused extensive damage offsite, such as to roads and bridges, or widespread flooding, the effect of this damage on emergency evacuation must be assessed.

Evaluation of the Methodology: The consequence/release methodology is, in its basic outline, a variant of the type of level-2 and level-3 analysis that is now a well-developed, mature PRA discipline. The methods and data used are similar or identical, including the use of containment event trees (or accident-progression event trees, as they are now often called) and offsite consequence analysis codes. While a few issues must be specially treated, we conclude that any competent PRA level-2/level-3 analysis team can perform this work, with no special training.

Unfortunately, the existence of a workable methodology does not guarantee its successful execution. Specifically, because some of the special issues --- such as offsite damage and its effect on evacuation --- are difficult and highly uncertain, the reliability and usefulness of the results can be significantly compromised. This is not a fault of the methodology *per se*, but

rather a potential for the analyst to be incomplete in developing all of the issues fully.

For this reason, it is quite important that the consequences/release analysis be reviewed to assure that its scope of coverage is adequate, and that no important issues are omitted or given only abbreviated treatment.

V.G Evaluation of the "Bottom-Line" Results for Core-Damage Frequency and Offsite Risk, and the Key Risk Insights

As the discussion above has indicated, the numerical uncertainties in the bottom-line results can be large (plus-or-minus an order of magnitude would not be uncommon). This is due in part to limitations on the accuracy of realistic wind hazard estimates, and in part to uncertainties in realistically calculating fragilities for structures, if it is found necessary to do so because a bounding approach isn't adequate.

The principal engineering insights depend in part on the numerical "bottom-line" results but usually not in a major way. These insights involve the identification of specific structures that may be vulnerable to extreme-wind-caused damage, and of configurations of safety systems and functions that, taken together, might lead to a core-damage accident. The configurations of interest can include contributions from non-wind-related failures and human errors, which can be identified using the full power of the PRA approach to do an integrated analysis.

Despite the numerically large uncertainties in the "bottom-line" numbers, these uncertainties should generally not invalidate the key insights concerning potential wind-related vulnerabilities. Conversely, if no vulnerabilities are identified and the plant is judged to be well designed against wind-initiated accidents, this conclusion should be quite robust despite the numerical uncertainties in the bottom-line numbers.

V.H References

Brookhaven, 1985: M. McCann, J. Reed, C. Ruger, K. Shiu, T. Teichmann, A. Unione, and R. Youngblood, "Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, Volume 2, Brookhaven National Laboratory and U.S. Nuclear Regulatory Commission (1985)

Coates & Murray, 1985: D.W. Coates and R.C. Murray, "Natural Phenomena Hazards Modeling Project: Extreme Wind/Tornado Hazard Models for Department of Energy Sites", Report UCRL-53526, Revision 1, Lawrence Livermore National Laboratory (1983)

Kimura and Budnitz, 1987: C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", Report NUREG/CR-5042, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1987). Supplement 1 to the same NUREG report, same title, covering seismic issues, is by P.G. Prassinos (1988)

Lawrence Livermore, 1989: P.G. Prassinos, J.B. Savy, C.Y. Kimura, G.E. Cummings, R.C. Murray, R.J. Budnitz, and M.K. Ravindra, "Individual Plant Examinations for External Events: Guidance and Procedures", Report NUREG/CR-5259, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission, draft version (1989)

McDonald, 1983: J.R. McDonald, "A Methodology for Tornado Hazard Probability Assessment", Report NUREG/CR-3058, Institute for Disaster Research at Texas Tech University, and U.S. Nuclear Regulatory Commission (1983)

NRC, 1983: J. Hickman et al., "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", Report NUREG/CR-2300, American Nuclear Society, Institute of Electrical and Electronic Engineers, and U.S. Nuclear Regulatory Commission (1983)

N-Reactor PRA, 1989 (draft): M. P. Bohn et al., "N-Reactor External Events Probabilistic Risk Assessment" (draft version, no report number yet), Sandia National Laboratories and Westinghouse Hanford Company (1989)

Ravindra and Banon, 1985: M.K. Ravindra and H. Banon, "Scoping Quantification of External Events in PRA for Nuclear Power Plants", Report SMA 12605.02, Structural Mechanics Associates, Inc., prepared for Sandia National Laboratories (1985)

Twisdale, 1988: L.A. Twisdale, "Probability of Facility Damage from Extreme Wind Effects", Journal of Structural Engineering 114, no. 10, pp. 2190-2209 (1988)

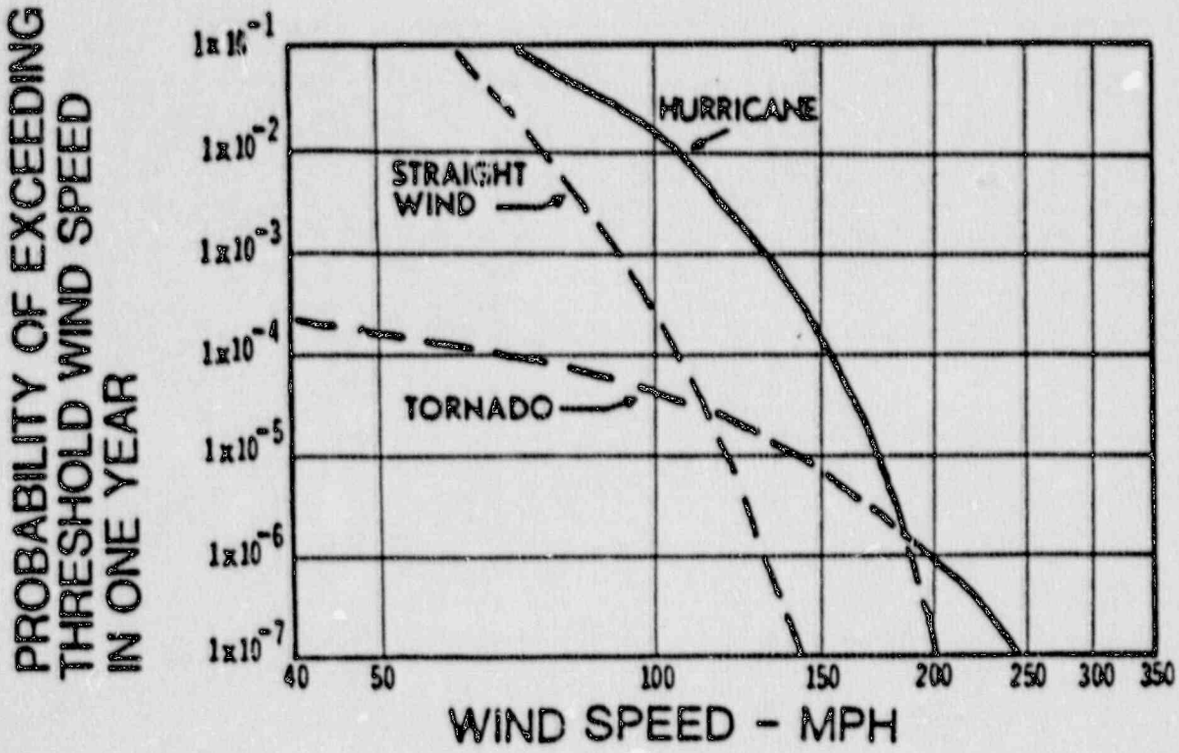


Figure V-1 *

Typical Tornado, Hurricane, and
Straight Wind Hazard Probability Models**

* from (Ref. Kimura & Budnitz, 1987)

** Note that the relative positions of the straight wind and hurricane probability models could be interchanged depending on the site.

VI. TRANSPORTATION ACCIDENTS

VI.A Summary Evaluation

In this section, we will discuss the usefulness and limitations of transportation accident PRA. The transportation modes that we will cover are:

- o aviation (commercial/general/military)
- o marine (ship/barge)
- o pipeline (gas/oil)
- o railroad
- o truck.

Hazards from transportation accidents include:

- o direct collisions with plant structures (marine and aviation)
- o explosions and fire releases
- o hazardous material releases (e.g. chlorine)

These accidents can cause (1) structural damage, (2) direct critical equipment damage or (3) injury or death to control room operators or other onsite personnel.

1) How reliable is the methodology for determining the initiating event frequency? As with other external-event PRA analyses, the reliability of the methodology depends upon the quality of the data for the initiating event frequency.

Accident frequency data for railroads, general aviation and commercial aviation are good. Federal agencies tabulate accident data and operating data on a relatively consistent basis and it is possible to make comparisons of accident and operating data on a yearly basis.

For pipeline operations, military aviation, and ship/barge traffic, current reliable data have yet to be found. Up-to-date accident frequency information does not exist for truck accidents. Federal agencies no longer collect the desired data. State agencies do collect data but cover only a limited portion of the total fleet population, and industry data sources are usually not compiled on a year-by-year basis.

It is important to note that the data must be collected in terms of the number of hazardous shipments with information including vehicle speed, type, weight, and type and amount of hazardous

material being transported. Another important point is that the generic accident data might have to be modified to allow for possible site-specific factors such as terrain, road and weather conditions near the plant.

2) How reliable is the methodology for making consequence calculations? As with other external-event PRA analyses, the initiating event frequency serves as an initial screening value to place an upper bound value on the risk. If this frequency is sufficiently low, then the entire category can be screened out and no further analysis is necessary.

If it is not screened out, then an analysis of plant responses should be done. This involves calculation of the probability of the hazardous material detonating, catching fire, diffusing to the plant site, forcing the plant operators to evacuate or isolate the control room, or damaging plant equipment. Any of these would result in a transient event, usually by precipitating a reactor scram.

In limited cases, these calculations have been made. Chelapati, Kennedy and Wall (1972) have calculated the probability of penetration of a reinforced concrete wall as a function of plant location and concrete thickness for airplane crashes. In the Waterford 3 SER (1981), it was calculated that a denotation of a 300,000-barrel gasoline tanker would produce at the plant a peak reflected overpressure of 2.7 psi. The SER concluded that this was an acceptable overpressure for the safety-related buildings.

3) How reliable is the overall methodology? Many plants dismiss the risk due to transportation accidents on the basis of a low initiating event frequency. However, for most plants, traffic density has increased over the years which makes recalculation of accident frequency necessary. There are a few plants that are at potential risk from an accident mode besides airplanes. (All plants have the possibility of airplane crashes.) For these plants, probabilistic analysis of the plant's response to a nearby transportation accident should be considered if the accident frequency is too high, such as above about 1×10^{-6} per year as suggested by Kimura & Budnitz (1987).

To date, a formal probabilistic plant response methodology for transportation accidents has not been developed. Upper bound assessments can be made only in terms of the initiating event frequency with the possibility of the inclusion of mitigation, such as isolating the control room or using an effective means of detecting natural gas leaking from a pipeline (see the Indian Point PRA, 1983). Of course, in many cases these assessments will be fully adequate.

VI.B Introduction --- A List of Potential Hazards

A ranking of the potential hazards from transportation accidents, taken from Kimura & Budnitz (1987), is presented in Table VI.1. This ranking was based on factors that determine the magnitude of the hazard such as (1) the amount of energy released in an explosion or fire or (2) the amount of toxic material released. These factors include:

- amount of hazardous material carried by each transportation mode shipment
- speed of each transportation mode
- mode vehicle weight
- transportation mode route distance to the plant.

"Direct collisions" are considered to be actual collisions by vehicles with plant structures within the exclusion area. Since pipelines cannot move, direct collisions do not apply. Accidents "near" the plant are considered to be transportation accidents outside the plant exclusion area but within five miles of the reactor containment. (According to the NRC Standard Review Plan, a transportation accident within a 5-mile plant radius is considered to be at least a potential hazard.) "Minor hazards" in Table VI.1 are dismissed from further consideration. "Medium hazards", according to Kimura and Budnitz (1987), may need investigation, while "major hazards" definitely need further investigation from a risk assessment viewpoint.

VI.C Transportation Fault Tree

Figure VI-1 is a top level fault tree (also referred to as a master logic diagram). Figure VI-1 has six sheets. The fault tree serves as a focusing tool for the important events to be identified in transportation risk analysis. There are 60 end events (i.e., basic events) in this fault tree. This means that frequencies/conditional probabilities would have to be obtained for 60 events if this fault tree is to be quantified.

These events are labeled E1 through E60. The transportation mode is indicated for each initiating event. Sheet 1 depicts the three generic ways by which a core melt accident can develop:

- direct vehicle impact (within exclusion area)
- direct vehicle impact with hazardous cargo aboard (within exclusion area)

- vehicle accident within plant vicinity with hazardous cargo aboard (outside exclusion area but inside a five-mile plant radius).

A direct vehicle impact means an accident within the exclusion area of the plant. An accident within the plant vicinity means an accident outside the exclusion area but within the five mile radius of the plant.

Sheet 1 of the fault tree shows that direct vehicle impact can be caused, for example, by airplane crashes or by barge/ship collisions with an intake structure (event E1). The conditional probability of major structural damage given direct impact (event E2) is needed for fault tree quantification.

Sheets 2 and 3 depict the possible events that can occur by direct vehicle impact with hazardous cargo on board. A hazardous cargo is any cargo which can detonate, burn, burn and release fumes/smoke, or release toxic vapors/gas. This includes (1) solid material such as dynamite or explosives, (2) liquids such as petroleum products, or (3) gas such as chlorine. The two transportation modes considered in this case are marine and aviation, since both can hit the plant directly with fuel on board. (In addition, barges/ships can carry other hazardous cargo as described above.)

Sheet 2 describes the potential explosion or fire that can occur with a direct vehicle impact. Events E3 AND E4, and E7 AND E8 represent accident initiating events. Events E5, E6, E9 and E10 represent conditions and responses that are necessary for plant damage to occur.

Sheet 3 describes the possible injury modes for the operators or other onsite personnel:

- trauma from falling objects, shrapnel from explosions
- burns due to fires or explosions
- asphyxiation due to fires/explosions (oxygen denial, smoke)
- poisoning due to toxic gas.

Mitigation measures against toxic gas poisoning include control room isolation.

Sheets 4, 5 and 6 describe transportation accidents that can occur within the plant vicinity. These are similar in development to sheets 2 and 3 with the following exceptions:

- aircraft carry little or no toxic material on board, so

if the aircraft does not hit the plant, it is assumed that there is no plant hazard

- o flammable solid materials, unlike flammable liquids or gases, cannot drift toward the plant before detonation

- o flame fronts or shock waves can be generated at various distances from the plant depending upon the location of the accident and cloud drift; the conditional probability of plant damage must be calculated, given that these flame fronts or shocks waves are generated at a specified distance.

- o there is more time for operator mitigation, such as control room isolation, for events involving toxic gas release or smoke/fume release from fires.

VI.D Accident Frequencies Near the Site

As described in the previous section, the frequency of transportation accidents near the plant site must be calculated in order to quantify the fault trees shown on sheets 4, 5 and 6 of Figure VI.1.

Generally, accident rates are tabulated in terms of vehicle-miles. In order to determine the frequency of transportation accidents near the plant site, the number of vehicle-miles per year near the plant must be determined. As described above, an area of radius 5 miles is used.

Next, the length of the transportation route within the 5 mile radius must be calculated. As shown in Figure VI.2, the offset distance D must be known. The vehicle hazard distance L is defined by the distance that is traveled by vehicles which are a potential hazard to the plant and are within 5 miles of the plant site. If the offset distance D of a transportation route is zero, then the vehicle hazard distance is 10 miles because the transportation route goes through the plant site and all vehicles that travel on that route within 5 miles of the plant must be considered a hazard.

As shown on Figure VI.2, the expression for the vehicle hazard distance L is given by:

$$L = (100 - 4 \times D^2)^{1/2} .$$

Once the vehicle hazard distance for a transportation route near the site has been determined, then the number of vehicles that travel that route per year must be determined. The number of vehicle miles is then

$$\text{Vehicle Miles/Year} = L \times \text{No. of shipments/year.}$$

Finally, the frequency of transportation accidents within five miles of a plant site is then:

$$\begin{array}{lcll} \text{Transportation Accidents per year within 5 miles of site} & = & \text{Vehicle Miles per year within 5 miles of site} & \times \text{Vehicle Accident Rate} \end{array}$$

The vehicle accident rate data must be obtained for each transportation mode.

VI.E References

Chelapati, Kennedy and Wall, 1972: "Probabilistic Assessment of Aircraft Hazard for Nuclear Power Plants," Nuclear Engineering and Design, Vol. 19, pg. 333-364 (1972)

Kimura and Budnitz, 1987: C.Y. Kimura and R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States", Report NUREG/CR-5042, Lawrence Livermore National Laboratory and U.S. Nuclear Regulatory Commission (1987)

Indian Point, 1983: Consolidated Edison Company and Power Authority of the State of New York and Pickard, Lowe & Garrick, Inc., "Indian Point Probabilistic Safety Study" (1983)

Waterford 3 SER, 1981: "Safety Evaluation Report Related to the Operation of Waterford Steam Electric Station, Unit No. 3", Report NUREG-0787, U. S. Nuclear Regulatory Commission (1981)

TABLE VI.1

(From Kimura and Budnitz, 1987)

POTENTIAL HAZARDS FROM TRANSPORTATION ACCIDENTS TO NUCLEAR POWER PLANTS

Transportation Mode	Accidents within Plant Exclusion Area			Accidents Outside of Exclusion Area But Within Five Miles of Reactor Containment(s)	
	Direct Collision with Plant Structures	Explosion, Fire Release	Hazardous Material Release	Explosion, Fire	Hazardous Material
Aviation	Major	Major	Minor	Minor	Minor
Marine	Major	Major	Major	Major	Major
Pipeline	N.A.	Major	Major	Major	Major
Railroad	Minor	Major	Major	Major	Major
Truck	Minor	Medium	Medium	Medium	Medium

N.A. = Not Applicable
Minor = Not Investigated Further
Medium = May Need To Be Investigated Further
Major = Should Be Investigated Further

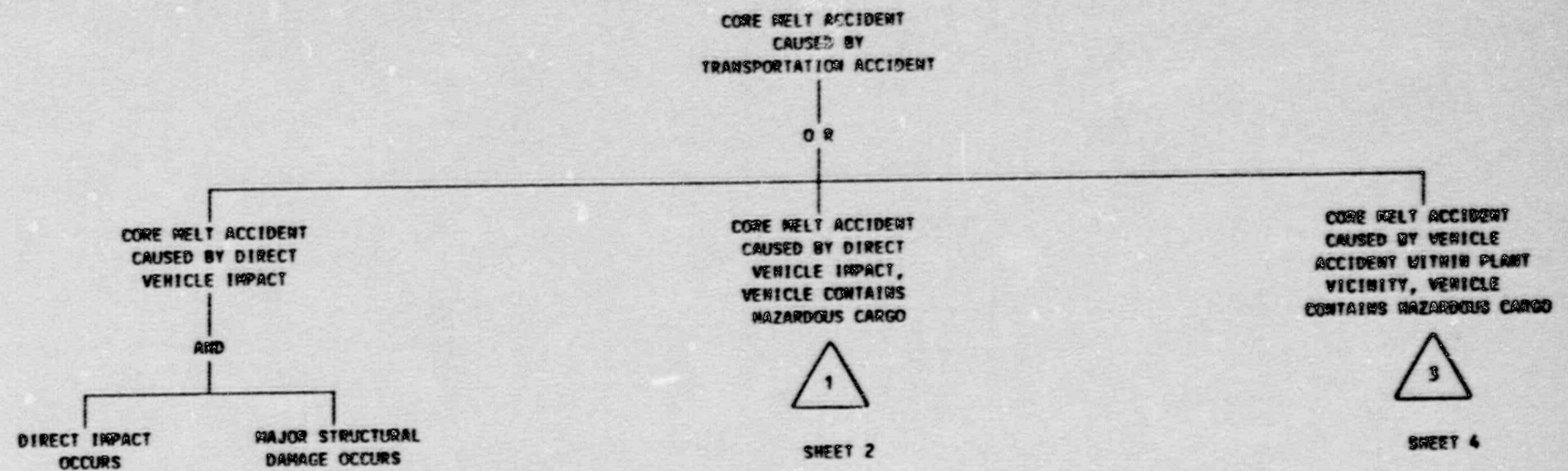


FIGURE VI-1 -- MASTER LOGIC DIAGRAM
(SHEET 1)

DIRECT IMPACT

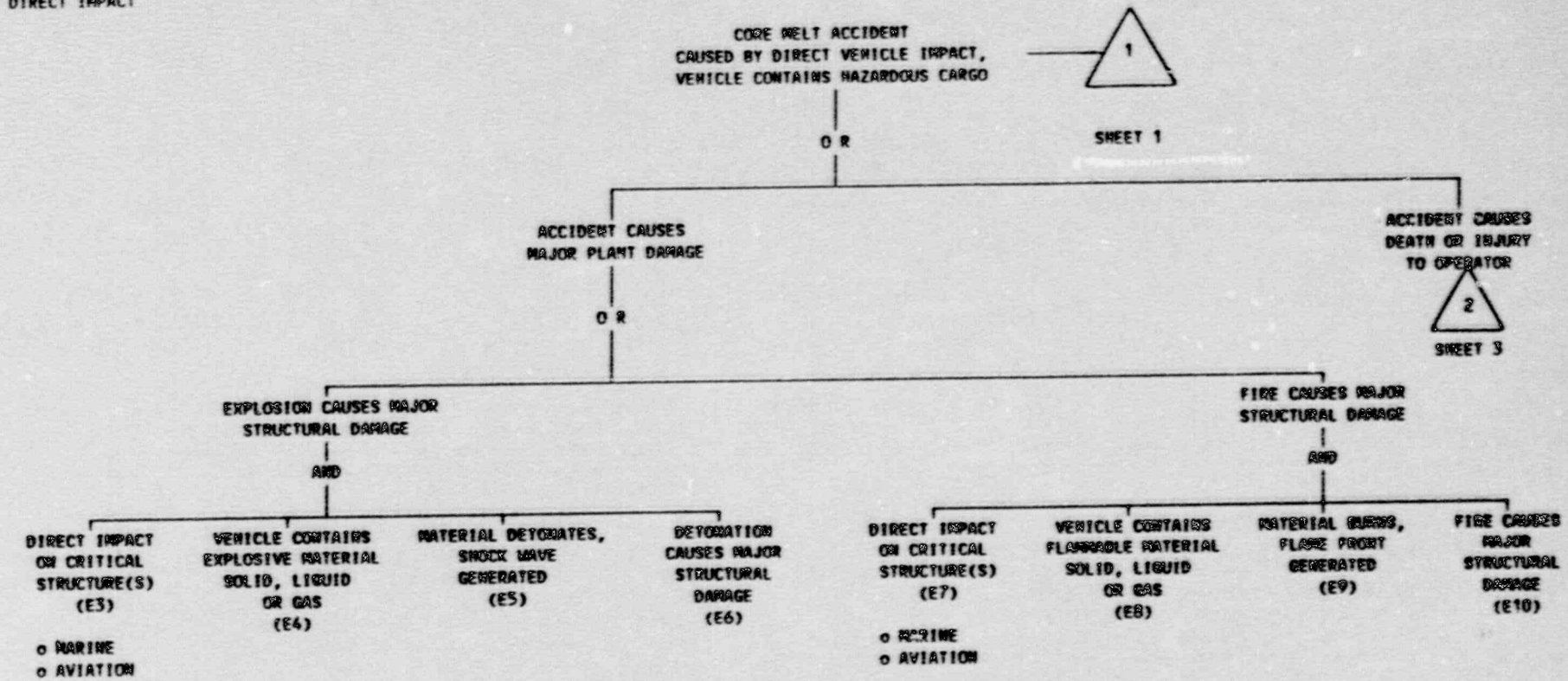
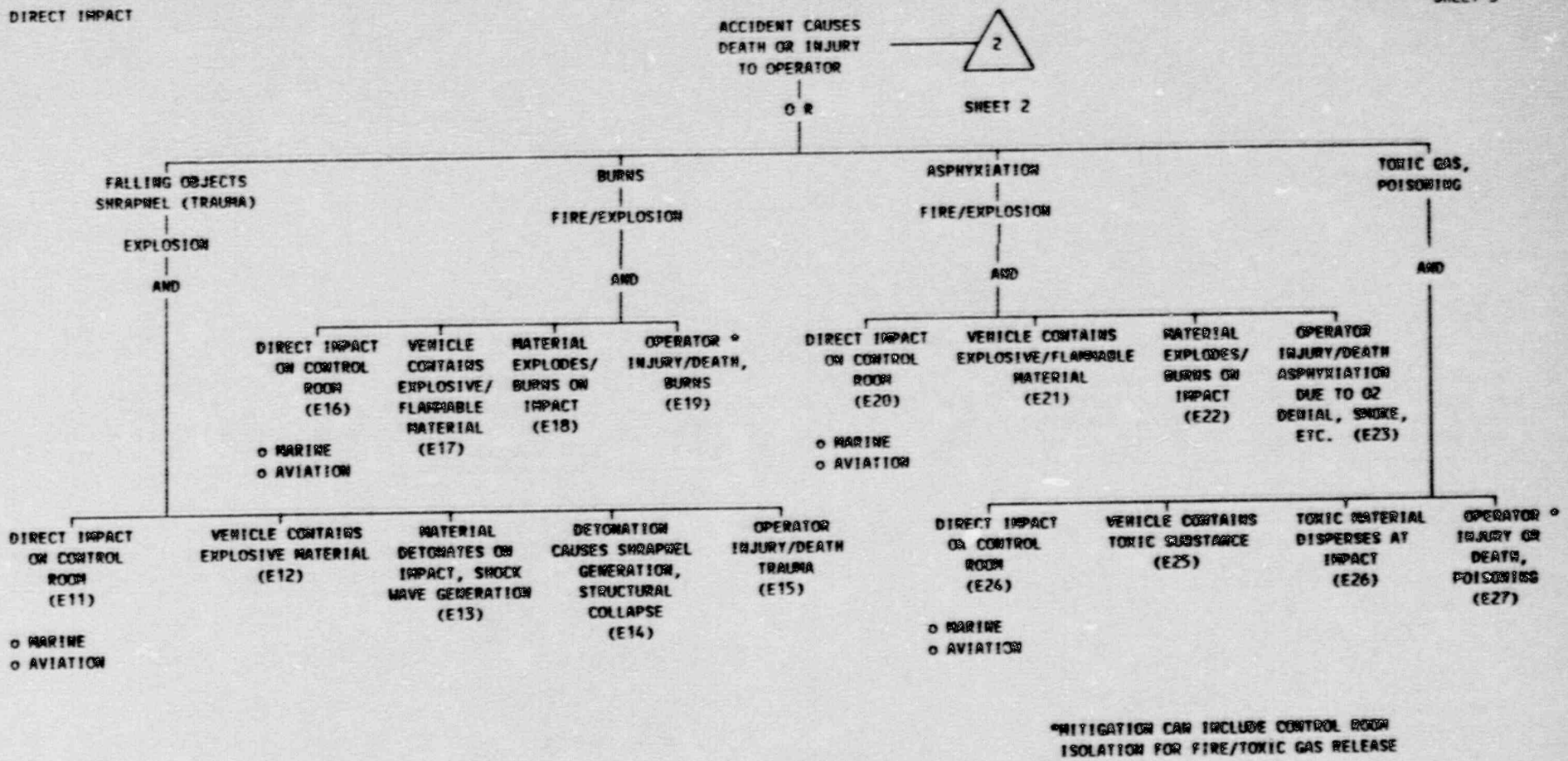


FIGURE VI-1 -- MASTER LOGIC DIAGRAM
(SHEET 2)

DIRECT IMPACT



*MITIGATION CAN INCLUDE CONTROL ROOM ISOLATION FOR FIRE/TOXIC GAS RELEASE

FIGURE VI-1 -- MASTER LOGIC DIAGRAM (SHEET 3)

ACCIDENT WITHIN PLANT VICINITY

CORE MELT ACCIDENT CAUSED BY VEHICLE ACCIDENT WITHIN PLANT VICINITY, VEHICLE CONTAINS HAZARDOUS CARGO

SHEET 1

O R

ACCIDENT CAUSES MAJOR PLANT DAMAGE

O R

EXPLOSION CAUSES MAJOR STRUCTURAL DAMAGE

O R

EXPLOSION CAUSES MAJOR STRUCTURAL DAMAGE (SOLID EXPLOSIVE MATERIAL)

AND

VEHICLE ACCIDENT (E28)

- MARINE
- RAILROAD
- TRUCK

VEHICLE CONTAINS SOLID EXPLOSIVE MATERIAL (E29)

SOLID DETONATES, SHOCK WAVE GENERATED, AT DISTANCE "X" (E30)

MAJOR STRUCTURAL DAMAGE OCCURS (E31)

EXPLOSION CAUSES MAJOR STRUCTURAL DAMAGE (LIQUID/GAS EXPLOSIVE MATERIAL)

AND

VEHICLE ACCIDENT (E32)

- MARINE
- RAILROAD
- TRUCK
- PIPELINE

VEHICLE CONTAINS LIQUID/GAS EXPLOSIVE MATERIAL (E33)

LIQUID GAS DETONATES,* SHOCK WAVE GENERATED, AT DISTANCE "Y" (E34)

MAJOR STRUCTURAL DAMAGE OCCURS (E35)

FIRE CAUSES MAJOR STRUCTURAL DAMAGE

SHEET 5

ACCIDENT CAUSES DEATH OR INJURY TO OPERATOR

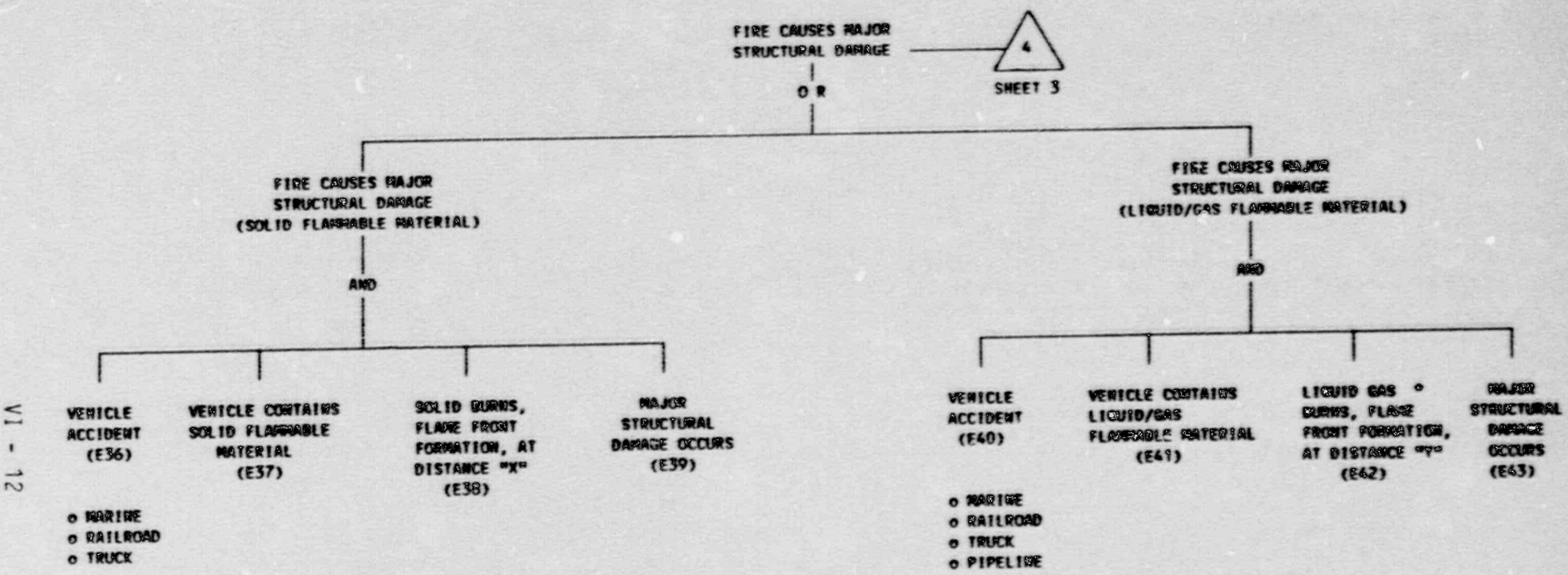
SHEET 6

* CLOUD CAN DRIFT TOWARDS PLANT BEFORE DETONATION

FIGURE VI-1 -- MASTER LOGIC DIAGRAM (SHEET 4)

ACCIDENT WITHIN
PLANT VICINITY

SHEET 5



* GAS/VAPOR CLOUD CAN DRIFT TOWARDS PLANT

FIGURE VI-1 -- MASTER LOGIC DIAGRAM
(SHEET 5)

ACCIDENT WITHIN PLANT VICINITY

ACCIDENT CAUSES DEATH OR INJURY TO OPERATOR

6

SHEET 5

O R

FALLING OBJECTS SHRAPNEL (TRAUMA)

EXPLOSION

AND

- VEHICLE ACCIDENT (E44)
  - o MARINE
  - o RAILROAD
  - o TRUCK
  - o PIPELINE
- VEHICLE CONTAINS EXPLOSIVE MATERIAL (E45)
- MATERIAL DETONATES, SHOCK WAVE FORMATION, SOLID AT DISTANCE "X" (LIQUID/GAS AT DISTANCE "Y") * (E46)
- DETONATION CAUSES SHRAPNEL GENERATION, STRUTURAL COLLAPSE (E47)
- OPERATOR INJURY/DEATH TRAUMA (E48)

BURNS

FIRE/EXPLOSION

AND

- VEHICLE ACCIDENT (E49)
  - o MARINE
  - o RAILROAD
  - o TRUCK
  - o PIPELINE
- VEHICLE CONTAINS EXPLOSIVE/ FLAMMABLE MATERIAL (E50)
- MATERIAL EXPLODES/ BURNS, SOLID AT DISTANCE "X" (LIQUID/GAS AT DISTANCE "Y")* (E51)
- OPERATOR INJURY/ DEATH, BURNS (E52)

ASPHYXIATION

FIRE/EXPLOSION

AND

- VEHICLE ACCIDENT (E53)
  - o MARINE
  - o RAILROAD
  - o TRUCK
  - o PIPELINE
- VEHICLE CONTAINS EXPLOSIVE/ FLAMMABLE MATERIAL (E54)
- MATERIAL EXPLODES/BURNS, SHOCK WAVE FORMATION, SOLID AT DISTANCE "X" (LIQUID/GAS AT DISTANCE "Y") * (E55)
- OPERATOR ** INJURY/ DEATH, ASPHIXIATION DUE TO O2 DENIAL, SMOKE, ETC. (E56)

TOXIC GAS, POISONING

AND

- VEHICLE ACCIDENT (E57)
  - o MARINE
  - o RAILROAD
  - o TRUCK
  - o PIPELINE
- VEHICLE CONTAINS TOXIC SUBSTANCE (E58)
- TOXIC MATERIAL DISPERSES AND CLOUD DRIFTS TOWARDS PLANT (E59)
- OPERATOR ** INJURY OR DEATH, POISONING (E60)

* CLOUD CAN DRIFT BEFORE DETONATION/COMBUSTION

** MITIGATION CAN INCLUDE CONTROL ROOM ISOLATION FOR FIRE/TOXIC GAS RELEASE

FIGURE VI-1 -- MASTER LOGIC DIAGRAM (SHEET 6)

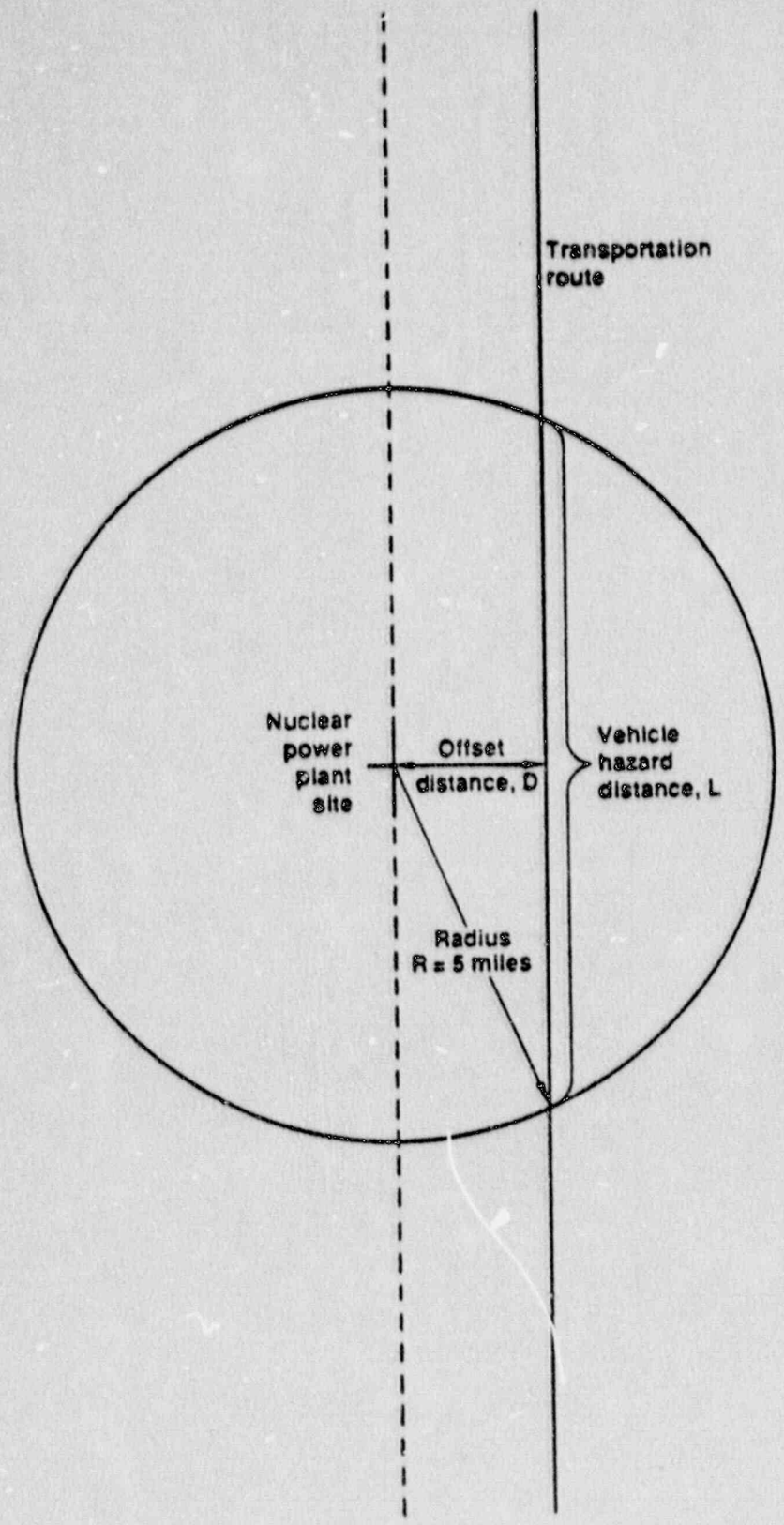


Figure VI.2 -- Vehicle Hazard Distance Determination

VII. ACKNOWLEDGMENTS

This project has been supported by the Office of Nuclear Regulatory Research of the U.S. Nuclear Regulatory Commission, under NRC's Small Business Innovation Research Program. The authors are grateful to Nilesh C. Chokshi, the NRC technical contact, for his support throughout this project.

M.K. Ravindra of EQE Inc. and R.C. Murray, C.Y. Kimura, and D.H. Chung of Lawrence Livermore National Laboratory provided assistance during the execution of the work, and their contributions are gratefully acknowledged.

One of us (RJB) wishes to offer special thanks to J.A. Murphy of NRC for more than 15 years of innovative contributions to the discipline of PRA across the whole spectrum of methodologies, which contributions have been a source of continuing inspiration for his own PRA work.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-5477

2. TITLE AND SUBTITLE

An Evaluation of the Reliability and Usefullness of External-Initiator PRA Methodologies

3. DATE REPORT PUBLISHED

MONTH: January YEAR: 1990

4. FIN OR GRANT NUMBER

D2506

5. AUTHOR(S)

R. J. Budnitz and H. E. Lambert

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

October 1 - May 15, 1989

8. PERFORMING ORGANIZATION – NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Future Resources Associates, Inc.
2000 Center Street, Suite 418
Berkeley, CA 94704

9. SPONSORING ORGANIZATION – NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This report, prepared to assist policy-level decision-makers, evaluates the extent to which each category of external-initiators PRA methodology produces reliable and useful results and insights, at its current state-of-the-art level. This report addresses this need in the following five categories of external initiators: (1) earthquakes; (2) internal fires; (3) external floods; (4) extreme winds; and (5) transportation accidents. Each initiator is examined separately. The thrust is to identify and describe the principal aspects of the current state-of-the-art PRA methodology, what aspects are less robust and therefore provide less reliable insights, and why.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

PRA
external events
decision-making

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page) unclassified

(This Report) unclassified

15. NUMBER OF PAGES

16. PRICE

NUREG/CR-5477

AN EVALUATION OF THE RELIABILITY AND USEFULNESS OF EXTERNAL-INITIATOR PRA METHODOLOGIES

JANUARY 1990