Copy______
PLG-0525
Volume 2

Three Mile Island Unit 1
Probabilistic Risk Assessment

TECHNICAL SUMMARY REPORT

Project Director
B. John Garrick

Project Manager
Douglas C. Iden

Principal Investigator
Frank R. Hubbard

Task Leaders
Mardyros Kazarians
Ali Mosleh
Harold F. Perla
Martin B. Sattison
Donald J. Wakefield

Prepared for
GPU NUCLEAR CORPORATION
Parsippany, New Jersey
November 1987

Pickard, Lowe and Garrick, Inc.
Engineers • Applied Scientists • Management Consultants
Newport Beach, CA Washington, DC

NOTICE

This is a report of work conducted by individual(s) and contractors for use by GPU Nuclear Corporation. Neither GPU Nuclear Corporation nor the authors of the report warrant that the report is complete or accurate. Nothing contained in the report establishes company policy or constitutes a commitment by GPU Nuclear Corporation.

SUMMARY OF CONTENTS

CONTENTS

CONTENTS (continued)

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

Abbreviation	Definition
ACR	air-cooled reactor
AFW	auxiliary feedwater
ADV	atmospheric dump valve
AOV	air-operated valve
ATOG	abnormal transient operational guidelines
ATWS	anticipated transient without scram
B&W	Babcock & Wilcox Company
BOP	balance of plant
Btu	British thermal unit
BWR	boiling water reactor
BWST	borated water storage tank
CARS	condenser air removal system
CAS	chemical addition system
CBV	control building ventilation
CBVS	control building ventilation system
CCF	common cause failure
CDF	cumulative distribution function
CFT	core flooding tank
CIV	containment isolation valve
CSF	conditional split fraction
CST	condensate storage tank
CRO	control room operator
CWS	circulating water system
DHCCW	decay heat closed cooling water
DHR	decay heat removal
DHRS	decay heat removal system
DHRW	decay heat river water
DPD	discrete probability distribution
EEHR	Environmental and External Hazards Report
EFW	emergency feedwater
EOF	emergency operations facility
EPRI	Electric Power Research Institute
ESAS	engineered safeguards actuation system
ESD	event sequence diagram
ESF	engineered safety feature
ETC	event tree code
FHA	fire hazards analysis
FSAR	Final Safety Analysis Report
FTAP	Fault Tree Analysis Program
GCR	gas-cooled reactor
GPUN	GPU Nuclear Corporation

LIST OF ACRONYMS (continued)

Abbreviation	Definition
HCR	human cognitive reliability
HPI	high pressure injection
HPIS	high pressure injection system
HVAC	heating, ventilating, and air conditioning
ICCS	intermediate closed cooling system
ICCW	intermediate closed cooling water
ICS	integrated control system
LBIS	line break isolation system
LCO	limiting condition for operation
LER	Licensee Event Report
LOCA	loss of coolant accident
LOFW	loss of main feedwater
LONS	loss of nuclear services
LORI	loss of reactor coolant system inventory
LORW	loss of river water
LOSP	loss of offsite power
LPI	low pressure injection
LPIS	low pressure injection system
LSS	low speed stop
MCC	motor control center
MFPT	main feedwater pump trip
MFW	main feedwater
MGL	multiple Greek letter
MOV	motor-operated valve
MSIV	main steam isolation valve
MSLB	main steam line break
MSS	main steam system
MSSV	main steam safety valve
MSV	main steam valve
MUP	makeup and purification
NPE	Nuclear Power Experience
NRC	U.S. Nuclear Regulatory Commission
NSCCS	nuclear services closed cooling system
NSCCW	nuclear services closed cooling water
NSRW	nuclear services river water
NSSS	nuclear steam supply system
OPM	Operations Plant Manual
OTSG	once-through steam generator
PCL	panel center left
PCR	panel center right
PDF	probability density function
PDS	plant damage state

LIST OF ACRONYMS (continued)

Abbreviation	Definition
PLF	panel left front
PLG	Pickard, Lowe and Garrick, Inc.
P&ID	piping and instrumentation drawing
PMR	Plant Model Report
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PRF	panel right front
PSHX	primary to secondary heat transfer
PSV	pressurizer safety valve
PTS	pressurized thermal shock
PWR	pressurized water reactor
RBCU	reactor building cooler unit
RBEC	reactor building emergency cooling
RBD	reliability block diagram
RBS	reactor building spray
RBSS	reactor building spray system
RCDT	reactor coolant drain tank
RCP	reactor coolant pump
RCS	reactor coolant system
RPS	reactor protection system
RSS	Reactor Safety Study
SCCW	secondary closed cooling water
SCM	subcooled margin
SGTR	steam generator tube rupture
SLB	steam line break
SLRDS	steam line rupture detection system
SRO	senior reactor operator
SRW	secondary river water
SSCCS	secondary services closed cooling system
SSE	safe shutdown earthquake
SSS	support state system
STA	shift technical advisor
TBV	turbine bypass valve
TMI-1	Three Mile Island Nuclear Generating Station, Unit 1
TPRA	TMI-1 probabilistic risk assessment
TSR	Technical Summary Report
ULD	unit load demand

1. INTRODUCTION

This document, the Technical Summary Report of the probabilistic risk assessment of TMI-1, is intended to provide an overview of the PRA performed by Pickard, Lowe and Garrick, Inc., and General Public Utilities Nuclear Corporation of the Three Mile Island Nuclear Station Unit 1. This section describes the background and the objectives of the study. Also described briefly is the approach followed in performing the PRA. The section ends with a summary of the contents of this document and of the individual sections and a treatment of current industry safety issues.

1.1 BACKGROUND

The TMI-1 PRA was undertaken by GPUN in the fall of 1983. The consulting firm of PLG was retained as the primary contractor for the conduct of the study. Its terms of reference were a Level 1 PRA, as defined by the PRA Procedures Guide (Reference 1-1), and treatment of external events. GPUN's motivation for undertaking such a study was the desire to adopt the PRA as a risk management tool in management decision making that would address issues of multiple objectives, including safety, plant availability, and economic costs and benefits.

1.2 OBJECTIVES

The overall objectives of the TMI-1 PRA were to:

- Perform an independent and plant-specific assessment of the level of safety of the operation of TMI-1 to ensure that GPUN is carrying out its corporate responsibility to generate electricity in a manner that affords adequate protection for the health and safety of its employees and the public.

- Improve GPU Nuclear's functional capabilities to use PRA as a tool for decision making and resource allocation for possible modifications to the plant configuration, operation, maintenance, and emergency planning.

- Provide a quantitative measure of risk independent of regulatory criteria with the documentation of results and methods in a form suitable for detailed technical review and public presentation.

To meet these objectives, specific goals in the course of the PRA have been to:

- Develop a quantitative assessment of the safety of TMI-1 in terms of accident sequences, their consequences, and the associated uncertainty.

- Identify the significant contributors to risk, considering accident precursors both internal and external to the plant.

- Rank plant systems and components quantitatively in terms of their impact on overall plant safety.

- Develop a plant risk model (including system models) and the tools for its eventual modification by GPUN in future TMI-1 risk management applications.

- Develop and organize a data base, with provisions for periodic updating, consistent with the requirements of the plant risk model and its tools.

- Establish a plan whereby GPUN can periodically update the TMI-1 risk assessment independently.

- Establish a plan by which GPUN, using in-house resources, can formally incorporate the methods and results of the risk assessment in the decision-making and resource allocation process for TMI-1.

1.3 SCOPE OF PRA

The TMI-1 probabilistic risk assessment is a plant-specific assessment of core damage and plant damage state frequency including simple initiators such as pipe breaks as well as the effect of floods, earthquakes, fires, and other more complex initiating events. It includes consideration of all alleviating* systems and all systems whose performance might adversely impact the consequences of an initiating event. Both so-called safety and nonsafety systems were considered for any favorable or unfavorable contribution they might make to influence the frequency of core damage at TMI-1 during normal operations. Containment safety features were included as well. The support systems, including ventilation, cooling water, and electric power systems, were given particular attention because of their greater risk potential.

Current emergency, operating, and maintenance procedures were analyzed in detail to ensure accurate predictions of the likelihood of both beneficial and deleterious operator actions. Both normal mitigating actions and actions to recover failed systems were considered along with a few errors of commission; i.e., instances wherein misleading indications might cause an operator to intrude and make things worse.

All analysis assumptions were reviewed with GPUN personnel prior to their incorporation into the PRA model. The nominal performance of the plant in response to all initiating events was reviewed in detail on the basis of event sequence diagrams by personnel from GPUN over a number of months. All assumptions about operator response included in the human actions analysis were also reviewed extensively at TMI. Plant-specific data were gathered from the TMI archives on operating logs, tag-out records, and the like to ensure that the data base used for estimating system performance and initiating event frequency reflected TMI's operating history.

*The term "alleviating" is used throughout the TMI-1 PRA reports in Webster's New Collegiate Dictionary sense of "b. to partially remove or correct." Other synonymous terms such as "mitigate" are reserved for other special applications, such as, "to mitigate the consequences of core damage."

Much time was spent at the plant walking down systems to ensure that the drawings used for systems analysis accurately represented the as-built plant configuration. The systems analysis performed for this PRA was based on PLG's extensive previous experience with the analysis of the B&W plants. The TMI-1 system models and split fractions were different from those used for any other plant that PLG has examined.

In a truly plant-specific risk assessment such as this, each new plant seems to reveal its own set of dominant risk contributors. Consequently, we found it wise to conduct this PRA in two phases to accelerate the process of learning TMI-1 plant-specific design and operations and to identify issues requiring technical resolution by GPUN and PLG as early as possible. Phase I was an abbreviated though comprehensive scoping analysis intended to facilitate a more detailed and lengthy second phase. The conduct of Phase I consisted of an approximate or focusing PRA to give early warning of those systems and assumptions that require more information or more detailed analysis prior to their incorporation in the final risk model. In the case of TMI, for instance, the control building ventilation system was found to be one whose failure would lead directly to core damage, but little was known about its failure history; for example, given system failure, it was not known how long it would take to heat up the rooms, at what temperature components in these rooms would begin to fail, etc. The results of Phase I precipitated a study that lasted more than a year prior to incorporation of these issues in the detailed Phase II PRA model.

Phase II analyzed very closely the systems and scenarios important to plant safety with the ultimate goal of determining if any design or operation changes are recommended. The Phase II risk model evolved over 2 years including four major revisions to reflect the expected TMI plant performance accurately. Each major revision was followed by further analysis to refine assumptions about plant systems and operator performance. In fact, to date, this PRA contains the most extensive set of operator actions ever incorporated in any PRA. These varied from the calibration of sensors to manual actuation of failed systems for which automatic actuation was not available.

In addition to producing the risk model, the scope of the PRA included the transfer of PRA technology including the use of all computer codes on the GPUN computer system for complete quantification. These codes were packaged in a set, a subset of which was developed specifically to simplify the quantification of the TMI PRA model.

As part of the technology transfer, all the members of the Technical Functions Risk Analysis Group were exposed to most aspects of the generation and the quantification of the TMI risk model. They have participated actively in all aspects of the PRA from performing systems analysis and event trees to quantifying them. The Technical Functions Risk Analysis Group was more involved in this process than any other utility group with which PLG has worked. The input of its members contributed significantly to the flavor and the perspective of this PRA.

Most of the initial effort on the TMI PRA used the mean values to estimate the uncertainty in all calculations. In the final analysis, the full probability of frequency distributions for component failure rates and initiating event occurrence rates were used to represent uncertainty. These distributions were then propagated through the model to produce uncertainty distributions on the scenario and core damage frequencies.

The TMI-1 PRA produced three products:

1. A set of final reports, including this summary report and an executive summary.

2. The PRA model, including event trees, system models, and computer code input.

3. Recommendations to reduce risk through changes suggested to procedures and equipment at TMI-1 during the course of the study.

1.4 REPORT ORGANIZATION

The TMI-1 PRA results are documented in seven detailed reports, each one consisting of one or more volumes and an executive summary. This technical summary is the first report. The others are:

- Plant Model Report
- Systems Analysis Report
- Data Analysis Report
- Environmental and External Hazards Report
- Human Actions Analysis Report

Separate reports were developed to reflect the major tasks of the risk assessment and to facilitate parallel preparation and review of task documentation. Most tasks were interactive; only the Plant Model Report depended extensively on the results of all other tasks.

1.4.1 TECHNICAL SUMMARY REPORT

The purpose of the Technical Summary Report is to provide, in a single coherent volume, a description of the main elements of the TMI-1 PRA and its results. If a reader only has a limited amount of time and wants to know in general terms what this PRA is all about, he should read this report. It is hoped it will whet his curiosity for reading more of the details in the other volumes of this report. Most of the why and how of this PRA is described in the detailed reports.

Section 1 of the Technical Summary Report describes the background, objectives, and scope of this PRA. Section 2 describes the historical perspective and technical background for the use of the PRA and for its methods. Section 3 and Appendix A briefly describe the plant; the safety functions used in this PRA and the relationship between the plant as analyzed and as it currently exists are also described in Section 3. Section 4 describes PLG's general PRA methodology and some of the specifics of how that general methodology was applied to TMI-1. Section 5 summarizes the results of the PRA. Appendix B contains some details of the PRA methodology contained in the individual reports.

1.4.2 PLANT MODEL REPORT

The Plant Model Report contains a description of all the event sequence diagrams and event trees defining the scenarios that make up the plant model for TMI-1. It describes the initiating events, the plant damage states, and the detailed results.

Section 1 puts the plant model into the general perspective of the risk assessment methodology described in Section 4 of this Technical Summary Report. The initiating events and support system model are described in Sections 2 and 3, respectively. Section 4 of the Plant Model Report describes the three-segment plant model and presents each frontline system event tree. Success criteria are described in Section 4.1.2. Section 5 defines the plant model end states or plant damage states used in the PRA, and Section 6 presents detailed results from the quantification of scenario and of core damage frequencies.

1.4.3 SYSTEM ANALYSIS REPORT

The Systems Analysis Report presents all of the system performance models used to calculate the numbers used for evaluating the event trees and thereby producing scenario frequencies. In addition, the interactions between systems are specified. The report first breaks down all systems into three categories (frontline, support, and systems of lesser consequence to the PRA that were not analyzed). Section 1 presents an overview of the calculational procedures used in the analysis, and Sections 2 through 17 each present the analysis of one of the 16 systems that were analyzed in detail.

1.4.4 DATA ANALYSIS REPORT

The Data Analysis Report presents the basic component data base developed for use in the TMI-1 PRA systems and initiating event frequency analysis. Section 4.5.2.3 of this report provides a discussion of some of the techniques used and steps taken in developing the data base.

Section 1 of the Data Analysis Report presents four general areas comprising the scope of the data analysis; namely, component failure rates, common cause failure parameters, component maintenance frequency and duration, and initiating event frequencies. Section 2 describes the general data analysis approach used for each of these areas. This approach is based on the concept of generic data usage. Section 3 provides TMI-1 plant-specific operating data as the cornerstone for a Bayesian update of the data estimates.

Several other types of data, such as component fragility curves used in the seismic analysis, fire frequencies used in the fire analysis, and human actions, are developed and presented elsewhere in the TMI-1 PRA Environmental and External Hazards Report.

1.4.5 ENVIRONMENTAL AND EXTERNAL HAZARDS REPORT

The Environmental and External Hazards Report presents a probabilistic evaluation of the impact of environmental and external hazards on TMI-1. Environmental hazards are equipment failure causes whose sources are within the plant boundaries and through which environmental interactions may simultaneously affect several plant components; e.g., fire, internal flood, steam, etc. External hazards, on the other hand, are causes of equipment failure that originate outside of the plant boundaries; e.g., earthquakes, external floods, aircraft crashes, etc.

Section 1 lists all of the hazards considered and explains the reasons for either their inclusion in or exclusion from the analysis. Section 2 addresses seismic analysis. It describes the seismicity of the site and the fragility of key building and equipment during an earthquake. The seismic analysis is then conducted on the basis of this information to determine the seismic contribution to plant damage state frequency. Section 3 describes the analysis of spatial interactions involving such environmental hazards as fire, flood, and steam that can cause intersystem dependent failures. Sections 4 through 8 treat external hazards exclusively, including flooding from external sources, extreme weather phenomena, turbine missiles, aircraft crashes, and hazardous chemicals, respectively.

1.4.6 HUMAN ACTIONS ANALYSIS REPORT

The Human Actions Analysis Report evaluates operator performance as it relates to the frequency of accident scenarios, the object of the evaluation being a quantification of the frequency of selected human actions to delineate the human contribution to the plant damage state frequencies.

Section 1 categorizes different types of human actions according to the timing of the action. These include human actions termed routine, inadvertant, dynamic, and recovery. Section 2 describes the methodology for the analysis and evaluation of these operator actions. Section 3 presents the conduct of operations at TMI-1, particularly the relationship of available, qualified manpower to man plant control stations in the event of an emergency. Finally, Section 4 documents the quantification of each identified human action.

1.5 TREATMENT OF CURRENT INDUSTRY ISSUES

This section describes selected issues that are currently of concern to the nuclear community and describes where and how they are addressed in the TMI-1 PRA. Table 1-1 lists these issues and identifies where in this section each is discussed. Table 1-1 also serves to begin the process of putting these issues into a context by grouping similar ones together.

1.5.1 DEPENDENCE

This section first defines dependence and describes various ways in which it is treated in the TMI-1 PRA (Section 1.5.1.1). Next, it responds to each of four terms currently used, sometimes erroneously, to discuss dependence and tells how they fit in.

1.5.1.1 Treatment in TMI-1 PRA

The concept of dependence is important to both probability theory and probabilistic risk assessment. In fact, it is the modeling of the dependence among the large number of plant components in TMI-1 that makes the PRA job complicated. If every component failure were to affect only a single component at a time, the reactor core would probably never be seriously threatened. As a matter of fact, it would require the unfortuitous coincidence of several of these failures before an accident could produce serious consequences, and such "independent" coincidences are truly rare. There would still be a need to model the logic of such a coincidence to account for its impact on the plant, but this effort would be relatively simple. Generally, no one component failure would, by itself, result in core damage. Typically, core damage involves the failure of multiple components, either if one failure led to another or if one condition caused more than one failure.

A dependent event is a system action or physical condition in an event sequence (scenario), the likelihood of which is changed by the events that precede it or by the conditions that exist when the event is expected to occur. In general, the likelihood of each event in a scenario is conditioned by each event that has occurred previously. As will be seen later, sometimes the impact of previous events is not significant. In other cases, previous events may preclude the subsequent ones. Such events are cf particular concern.

The joint likelihood of two or more events occurring simultaneously but independently is usually so small that it is not important to risk. For example, two independent events that each have a likelihood of 1 chance in 1,000 of occurring, have a joint likelihood of 1 chance in 1,000,000 of occurring, a number probably too small to warrant further consideration. Therefore, the TMI-1 PRA focuses its attention more on dependent events, on cascades or clumps of events, and on multiple events that result from each other or from the same cause. This cause can be a condition in the plant, such as from an initiating event, from environmental conditions, or from the state of plant parameters, or it can be a similar manufacturer for a component. In the example cited above, a dependent failure would manifest itself in the likelihood of occurrence of one event being dependent on whether the cther event had occurred. If the degree of coupling (dependence) between the failures is strong, then the joint likelihood of both events in the previous example occurring may be closer to 1 chance in 1,000. This report relies on the well established concepts and terminology of probability theory and logic modeling to deal with dependent events. One exception is the term "common cause failure." This term is used to describe possibly unforeseen or deliberately unmodeled aspects of system design that could lead to the joint failure of two components, which would more likely than the joint probability of their failing independently. The systems analysis block diagrams (see System Analysis Report) include explicit "common cause failure" terms.

The concept of dependence is considered in many places and at many levels of the study, including:

- Initiating Events. Each initiating event is carefully examined to determine which of the alleviating systems needed may be disabled as a direct consequence of the initiating event itself. This dependence is modeled by grouping initiators demanding similar alleviating systems (see Section 2 of the Plant Model Report), then defining the correct boundary conditions on each alleviating system to make their analysis specific to this initiator group (see the "boundary condition" tables in Section 4 of the Plant Model Report).

Initiating events that create environmental conditions in TMI-1 that might impact more than one event in a scenario were considered. If their likelihood and potential consequences were judged to be significant, they were modeled explicitly. Some of these events include steam line breaks and loss of reactor coolant system inventory events, as described in Section 2 of the Plant Model Report, and "external events" such as earthquakes, fires, floods, missiles, and high winds, as discussed in the Environmental and External Hazards Report.

- Top Events. Each event in each scenario is examined to specify its correct boundary conditions, given the previous events in the scenario. A branch may not appear in an event tree because the event whose failure would lead to it is not needed, is certain to be successful, cannot be successful, or is already failed because of events that have occurred previously in the scenario. Previous events may only change the availability of a subsequent alleviating system without eliminating the branch. Such a situation is indicated on the event tree and in the boundary condition table by a numerical specification, such as HPA-2 when HPA-2 refers to the second boundary condition for the high pressure injection system train A (see Plant Model Report, Section 4).

- Support Systems. Support systems that upon failure, impact frontline systems are modeled explicitly in the support system model, as described in Section 3 of the Plant Model Report. The assumed impact of support system failures on each event of a scenario is specified in the boundary conditions table for each event tree (see Sections 3 and 4 of the Plant Model Report).

- Human Actions. Human actions that might impact more than one event in a scenario are modeled explicitly as top events of the event trees. An example of this is Top Event TH, operator throttling HPI flow, which appears in many of the transient event trees. Human actions that impact only one system, but more than one component in that system (for instance test or maintenance errors), are modeled explicitly in the systems analysis (see the Systems Analysis Report).

Most cases of dependence identified during the course of the study were modeled explicitly. Allowance was made for real but undefinable dependencies by using "common cause" terms in the systems analyses. Furthermore, certain dependencies acknowledged by the nuclear industry and specifically considered in the TMI-1 plant design were judged to be insignificant contribuiors to risk and were therefore not explicitly modeled in the TMI-1 plant model. These include the effect of flooding resulting from high energy line breaks and the impact of seismic Class II components falling and striking seismic Class I components.

1.5.1.2 Commonly Used Terms

The following terms represent issues of concern with respect to the treatment of various types and aspects of dependence.

- Common Cause Failure. A term used to cover various types of dependent (usually failure) events that share a cause. Operating history data have shown that such joint mechanisms exist. Where they may be significant contributors to risk, they were modeled as dependent failures. In this study, the term "common cause failure" refers exclusively to cases of dependence that were left unmodeled either intentionally or unintentionally because their joint failure mechanisms were not well-enough understood.

- Common Mode Failure. A term often misunderstood used either synonymously with the term "dependent failure" or as representative of the subset of dependent failures of two pieces of equipment failing in the same way or failing because they are in the same "mode." This term is intentionally not used in this study.

- System Interactions. Typically, this term refers to adverse or unrecognized dependencies among events in a scenario. Used as an "NRC unresolved safety issue," this term refers to all such interactions regardless of their contribution to risk. System interactions are generally subdivided into "functional" and "spatial" dependencies. Both dependencies were modeled explicitly in the PRA: functional interactions, as described above, in the Systems Analysis and Plant Model Reports and spatial interactions in the Environmental and External Hazards Report.

- Environmental Effects. This term refers to dependence between events stemming from environmental conditions in the plant. For instance, the impact of the failure of the control building ventilation system that cools the electronic equipment and electric switchgear in various rooms is modeled explicitly in the support system model, as described in Sections 3 and 4 of the Plant Model Report.

1.5.2 SPECIAL INITITATING EVENTS

Numerous initiating events have received significant attention recently. All such events are treated explicitly and in the appropriate context in this report. Some scenarios that are sometimes incorrectly called initiating events, such as reactor coolant pump seal LOCA and failure to reclose a primary relief valve, are discussed in Section 1.5.3, Special Scenarios, since they are not initiating events but rather a result of another initiator and a subsequent failure(s).

Among the initiating events of special recent concern are:

- Steam Generator Tube Rupture. This event is complicated by the required operator actions. It is discussed in detail in Section 4.2.8 of the Plant Model Report where it is treated explicitly in its own event tree.

- Loss of River Water. This initiating event is analyzed explicitly in Section 4.2.19 of the PMR. It is of particular interest because it might lead to both reactor coolant pump seal leakage and high pressure injection pump failure.

- External Events. All external events (that is, events originating outside of plant systems that create adverse conditions in TMI-1 while perturbing the RCS) are treated explicitly. The external events treated explicitly in this study were all treated in the EEHR.

  - Earthquakes
  - Fires
  - Internal Floods
  - External Floods
  - Wind and Tornadoes
  - Aircraft Accidents
  - Turbine Missiles
  - Hazardous Chemicals

  Those judged to be significant to risk were analyzed in the same way as internal events both in the scenario definition and quantification process. Event trees were made for each important external event. These trees were treated in the same way as the internal event trees in the identification of dominant scenarios.

- Events Initiated from Other Than Full Power. In this study, as in most others performed to date, only events initiated from higher than approximately 15% reactor power were considered. At lower power levels, the feedwater will be controlled manually with the main feedwater system. All events considered in this study were initiated with the feedwater level control system in automatic and the turbine generator on line.

  It was assumed that at lower power levels the possible scenarios leading to core damage would be much less frequent than the comparable ones occurring from full power. There are several reasons for this assumption. One is that the plant spends only a small fraction of the calendar year at power levels in which the feedwater control is in manual. Second, events at these power levels are much more likely to be alleviated by operator response because the operator is manually controlling most plant functions. Most initiating events are not possible from other operating modes. For instance, loss of main feedwater or a reactor trip cannot happen in operating modes in which the reactor is already tripped and decay heat is being removed with the condensate booster pumps. Also, lower decay heat, stored energy levels, and fission product levels significantly reduce any consequences. In addition, everything will happen more slowly, making it more likely that the operator will successfully alleviate the consequences of the events.

  These positive factors are somewhat balanced by the fact that as the plant is cooled down the engineered safety features no longer needed are bypassed one by one as the pressure decreases. After being bypassed, they are nc longer available to automatically alleviate events but may be available for manual actuation. In addition, the technical specifications on safety equipment are different and are usually less demanding than they would be at full power. This means that a higher system unavailability is common during these periods. On balance, however, the TMI-1 PRA team considered that the impact of events from less than 15% power would be insignificant.

- Check Valve "V" Sequence or "V"-Sequence. This is an example of an initiating event that is usually called a scenario. This is because in some plants this initiating event can cause core damage without any other system failures. No alleviating systems can help if the break occurs outside the reactor building and the release therefore bypasses the containment altogether. In the TMI-1 PRA this initiator has been called by the name of the valves that in TMI-1 would have to open, inadvertently or due to a failure, to fail the lower pressure piping downstream of them to cause this initiating event. (See Inadvertent DHR Isolation Valve Opening, PMR Section 4.2.5.) Since the frequency (see Data Analysis Report, Section 3.5.2.6) of this event is very low it was assumed (as a modeling simplification) that it goes directly to core damage and therefore it is not treated explicitly in its own event tree.

- Loss of ICS/Instrumentation. Integrated control system failure caused specifically by loss of ICS power supply bus ATA was considered explicitly in this study. PMR Section 4.2.15 describes the loss of bus ATA power event tree. This initiating event results in main feedwater being ramped back to 50%, so that the RCS reacts to what appears to be a loss of feedwater. After the resulting reactor trip, the main feedwater stays at 50% (when less than 10% is needed) resulting in an excessive cooldown. At TMI-1, the failure modes of the power-operated relief valve, turbine bypass valves, and atmospheric dump valves minimize the effects of this event. It was also found that none of the other instrumentation or control equipment needed to alleviate this scenario was lost.

1.5.3 SPECIAL SCENARIOS

Certain scenarios are of special interest because they are NRC unresolved safety issues. In addition, some have been shown in other PRAs to be significant risk contributors.

- Station Blackout. This type of scenario can result from any of the initiating events defined in Section 2 of the PMR when power from the offsite grid (Top Event OP) and the diesel generators or onsite distribution system (Top Events GA and GB) fails completely. All such scenarios were considered explicitly in the evaluation of the event trees. Those initiated by the loss of offsite power are considered in the loss of offsite power event tree (see PMR Section 4.2.17), and those occurring from reactor trip and other initiators were treated in their own frontline, early response event trees (see PMR Section 4.2). The loss of onsite and offsite electric power is treated in the support system model described in Section 3 of the PMR.

- Anticipated Transients without Scram. The possibility of the reactor failing to trip on demand was considered for every initiating event described in PMR Section 2 in which the trip actuation setpoints were reached and reactor trip was required for reactivity control. The "without trip" scenarios are considered explicitly in each frontline event tree in the PMR except in the trees for "reactor trip" and for the large, medium, and small loss of RCS inventory initiating events.

- Reactor Coolant Pump Seal LOCAs. Scenarios that lead to reactor coolant pump seal degradation are possible in any event tree in this report except in those for the loss of coolant accidents. If both seal cooling and seal injection flow were lost, the seals were assumed to begin to degrade. Such scenarios were treated explicitly in all transient trees. The important station blackout scenarios in the loss of offsite power event tree were time limited by either the batteries running down, causing the auxiliary feedwater to stop leading to the emptying of the steam generator and boiling off the RCS inventory, or by the loss of RCS inventory due to the seal failure. In the case of the loss of river water initiating event, the time that it would take for the failed seals to cause the core to uncover should be adequate time to recover HPI flow to the RCS via recovery of river water. Such recovery was incorporated into the scenarios in the loss of river water event tree.

- Primary Relief Valves Open and Fail to Reclose. Most event trees in the PMR except those for the LOCAs ask whether the pilot-operated relief valves or primary safety valves, open and whether if opened, they reclose. This question is asked in two instances:

  1. If excessive cooldown takes place and the operator fails to throttle HPI flow prior to opening of the PORV.

  2. If there is a reactor trip failure.

  Such reclosure failure can lead to rapid loss of RCS inventory as would occur following a pipe break. It requires similar alleviation.

- Bleed and Feed Cooling (also known and referred to herein as "HPI Cooling". In the event trees, for all transients and for the very small loss of RCS inventory, the possibility of heat removal from the RCS using the RCS relief valves and high pressure injection flow is considered. In this study, this cooling mode is called "HPI cooling." HPI cooling was assumed to be successful if one out of the three primary relief valves opened and one HPI pump was started either manually or automatically. (Automatic start would occur only if the engineered safeguards actuation system was previously actuated for other reasons.) The viability of HPI cooling for removing decay heat has been confirmed by B&W transient analysis. HPI cooling was not considered as a viable method for cooling the RCS to decay heat removal system entry conditions; i.e., as a way of removing both decay heat and latent heat (the heat stored in the RCS) due to the considerable period of time required for cooldown. Of course, PSVs would not work for removing latent heat because they cannot be held open.

- Pressurized Thermal Shock. If scenarios lead to high RCS pressure and relatively low RCS temperatures, it is postulated that the possibility of crack propagation in the reactor vessel increases. This is because exposure of the reactor vessel to neutron flux raises the ductility transition temperature; i.e., the temperature at which carbon steel suffers a step increase in brittleness. This transition temperature has been well known for years. It has been the cause of automobile axle failures in Alaska and "liberty" ship hull failures at low temperatures. Usually, the transition temperature is outside the normal operating range of nuclear power plants. However, concerns with what the transition temperature might be after years of reactor operation has caused strict pressure-temperature limits to be established for operation of the reactor coolant system.

  Recent events have occurred at nuclear power plants that have violated these limits and, for highly irradiated pressure vessels, could have caused concern for reactor vessel integrity. These events have resulted from excessive cooldown of the RCS followed by repressurization via the high pressure injection system.

  The transient event trees used in this study include a number of cooldown scenarios. These scenarios result in excessive cooldowns (i.e., ones for which high pressure injection will be actuated) if the initiating event plus one of the following combinations of additional events occurs:

  - Failure of the main feedwater to ramp back.

  - Failure of the emergency feedwater control system to limit the feedwater delivered.

  - Failure of all secondary system steam relief valves--turbine bypass valves, atmospheric dump valves, or main steam safety valves--to reclose.

  Excessive main feedwater, steam line break, loss of bus ATA, and very small RCS pipe break initiating events would also cool down the RCS and actuate the high pressure injection.

  For all scenarios in which such excessive cooldown events occur, the high pressure injection system is assumed to operate. A question (top event) is then asked about whether or not the operator successfully throttles HPI flow prior to water being driven through the PORV. Driving water through a PORV makes it less likely that it will reclose. These scenarios were judged in this study to be more significant to risk because of their potential for leaving a primary relief valve open than because of the likelihood that the reactor vessel might fail.

  Top Event RV was included in all event trees where PTS might occur. This top event represented the conditional likelihood of reactor vessel failure, given that an excessive cooldown has occurred. GPUN has estimated (based on previous work by B&W) that the conditional failure frequency of the reactor vessel, given that an excessive cooldown scenario has occurred, is always less than 5×10^{-4}. This averages the frequency over the remaining plant lifetime, and takes credit for a reactor vessel flux reduction program. This range of values, when combined with the more frequent excessive cooldown scenarios (for instance, failure of MFW to ramp back and failure of the operator to throttle HPI flow), results in quite low scenario frequency. In addition, even if the reactor vessel did fail, it is most likely that it would fail as a leak at the core midplane. (This is the area of highest neutron fluence.) Failure of the reactor vessel at the midplane would not necessarily preclude injection flow to the core. It may be no worse than a large loss of RCS inventory event, which is already evaluated in the Plant Model Report. The TMI-1 PRA does not, however, take credit for mitigating a reactor vessel rupture.

- Cold Shutdown. Most events considered in this study were considered to have ended if 24 hours at operating temperature and pressure with the reactor tripped had elapsed. Reducing the RCS temperature and pressure to 275°F and 400 psi, respectively, and operating the decay heat removal system was considered to be necessary for steam generator tube rupture and for continued small RCS inventory loss events wherein it was necessary to cool the RCS in order to fix the problem.

  In the tube rupture case, recirculation via the containment sump is made impossible by the initiator, yet continued RCS inventory control is required. The alternatives to core uncovery are to replenish the borated water storage tank to provide for long term makeup or to get the RCS cooled to less than 212°F and arrest the inventory loss to the secondary system. The continued small RCS inventory loss events are treated in the reactor trip event tree for cases in which RCS leakage is within the capabilities of normal makeup; i.e., less than 150 gallons per minute, but more than technical specification allowable leakage.

1.5.4 HUMAN ERRORS

Human errors are dealt with on two levels in this study. If they affect more than one system or change the course of a scenario, they become event tree top events (see TH, failure to throttle HPI flow in the PMR). If such errors only impact one system, they are then included in the unavailability evaluation of that particular system. In either case, the evaluation of the likelihood of such events is discussed in the Systems Analysis Report. Human errors involved with testing or maintaining the system are also described in the Systems Analysis Report.

Four types of human errors are possible. Like other PRAs performed to date, this study addresses in detail only the first three of the following four types and provides some consideration of the fourth:

- Testing and maintenance or other technical specification-related errors wherein a component is left in a state from which it cannot perform its alleviating action. Such errors were considered for all systems; however, they did not prove to be important for all of them.

- Procedural errors wherein the operator fails to perform actions required by the emergency or operating procedures for a particular scenario. The failure of the previously mentioned TH top event (HPI throttling) is an example of a procedural error.

- Errors in selecting the correct procedure. In some cases, the identity of a specific scenario may be sufficently ambiguous that the operator could choose an incorrect emergency procedure to follow. In such a case, all the operator's subsequent actions may be inappropriate to the situation at hand. The only such error considered to be important in this study was ID (failure to identify correct procedure) in the steam generator tube rupture event tree (see PMR Section 4). Failure of Top Event ID means that the operator has mistaken the SGTR for a very small loss of RCS inventory event. Such errors will look, at first glance, like errors of commission.

- Other errors of commission in which, for instance, the operator steps in and turns off a pump without being misled by having picked the wrong emergency procedure. Such errors are extremely difficult to predict and have not been treated in detail in the TMI-1 PRA. One example of such an error, the inadvertent throttling of HPI flow, is considered in Top Event BW (split fractions BWE and BWF).

1.5.5 UNCERTAINTY

Consideration of uncertainty is a very fundamental aspect of this study. In fact, the study team considers uncertainty and risk to be inseparable. If there were no uncertainty about what the risk from operating TMI-1 was going to be, there would be no reason to do a risk assessment.

Uncertainty in every important input value is propagated through to the final plant damage state and core damage frequency curves, which are presented in "probability of frequency" format (see Section 5). These express the study team's state of knowledge about how well the team was able to calculate the frequency of all important scenarios.

A two-step process (see Section 4) was used to first find the important scenarios, and then to propagate the uncertainty from component distributions to risk curves for those scenarios that were important ("dominated risk"). How the important scenarios were picked is described in Section 6 of the PMR. How the uncertainties were propagated through these dominant scenarios is described in Section 4.4 of this report and in Section 6 of the PMR.

The first step was to allow a single characteristic of the distribution (usually the mean) to represent the top event likelihood of failure in the event trees. These means came from complete distributions that were the result of propagating component distributions through the systems analysis equations (see Systems Analysis Report). All scenarios in the event trees were evaluated with these means; then, only those scenarios necessary to represent a large fraction of the frequency of each type of event tree consequence (plant damage state) were kept. A logical, or Boolean, equation and its algebraic equivalent were written for each type of consequence category and then reduced. This allowed all dependent events to be treated properly. Next, the probability of frequency distributions for the top and initiating events that had been represented by their mean were used in logical expressions to derive a distribution for the frequency of each plant damage state and for core damage.

1.5.6 PROBABILITY AND FREQUENCY

Special language is used in this report to allow the study team to consistently describe its state of knowledge about each input or calculated value. The probability of frequency format was used.

Frequency was used to describe a "hard," measurable number, which can be thought of as the outcome of a thought experiment or an experiment to be done in the future. Probability, on the other hand, is a different notion, which is introduced because rarely in life is anything known with complete certainty. Probability is used as a way to communicate our state of confidence on any particular matter. It is a numerical scale introduced to quantify states of confidence or states of knowledge. To make this notion useful, we must clearly define the connection between the numerical scale and the state of confidence.

This can be done in several ways. The most direct, however, is to use frequency in the following way. Suppose a lottery basket contains coupons numbered from 1 to 1,000. Suppose the basket is thoroughly mixed and that a coupon is to be drawn blindfolded. Will the coupon be numbered 632 or less? With respect to this question, a certain state of confidence is experienced. Similarly, others experience a state of confidence with respect to this same question. This state of confidence is called, "probability 0.632," equal to the frequency of such draws in an infinitely repeated experiment. In the same way, the entire probability scale can be calibrated, from zero to one, using frequency as a standard of reference.

This method of definition shows the intimate connection between probability and frequency. This connection needs to be recognized always, but at the same time must not be allowed to obscure the fundamental difference. Frequency is used to calibrate the probability scale in a "bureau of standards" sense. Once the calibration is established, probability can be used to discuss a state of confidence in areas where one-time events are being addressed.

For each frequency used, a distribution of probability that the frequency has a particular value was established. This distribution plots a range of frequency against the likelihood that each frequency value is the correct one. All such values of probability that any particular frequency is the correct one represent a probability of frequency curve. Such curves are used wherever uncertainty is represented in this study. (See Section 4 for a description of how this is done.) The methods used in this report for propagating uncertainties did not require that the probability of frequency curves have any particular shape.

1.5.7 SUCCESS CRITERIA

Success criteria were established for the performance of each system in each top event in the event trees. These criteria specify to what degree each system must perform to accomplish its action. All such criteria are described in Section 4.1.4 of the PMR.

In general, the success criteria used in this study were kept as realistic as possible. Some exceptions may exist when realistic analyses for success criteria were unavailable, and could not be performed within the scope of the PRA. Realistic values were used for two reasons. First, to use "conservative" success criteria, e.g., the ones in the Final Safety Analysis Report, would usually produce excessively high estimates of the risk from operating TMI-1. Second, in some particular scenarios, combinations of conservative success criteria were found to not always result in conservative estimates of the scenario frequency and consequences. For both of these reasons, it would have been undesirable to use anything less than the most accurate possible success criteria.

1.5.8 QUALITY ASSURANCE OF THE TMI-1 PRA

1.5.8.1 General Quality Assurance Practices

The essential differences between a rigorous scientific study and a nonscientific, intuitive evaluation are the use of appropriate and consistent methods, careful documentation, and peer review. PRA is a highly scientific endeavor requiring the highest levels of technical competence and integrity.

As with any scientific endeavor, the quality of a PRA study hinges on the use and documentation of appropriate assumptions, methods, data, and analysis. The purpose of careful documentation is essentially twofold. One major purpose is to aid the analysts in maintaining control over the process; i.e., it builds a "blueprint" of the progress, which permits tracing logical progressions from initial assumption to final results. The second function of the documentation is to facilitate peer review. critiques, and reproducibility.

Given the requirements for a quality study, it is easy to see that the competence and integrity of the people involved are of paramount importance. For a PRA to be successful, the study team must be made up of at least the following:

- Experts in the analytical and probabilistic methods employed in the analysis.

- Engineers who have hands-on knowledge of the workings of the engineered systems being analyzed.

- Practitioners who can translate analytical methods and plant knowledge into meaningful models for quantifying risk.

- Engineers and scientists with concentrated knowledge of the behavior of systems under normal and abnormal conditions.

- Specialists in phenomena that are relevant to the study. Such phenomena might include earthquakes, fires, floods, and extreme winds.

- Authors who have special skills in communicating highly technical and scientific work.

The most important consideration for verifying the quality of a PRA is to perform the work correctly in the first place. Quality assurance is enhanced by segmenting the study into stages so that the analyst has checkpoints on his progress. Internal procedures require the analyst to present his work to his associates and defend the results. This technique is very effective in creating a sense of responsibility and professionalism. In addition, a different analyst checks the model and duplicates the key calculations. The work is subject to detailed review by senior members of the study team and by a technical review board. This review checks on the overall methods employed, makes spot checks of detailed models and calculations, questions all assumptions, carefully reviews all documentation, and identifies the weakest and strongest points in the analysis.

1.5.8.2 TMI-1 Specific Quality Assurance Procedures

The objective of the TMI-1 PRA quality assurance program developed by PLG was to ensure that the services provided were reliable, traceable, and in full compliance with all applicable Federal regulations and industry standards. For this project, additional emphasis was placed on technical review. A description of the technical review levels is provided in Table 1-2. A brief description of the quality assurance procedures follows:

- The document control system specified procedures for identifying and logging documents transmitted and received and for storing and retrieving project files.

- Corrective action procedures established requirements for controlling corrective actions for quality assurance program deficiencies discovered during technical analysis and reviews or quality assurance program audits. The procedures addressed the responsibility for detection and correction of the deficiency, the filing of Corrective Action Reports, and the tracking of report status.

- Quality assurance program audit procedures established guidelines for the frequency, scope, and documentation of internal audits and the responsibilities of the company officers and managers. The internal audits were made to ascertain that the specified quality assurance procedures were being followed and to uncover any deficiencies in the procedures.

- Independent technical review guidelines established the scope of the reviews and the responsibility of the project managers in these reviews.

- The computer code quality assurance program established the responsibilities of the project manager, computer coordinator, computer code author, and code verifier. The program also set guidelines to ensure that the codes performed as intended and were properly documented.

- The document change control defined procedures for processing and approving changes to project documents. Project documents included the project plan, quality assurance manual, and any other documents affecting control of the project.

- Subcontractor selection procedures set responsibilities and selection and documentation guidelines to ensure that subcontractors met the same technical and quality assurance standards set forth in the manual.

- Federal regulation compliance procedures set guidelines to ensure that the appropriate lawful actions would be taken should significant safety defects in the plant be revealed.

1.6 REFERENCE

1-1. American Nuclear Society and Institute of Electrical and Electronics Engineers, "PRA Procedures Guide; A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, NUREG/CR-2300, 1983.

TABLE 1-1. DISPOSITION OF ISSUES OF CURRENT CONCERN

Issue	Reference
• Common Cause Failure • Common Mode Failure • System Interactions • Environmental Effects	Section 1.5.1, Dependence
• Steam Generator Tube Rupture • Loss of River Water • "External Events" • Missiles • Tornados • Earthquakes • Events from Other than Full Power • Check Valve "V" Sequence • Loss of ICS/Instrumentation	Section 1.5.2, Special Initiating Events
• Anticipated Transient Without Scram • RCP Seal LOCA • PSVs/PORVs (Primary Valves) Fail to Reclose • Bleed and Feed Cooling • Pressurized Thermal Shock • Station Blackout • Cold Shutdown	Section 1.5.3, Special Scenarios
• Human Errors	Section 1.5.4, Human Errors
• Uncertainty	Section 1.5.5, Uncertainty
• Probability Versus Frequency	Section 1.5.6, Probability and Frequency
• Success Criteria	Section 1.5.7, Success Criteria

TABLE 1-2. REVIEW RESPONSIBILITIES

Stage	Review Objective	Person Responsible
1	Check all calculations, computer input and output; proofread documents prepared by publications department for technical accuracy.	Analyst/Author
2	Double-check all calculations; review documentation for technical accuracy; ensure consistency of documentation within technical area (e.g., systems); ensure that the right tools are used.	Task Leader
3	Review all deliverables; ensure project objectives are met; ensure consistency among technical areas and documentation; be responsible for resolution of all review comments and assignment of work needed to resolve review issues.	Project Manager
4	Assure that all parts of the project team perform their assigned responsibilities; review results and conclusions of key deliverables.	Project Director
5	Review all deliverables for correctness of interpretation of plant design and planned operation, documentation, safety analyses, and modeling of plant and site unique characteristics.	Client (GPUN)
6	Perform quality assurance audits; conduct quality assurance training; maintain quality assurance records.	PLG Quality Assurance Manager
7	Perform overall independent review of the report section deliverables in early draft form, particularly methods and results.	Technical Review Board

2. HISTORICAL PERSPECTIVE

Nuclear safety has been a visible and fundamental concern in the development and commercialization of nuclear power. From the beginning of the nuclear industry, safety design philosophy has centered around the "defense in-depth" characterized by the multiple fission product barrier concept supported by upper bound, deterministic calculations. This approach has served the cause of nuclear safety well. Carried to an extreme, however, it can lead to the wasteful use of resources and the unnecessary introduction of equipment complexity, which can actually reduce safety. With the growth of experience of operating nuclear power plants, the upper bound calculations have been supplemented with an analytical approach that assesses nuclear power plant safety more realistically by putting such upper bound results into context. PRA is the approach. PRA is both a systematic identification of the levels of damage that could result from nuclear plant operation and a rigorous assessment of the likelihood of such occurrences.

The upper bound deterministic approach for assessing nuclear power plant safety is specified in the Code of Federal Regulations. The Code requires the analysis of a fixed set of predefined accidents for the reactor plant. Originally, the most severe of these accidents, the maximum hypothetical accidents, were selected to establish required distance factors from the plant (Reference 2-1). The somewhat arbitrary nature of these distance factors began to stir interest. In the early 1960s, F. R. Farmer of the United Kingdom proposed a new approach to power plant safety based on the reliability of consequence limiting equipment (Reference 2-2). At the time, the United Kingdom, facing a need to bring nuclear power plants closer to large populations, began to abandon the somewhat arbitrary notions of plant safety and espoused a more realistic and quantitative definition of risk to public health. Meanwhile, in the United States, a series of studies sponsored by the U.S. Atomic Energy Commission was undertaken in the early and mid-1960s to probe the merits of using reliability techniques in the safety analysis of American nuclear power plants. These studies (References 2-1 and 2-2) identified the need for special data and analytical tools, such as fault tree analysis, to perform meaningful quantitative risk analysis.

Interest in probabilistic risk assessment continued to grow during the 1960s. Analysis techniques were borrowed from statisticians and reliability engineers (References 2-3 through 2-5) and were developed into tools suitable for predicting failure frequencies for large, complex nuclear power plant systems. The benefits in terms of safety control and understanding were documented in Reference 2-3. (This reference developed a methodology for attacking the problem of probabilistic risk assessment of complex plants.) With the evolution of reliability techniques, people began to believe that it was possible to estimate the likelihood of low frequency, high consequence accidents at nuclear plants. In 1972, the U.S. Atomic Energy Commission undertook the Reactor Safety Study under the direction of Professor N. C. Rasmussen of the Massachusetts Institute of Technology (Reference 2-6). This project took 3 years to complete and marked a turning point in attitudes toward measuring nuclear safety. It was the most thorough investigation of reactor safety of its time and, as such, it set the stage for the understanding of safety for years to come. It calculated the risk from the operation of 100 U.S. light water reactors of then current design operating at base power. The report showed the way to derive and present risk results meaningfully to technical specialists and policy makers alike. The finished document formed a basis for thorough discussion of risk methodology, thereby focusing criticism, review, and improvement. Three important findings of the study were that: (1) the risk associated with the operation of selected nuclear power plants was indeed small, (2) the dominant contributor to risk was not the large loss of coolant accident, as previously emphasized in the Code of Federal Regulations, but (3) it was the transients and the small LOCAs that often make up most of the contribution to risk.

Although seminal in nature, the Reactor Safety Study was criticized extensively. Between release of the draft report in August 1974 and the final version in October 1975, comments were received from 87 organizations and individuals representing government, industry, environmental groups, and universities. Many of these comments had a significant impact on the final report. For example, the American Physical Society Study Group on Reactor Safety pointed out serious omissions in the consequence calculations. The Union of Concerned Scientists, released its review of the study in 1977 (Reference 2-7). It criticized all aspects of the report--its objectivity, the accident analysis, and the consequence analysis.

The most complete and even-handed review of the WASH-1400 report was conducted by the Risk Assessment Review Group chaired by Professor H. W. Lewis of the University of California, Santa Barbara (Reference 2-8). The group was organized by the U.S. Nuclear Regulatory Commission on July 1, 1977, at the request of Congressman Morris K. Udall, Chairman of the Committee on Interior and Insular Affairs, who had held hearings on the Reactor Safety Study.

Following the release of the Lewis Report, the NRC issued a press release (Reference 2-9) withdrawing its endorsement of the WASH-1400. This announcement has since caused great misunderstanding of the criticism offered by Lewis, et al., and of the validity of WASH-1400 itself. It is important to note, however, that neither the Lewis Report nor the NRC press release disavowed the fault tree/event tree methodology.

The most astounding statement by the NRC was that "the Commission does not regard as reliable the Reactor Safety Study's numerical estimate of the overall risk of reactor accidents." This action was based upon the Lewis Report conclusion that "absolute values of the risks presented by WASH-1400 should not be used uncritically." The leap from this cautious caveat to rejection was a large one indeed. The Lewis Report found that the RSS error bands were understated, thus misrepresenting the uncertainties associated with a potentially inadequate data base with the occasional use of weak statistical methods and with some calculational inconsistencies. In particular, the Lewis Report urged caution in the use of the numbers, but did not reject them completely. In summary, the general methodology was strongly supported and recommended for future use. Care in stating the bounds of knowledge, however, is necessary.

The accident that occurred at the Three Mile Island Nuclear Generating Station, Unit 2 in March 1979 (Reference 2-10) had a profound impact on the nuclear industry and on the concept of risk assessment. Portions of the TMI-2 sequence of events were not included in detail in the RSS analysis, causing many to question the validity of the analyses.

In truth, the transient at TMI did fit the RSS sequences, albeit not exactly. The transient fit in the sense that a small LOCA with failure of high pressure injection was included as one of the RSS sequences. However, it did not fit exactly because the numerical probabilities that the RSS placed on this scenario represented an accident progression going all the way to core melt. What the RSS did not estimate was the likelihood that an operator would interrupt the core damage.

The initial reaction to the TMI accident was negative with respect to the value and role of probabilistic risk assessment; on reflection, the attitude soon changed. Two important post-TMI independent studies recommended greater use of probabilistic analysis techniques in assessing nuclear plant risks and in making decisions about nuclear safety. They were the report of the President's Commission on the Three Mile Island accident (Reference 2-11) and the so-called Rogovin Report (Reference 2-12). Following the lead of the reports of these commissions, several post-TMI NRC reports also noted the value of quantitative risk analysis (References 2-13 through 2-16).

Evidently, the use of probabilistic methods in nuclear safety analysis received a singular boost from the RSS. However, as a result of the many controversies surrounding the RSS and the TMI-2 accident, it became obvious that certain areas of the methodology used in the RSS would have to be enhanced for probabilistic risk assessment to be better understood; i.e., to be more scrutable. In particular, it would be necessary to provide:

- A better executive summary.

- A quantitative expression of the uncertainty in the risk results and in all the input variables, data, etc., that are used.

- A full display of the events and hardware contributing to risk in such a way that the impact on risk of changes in design and operations could be easily seen.

- Documentation that allows all models, boundary conditions, accident scenarios, and supporting data to be easily traced.

- A full treatment of all accident initiators, including those due to earthquakes, fires, floods, and winds.

- Detailed analysis of accident phenomena, including in-vessel and ex-vessel degraded core behavior, transient analysis, containment response, and source term definition.

- Consequence analysis based on plant-specific/site-specific weather and evacuation models.

The accident that occurred at the Three Mile Island Nuclear Generating Station, Unit 2 in March 1979 (Reference 2-10) had a profound impact on the nuclear industry and on the concept of risk assessment. Portions of the TMI-2 sequence of events were not included in detail in the RSS analysis, causing many to question the validity of the analyses.

In truth, the transient at TMI did fit the RSS sequences, albeit not exactly. The transient fit in the sense that a small LOCA with failure of high pressure injection was included as one of the RSS sequences. However, it did not fit exactly because the numerical probabilities that the RSS placed on this scenario represented an accident progression going all the way to core melt. What the RSS did not estimate was the likelihood that an operator would interrupt the core damage.

The initial reaction to the TMI accident was negative with respect to the value and role of probabilistic risk assessment; on reflection, the attitude soon changed. Two important post-TMI independent studies recommended greater use of probabilistic analysis techniques in assessing nuclear plant risks and in making decisions about nuclear safety. They were the report of the President's Commission on the Three Mile Island accident (Reference 2-11) and the so-called Rogovin Report (Reference 2-12). Following the lead of the reports of these commissions, several post-TMI NRC reports also noted the value of quantitative risk analysis (References 2-13 through 2-16).

Evidently, the use of probabilistic methods in nuclear safety analysis received a singular boost from the RSS. However, as a result of the many controversies surrounding the RSS and the TMI-2 accident, it became obvious that certain areas of the methodology used in the RSS would have to be enhanced for probabilistic risk assessment to be better understood; i.e., to be more scrutable. In particular, it would be necessary to provide:

- A better executive summary.
- A quantitative expression of the uncertainty in the risk results and in all the input variables, data, etc., that are used.
- A full display of the events and hardware contributing to risk in such a way that the impact on risk of changes in design and operations could be easily seen.
- Documentation that allows all models, boundary conditions, accident scenarios, and supporting data to be easily traced.
- A full treatment of all accident initiators, including those due to earthquakes, fires, floods, and winds.
- Detailed analysis of accident phenomena, including in-vessel and ex-vessel degraded core behavior, transient analysis, containment response, and source term definition.
- Consequence analysis based on plant-specific/site-specific weather and evacuation models.

The first study to be completed after the RSS to include many of these new features was the "OPSA, Oyster Creek Probabilistic Safety Analysis," a draft report which was completed in 1979 (Reference 2-17). The Zion (Reference 2-18) and Indian Point PRAs (Reference 2-19) and others performed by PLG for various utilities built on the Oyster Creek PRA methods and added important improvements, including: expanded common cause failure analysis, uncertainty quantification methods, methods for assembling and dissecting the results, analysis of dependent failures and human interactions, containment and core response analysis, modeling of external events (earthquakes, fires, floods, etc.) and incorporation of the site-specific topography, emergency preparedness plans, and changing weather patterns in the consequence model. In this report, a PRA incorporating all these features is termed a "full-scope PRA." One impact of the above advances has been a m re accurate specification of the contributors to risk. The methodology now allows us to identify the contributors to risk and to observe in increasing detail what is driving the risk level. This is vital for making decisions on design modifications, procedural options, or any other risk management action on the part of the utility. Knowledge of the risk and its structure enables effective risk management.

In addition to the advances made by these recent PRAs, a very significant sign of the developing maturity of risk assessment was the publication of a PRA Procedures Guide (Reference 2-20). Developed by experienced practitioners in private industry and in national laboratories, this guide defines what is meant by a PRA and describes some of the alternative methods available for performing each of its aspects.

Another impact of these advances has been to enhance the usefulness of PRA in risk management and in the regulatory process. The latter includes conformance with regulatory safety goals (Reference 2-21), post-TMI-2 accident licensing requirements (Reference 2-22), environmental impact reports, and emergency preparedness plans (Reference 2-23).

All of these impacts are precisely what is intended to be achieved by the TMI-1 PRA. The risk profiles from other PRAs cannot be used for the TMI-1 Station. Recent experience indicates that risk profiles are even more plant specific than was realized following the early PRAs. A striking example is the difference in risk levels and dominant contributors between the Indian Point Units 2 and 3, which are similar units located on the same site (Reference 2-24).

In conclusion, it is becoming clear that the ultimate reason for doing a risk assessment is that there is an underlying decision (or many decisions) to be made. The risk assessment provides vital input to the decision-making process formalized by decision analysis. In this section, we give a brief review of the well-known decision theory diagram (Figure 2-1) and therefore, of the context for using risk assessment.

At the left in this diagram, the point of decision is represented with various items of information as input. On the basis of this information, we need to choose between options A, B, ... N.

If we knew for certain what would be the outcome of each option, the decision, of course, would be easy. What makes the situation interesting is uncertainty. The uncertainty is represented in the diagram by showing a set of possible outcomes (e.g., A_1, A_2...) for each option. The best we can do, standing at the decision point, is to look ahead and assign a probability to each of the possible outcomes, assuming we choose the corresponding option. These probability values represent our state of knowledge at the point of decision, based upon all the information available there.

Associated with each outcome is a set of "impacts," which we regard as listed in a linear array called the impact "vector" to denote the fact that, in general, there are many different impacts or categories of impact associated with a given outcome.

Next, we must feed into the decision process the notion of "preference"; that is, we must say which sets of impacts we prefer to which others and by how much. Analytically, this is done by establishing a "utility" function which makes each impact vector into a single scalar, an ordinary number that expresses our preference value for that set of impacts. This being done, we may now calculate the "expected utility" associated with each option as the sum, over the possible outcomes of that option, of the product of the probability of that outcome multiplied by its utility.

According to this model of the decision process, then, the optimum decision is that option having the largest expected utility. This is the fundamental model of a decision situation. It is necessary to remark that in order for the model to represent a real-life decision situation, it must include all the options present in that situation, including, for example, the option of not deciding--which is itself a decision, although rarely the optimum one. Similarly, it should include the option of delaying the decision while we gather further information. Both of these options have probabilities, outcomes, impacts, and utilities like any other option and should be included explicity in the decision diagram.

Figure 2-2 gives an alternate formulation of the decision diagram that is better suited to our needs here. For this purpose, we define impacts so that there are only three components in our impact vectors, namely, "cost," c, "benefit," b, and "damage," x. We consider, moreover, the simplest case in which our uncertainties about the magnitude of cost, benefit, and damage are independent of each other. We may then draw the decision diagram in the form of Figure 2-2.

In this figure, we allow C_A, the cost of option A, to stand for the entire probability density function (pdf) $P_A(c)$; similarly, we allow B_A, the benefit of A, to stand for the pdf $P_A(b)$. In the case of damage (in keeping with current convention), we show the probability curve drawn in complementary cumulative form, and we denote this curve by $R_A(x)$, the risk of A.

We now think of the triplet $<C_A, B_A, R_A>$ as characterizing option A. Similarly, $<C_N, B_N, R_N>$ characterizes N, etc. The utility function now becomes a mapping from such triplets to scalars.

Thus,

$$U_A = U\ (<C_A,\ B_A,\ R_A>)\ \cdots\ U_N = U\ (<C_N,\ B_N,\ R_N>)$$

where the scalar U_A now expresses our degree of preference for the triplet $<C_A, B_A, R_A>$, etc. The optimum decision is then that option having the largest ut·lity value.

The purpose of risk analysis, as shown in Figure 2-2, is to provide the curve R_A. For a valid decision analysis, similar curves, R_B, ... R_N, should be calculated for each option. Only the risk assessment is addressed in this report.

A PRA can put a decision into perspective about whether to modify a plant or its procedures for operation and maintenance by comparison with other sources of risk and with various proposed safety goals or acceptable risk criteria. After the final results have been assembled, the methodology permits a clear examination of risk contributors from several different perspectives. The structure of the risk model allows us to determine risk contributors in successive levels of detail. With this detail, we are in a position to identify options that can be most effective in reducing risk. Thus, quantified risk before and after any proposed change allows us to define the effectiveness of the change.

Risk reduction may result from changes in specific plant components, personnel training, procedures, safeguards, containment, or emergency plans. The plant and site-specific risk model developed in this project is designed to accommodate this level of decision analysis.

In constructing a plant-specific risk model for TMI-1, the risk assessment team has taken advantage of lessons learned from previous PRAs (Reference 2-24). Some highlights of these lessons are:

- Important scenarios, such as those that occurred at the Salem plant (automatic scram failure), can be identified and their likelihood anticipated in advance of their occurrences. This tends to validate the whole idea of deriving risk estimates from risk models.

- Nuclear plants are much more able to cope with a damaged core or even a core meltdown than had been generally perceived in the past. As a result, the likelihood of the owner/operator experiencing a loss associated with damage to the plant is much greater than the likelihood of experiencing damage to public health and property.

- Contributors to risk vary, depending on the type of consequence considered. Hence, a risk management strategy that focuses on core melt frequency is not likely to result in the same set of actions as a strategy that focuses on the risk of early fatalities or one that focuses on the risk of latent fatalities.

- Core melt progression studies done in support of PRAs have moved a long way toward dispelling certain perceptions regarding the "China Syndrome" scenario. The evidence is very strong that containment basemat melt-through is not an inevitable consequence of a core meltdown accident. Studies that have been made relative to liquid pathways for radioactive material have indicated little or no consequence with respect to health and safety even when basemat melt-through is postulated to occur.

- Full scope PRAs have indicated the importance of including the analysis of such external events as earthquakes, fires, flood, and high intensity winds. In a number of cases, the external events have been shown to be the major contributors to risk.

- The emphasis in new plants on independence and separation of safety system equipment trains has not necessarily reduced risk. While such designs reduce the risk contributions from such rare events as pipe ruptures, large fires, and extensive flooding, they make it more difficult to protect the plant against frequently occurring failures. That is, the absence of crossties between systems denies access, for example, to alternate supplies of cooling water. Because of their higher frequency, such events as normal challenges to these systems often turn out to be more important contributors to risk than the less frequent energetic events.

REFERENCES

2-1. DiNunno, J., F. Anderson, R. Baker, and R. Waterfield, "Calculation of Distance Factors for Power and Test Reactor Sites," TID-14844, March 1962.

2-2. Farmer, F. R., "The Growth of Reactor Safety Criteria in the United Kingdom," Anglo-Spanish Nuclear Power Symposium, Madrid, November 1964.

2-3. Garrick, B. J., and W. C. Gekler, "Reliability Analysis of Nuclear Power Plant Protective Systems," HN-190, U.S. Atomic Energy Commission, May 1967.

2-4. Garrick, B. J., "Principles of Unified Systems Safety Analysis," Nuclear Engineering and Design, Vol. 13, No. 2, 1970, pp. 245-321.

2-5. Locke, J. H., et al., "Canvey: An Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock Area," U.K. Health and Safety Executive, May 1978.

2-6. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

2-7. Union of Concerned Scientists, "The Risks of Nuclear Power Reactors: A Review of the NRC Reactor Safety Study," WASH-1400 (NUREG-75/014), August 1977.

2-8. Lewis, H. W., et al., "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission," NUREG/CR-0400, September 1978.

2-9. "Nuclear Regulatory Commission Issues Policy Statement on Reactor Safety Study and Review by Lewis Panel," NRC Press Release, No. 79-19, January 19, 1979.

2-10. Electric Power Research Institute, "Analysis of Three Mile Island--Unit 2 Accident," Nuclear Safety Analysis Center, NSAC-1, July 1979.

2-11. "The President's Commission on the Three Mile Island Accident: The Need for Change - The Legacy of TMI," October 1979.

2-12. Rogovin, M., and G. T. Frampton, "Three Mile Island, A Report to the Commissioners and to the Public," Government Printing Office, January 1980.

2-13. U.S. Nuclear Regulatory Commission, "TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations," NUREG-0578, July 1979.

2-14. U.S. Nuclear Regulatory Commission, "TMI-2 Lessons Learned Task Force Final Report," NUREG-0585, October 1979.

2-15. U.S. Nuclear Regulatory Commission, "Action Plans for Implementing Recommendations of the President's Commission and Other Studies of TMI-2 Accident," Draft Report, NUREG-0660, December 1979.

2-16. U.S. Nuclear Regulatory Commission, "Review of NRC Regulatory Processes and Functions," NUREG-0642, January 1980.

2-17. Garrick, B. J., et al., "OPSA, Oyster Creek Probabilistic Safety Analysis," draft, prepared for Jersey Central Power and Light Company, PLG-0100, August 1979.

2-18. Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study," prepared for Commonwealth Edison Company, September 1981.

2-19. Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Indian Point Probabilistic Safety Study," prepared for Consolidated Edison Company of New York, Inc., and the Power Authority of the State of New York, March 1982.

2-20. American Nuclear Society and Institute of Electrical and Electronics Engineers, "PRA Procedures Guide; A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, NUREG/CR-2300, 1983.

2-21. U.S. Nuclear Regulatory Commission, "Safety Goals for Nuclear Power Plants," NUREG-0880, May 1982.

2-22. U.S. Nuclear Regulatory Commission, "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License," NUREG-0718, March 1981.

2-23. U.S. Nuclear Regulatory Commission, "Criteria for Preparation and Evaluation and Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," NUREG-0654, Revision 1, November 1980.

2-24. Garrick, B. J., "Lessons Learned from First Generation Nuclear Plant Probabilistic Risk Assessments," Workshop on Low-Probability/High-Consequence Risk Analysis, Arlington, Virginia, June 15-17, 1982.

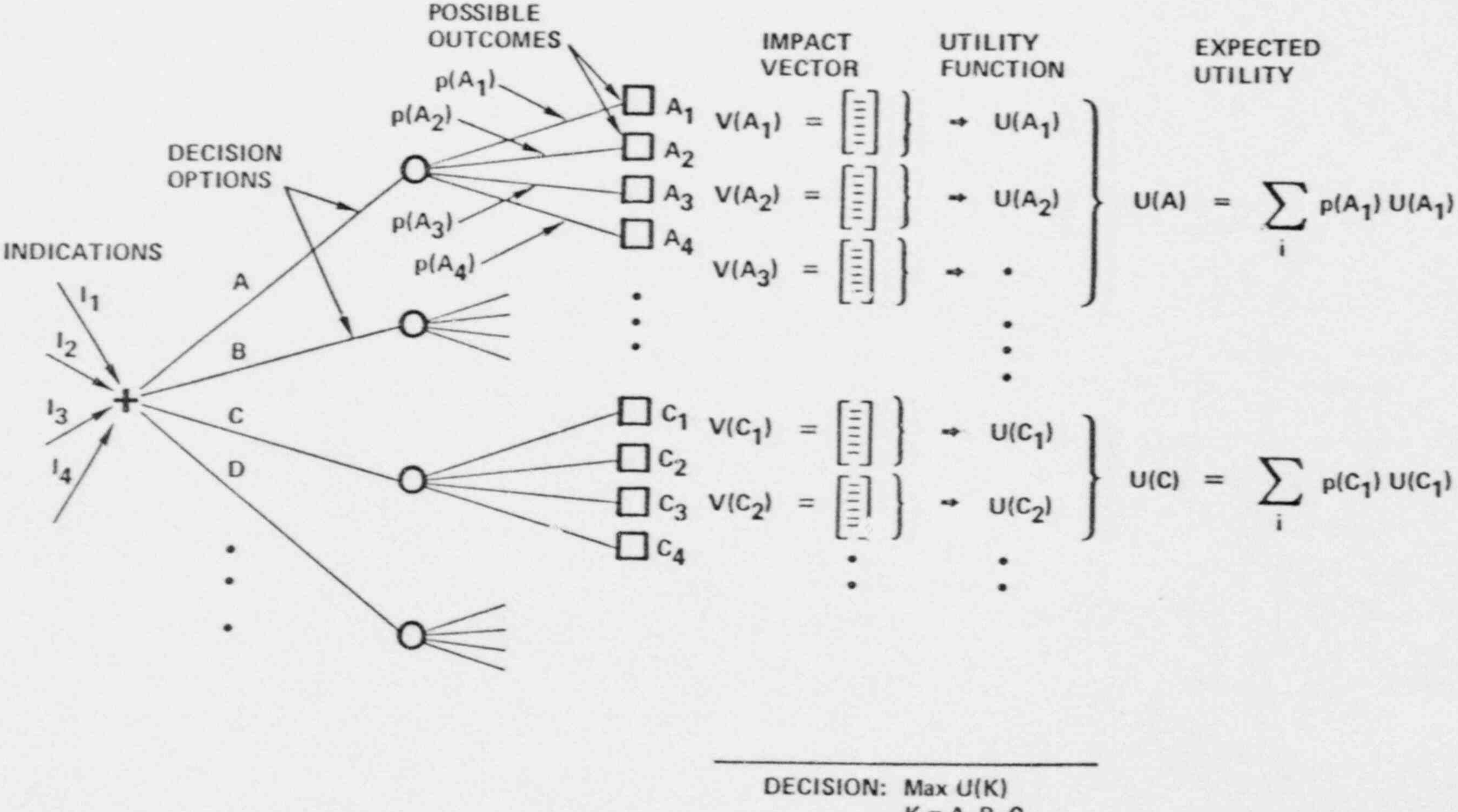


FIGURE 2-1. THE ANATOMY OF A DECISION

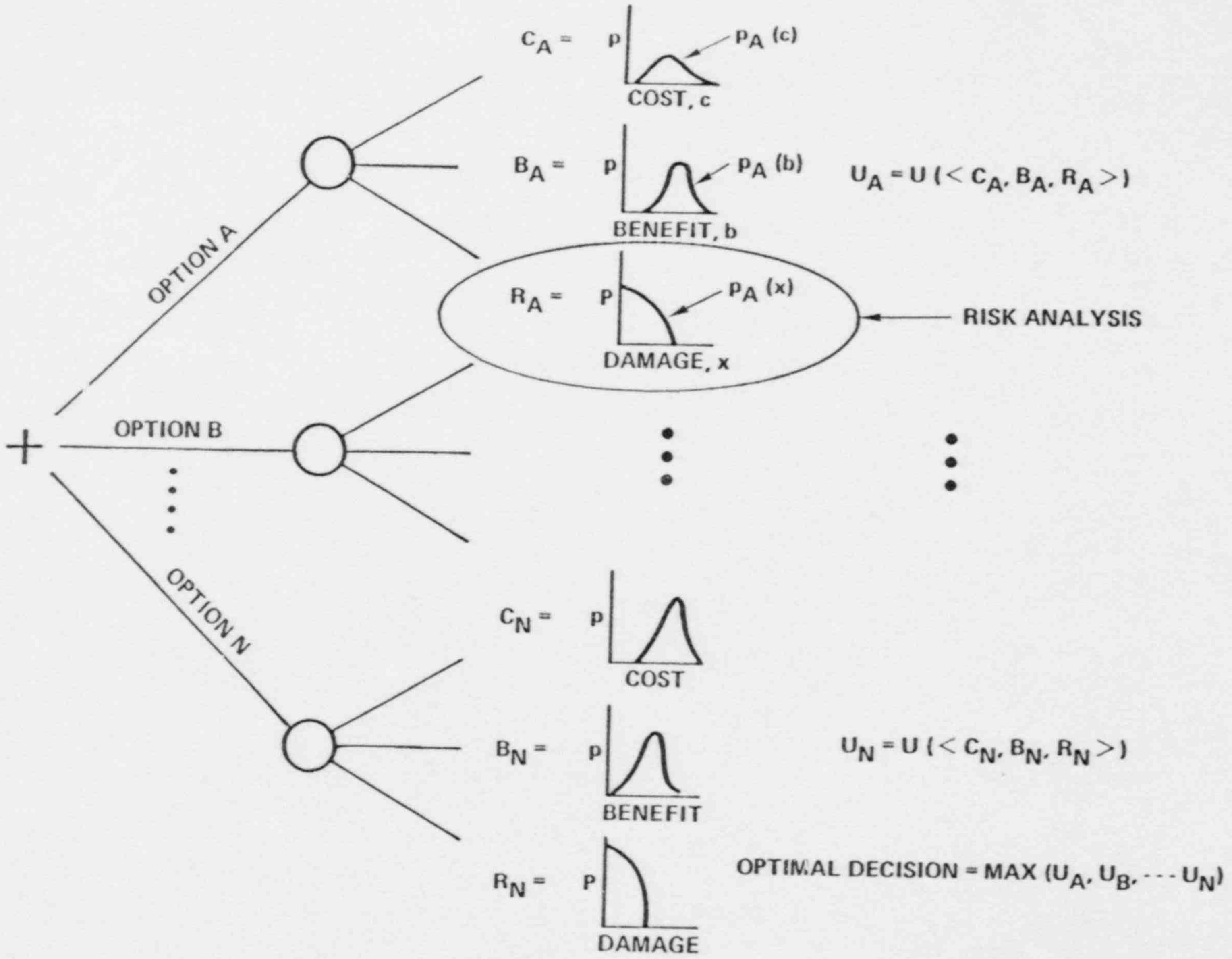


FIGURE 2-2. ALTERNATE FORMULATION OF THE DECISION MODEL

3. PLANT PERSPECTIVE

This section describes the TMI-1 plant, its safety functions, and the relationship of the PRA model to the plant, as built.

3.1 DESCRIPTION OF PLANT AND SITE

The Three Mile Island Nuclear Station Unit 1 is located on Three Mile Island in the Susquehanna River, Londonderry Township, Dauphin County, about 10 miles south of Harrisburg, Pennsylvania. TMI-1 is rated at 871 MWe (gross), and is licensed for a core power of 2,535 MWt. It went into commercial operation in September 1974.

The TMI-1 NSSS was supplied by Babcock & Wilcox Company, and the turbine generator was supplied by General Electric. Gilbert Associates, Inc., was the architect-engineer.

TMI-1 is owned jointly by Jersey Central Power and Light Company, 25%; Metropolitan Edison Company, 50%; and Pennsylvania Electric Company, 25%; all owners are operating companies of the General Public Utilities Corporation. It is operated by GPU Nuclear, also a GPU subsidiary.

Three Mile Island is located approximately 2-1/2 miles south of Middletown, Pennsylvania, at longitude 76°F 43'-30" west and at latitude 40°F 8' north. It is one of the largest of a group of several islands in the Susquehanna River and is situated about 900 feet from the east bank. It is elongated parallel to the flow of the river, with its longer axis oriented approximately due north and south. The island is about 11,000 feet in length and 1,700 feet in width. This unit is located in the northern one-third of the island.

The exclusion area includes portions of Three Mile Island, the river surface around it, and a portion of Metropolitan Edison Company-owned Shelley Island. Metropolitan Edison Company directly owns the site and all but a small portion on the southern end of Shelley Island. The remainder of Three Mile Island is held by a wholly owned subsidiary of Metropolitan Edison Company.

The following sections contain a brief description of the reactor, the reactor coolant system, and the reactor building. All the individual systems analyzed in the PRA are described in Appendix A.

3.1.1 REACTOR AND REACTOR COOLANT SYSTEM

The TMI-1 reactor is licensed for operation at 2,535 MWt. (All ratings in this description are used for reference only, and may not be exact or up-to-date.) The core contains 177 fuel assemblies arranged in a square lattice approximating the shape of a cylinder with an equivalent diameter of 128.9 inches and an active fuel length of 142.25 inches.

Each fuel assembly contains 208 fuel rods, 16 control rod guide tubes, and 1 central instrumentation tube arranged in a 15' x 15' array.

Power control is achieved with 61 control rod assemblies, 8 axial power shaping rod assemblies, and soluble poison. Each assembly consists of 16 rods held by a spider and coupled to a sealed roller nut and leadscrew-type control rod drive. On a scram, the 61 control rod assemblies drop into the core by gravity when current is removed from the drives.

The reactor coolant system consists of the reactor vessel, pressurizer, four reactor coolant pumps and two once-through steam generators. The reactor coolant system removes the heat generated in the reactor and delivers it to the steam generators. The pressurizer provides an overpressure to ensure a subcooled condition in the reactor coolant system, a surge tank for volumetric changes, and pressure control flexibility for all combinations of reactor operations.

The system is arranged in two heat transport loops, as shown in Figure 3-1. Each loop has one steam generator and two reactor coolant pumps. The reactor coolant is transported through piping connecting the reactor vessel to the steam generators and flows downward through the steam generator tubes, transferring heat to the steam and water on the shell side of the steam generator. In each loop, the coolant is returned to the reactor vessel through two lines each containing a coolant pump.

The reactor vessel is carbon steel with stainless clad, 40 feet 8-3/4 inches high overall and 171 inches in diameter. All major penetrations are located above the level of the top of the core.

The four reactor coolant pumps are vertical single stage centrifugal-type pumps with controlled leakage seal assemblies. Seal water is provided by high pressure water from the makeup pumps. Intermediate closed cooling water is supplied to the thermal barrier cooling coils. Each reactor coolant pump is rated at 88,000 gpm.

The two steam generators are vertical, straight-tube, once-through shell and tube type, which produce superheated steam at constant pressure throughout the power range. At full load, each generator produces 5.6×10^6 pounds of steam per hour at 910 psig and 570°F. Emergency feedwater is provided to the generators through dedicated auxiliary feedwater rings at the top of the generators.

The pressurizer is connected to the reactor coolant piping by a surge line and a spray line. Two code safety valves and one pilot-operated relief valve connected to the pressurizer protect all reactor coolant system components from exceeding the design pressure.

The reactor coolant system pressure is maintained by a pressure control system that energizes the pressurizer heater banks in sequence as pressure decreases below normal and opens the spray valve and pilot actuated relief valve when the pressure increases above normal.

All the plant systems analyzed in detail for the PRA are described in Appendix A. These are: electric power (Section A.1), engineered safeguards actuation (Section A.2), nuclear services river and closed cooling water systems (Section A.3), decay heat river and closed cooling water systems (Section A.4), control building ventilation system (Section A.5), reactor protection system (Section A.6), turbine trip (Section A.7), main steam system (Section A.8), main feedwater and ICS (Section A.9), emergency feedwater (Section A.10), pressure control (Section A.11), high pressure injection and makeup and purification (Section A.12), and low pressure injection and decay heat removal (Section A.13).

3.1.2 REACTOR BUILDING SYSTEM

The reactor building is a reinforced concrete cylinder with a flat foundation and a shallow dome roof. The inside diameter is 130 feet and the cylinder height is 157 feet. The wall is prestressed with a post-tensioning system in two directions, while the roof is prestressed in three directions. There is a 3/8-inch carbon steel liner on the wall and dome, and a 1/4-inch liner in the base. The safety features systems designed to protect containment integrity and reduce the amount of radioactivity lost from the reactor building in case of the loss of its integrity are described in Appendix A, Section A.14 (Reactor Building Isolation), Section A.15 (Reactor Building Emergency Cooling System), and Section A.16 (Reactor Building Spray System).

3.2 SAFETY FUNCTIONS AND HAZARDS FOR THE TMI UNIT 1 PLANT

Webster's dictionary defines risk as "the chance of injury, damage or loss." It defines hazard as "peril; danger." Hazard, therefore, can be thought of as a source. Risk is the likelihood that this source, or hazard, produces an injury or damage. This is the sense in which these words are used in this study. This idea can be expressed in the form of a symbolic equation

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}}$$

This equation also incorporates the idea that risk can never be zero as long as a hazard is present, but it can be very small. The radioactive material produced at TMI-1 is the hazard; the likelihood of spreading this radioactivity through the surrounding population is the risk.

Most of the radioactivity produced in the plant remains at its source, namely, the fuel pellets. The largest quantity of radioactivity is located at the reactor core and the spent fuel storage pool. Smaller sources of radioactivity are normally present at the plant in the waste gas and liquid waste streams.

The reactor core, although a hazard, need not be a significant risk if the probability of a release of radioactivity into the environment is sufficiently small. The potential for releases varies, depending on the degree of disturbance to the core and the subsequent operation of the systems that are designed to return the plant to a safe condition. The largest risk presented by the TMI Unit 1 plant is from the release of large fractions of the radioactive material in the core. Large fractions of the radioactive material in the reactor core can only be released as a result of extensive core damage. In the absence of extensive core damage, the fission product release that takes place is associated with initial cladding rupture. This release consists mostly of radioactivity that escaped from the fuel pellets to void spaces within the fuel rods during normal reactor operation. During the rapid depressurization of the contained gases in the void spaces following cladding rupture, additional radioactive fission products are driven from the fuel pellets to the void spaces. The fraction of the core that is released in this manner is several orders of magnitude lower than that associated with extensive core damage. Thus, extensive core damage is the central undesired event for this risk assessment.

For extensive core damage to occur, it is necessary to create a severe imbalance between the amount of energy generated by the fission process (or by residual heat from fission products) and the capacity of the plant to remove heat. Explosions and other exothermic chemical reactions between the cladding and the steam may create sufficient energy to damage the cladding and release radioactivity. The functions that must be performed in order to control the sources of energy in the nuclear power plant and the hazard embodied in the radioactive material in the core are called safety functions.

The concept of safety functions forms the basis for choosing scenario initiators and for delineating the actions either required or possible to alleviate the consequence of each initiator; i.e., for initial structuring of a list of core damage scenarios (see Sections 4.1 and 4.2 for more about structuring this list). Safety functions are defined as groups of actions that prevent extensive core damage, prevent reactor building failure, or minimize direct radioactivity releases. Actions may result from the automatic or manual actuation of a system, from passive system performance, or from natural feedback inherent in the plant design.

There are 10 safety functions that must be maintained at all times to alleviate initiating events and thereby contain stored radioactivity. These safety functions are listed with their purposes in Table 3-1. These safety functions may be divided into three classes:

1. Core protection safety functions.
2. Containment integrity safety functions.
3. Direct radioactive material release safety functions.

The relationship between these classes is shown on Figure 3-2. The plus signs indicate that it is necessary to protect the core, maintain containment integrity, and control direct radioactivity releases in order to limit the release of radioactivity to the general public. In all safety functions, the word control means accomplishment of the safety function so that extensive core damage is prevented or radioactive releases are kept within acceptable limits.

3.3 RELATIONSHIP OF THE PRA MODEL TO THE TMI-1 AS-BUILT PLANT

During the course of the development of the TMI-1 PRA, the plant was been modified to comply with regulatory requirements and to increase the availability/maintainability of the unit. Some of the modifications have been followed closely by the PRA team and incorporated into the plant model even before they have been installed. For example, the PRA includes the emergency feedwater and heat sink protection systems modifications made during the 1986-1987 refueling outage.

In the early stages of the PRA, the instrument air dryer transfer valve was identified as a major contributor to the loss of instrument air. The complete air dryer assembly has since been replaced and includes a new type of transfer mechanism. This new mechanism has been included in the air system model but still remains as a single failure point for the instrument air system.

As described in Section 5.2.3. of this summary, the loss of the control building ventilation system is the sequence that dominates the total frequency of core damage. During the first phase of this PRA, a loss of control building ventilation was seen as a major contributor to core damage, and, as a result, a study was undertaken to better understand the time available to the operators if the loss occurred. It was determined that a system of portable ventilation fans and ducts could be used if the normal system failed. This system of portable fans and a procedure for installing the fans is included in the PRA even though the system is not yet fully operational.

During the 1986-1987 refueling outage, major modifications occurred to upgrade the routing and protection of cables to comply with the requirements of 10CFR50, Appendix R. Revision 7 of the GPUN Fire Hazards Analysis report was used as a basis for developing the fire scenarios in the PRA. Other modifications that changed cable routing after this revision of the FHA report have not been incorporated in this revision of the PRA.

As the PRA project progressed toward completion, the TMI-1 operating procedures were being modified and upgraded to conform to the B&W Owners Group Abnormal Transient Operating Guidelines. The PRA team has monitored the evolution of these procedures closely and included their impact in the development of the human action failure probabilities.

Each core protection safety function has a priority relative to the others, as shown in Figure 3-3. In general, reactivity control is the foremost function because the amount of heat that must be removed from the core is determined by how well this function is performed. Next in precedence are those functions for appropriately maintaining a core cooling medium. To achieve this, actions must be accomplished to maintain an adequate reactor coolant system inventory and an appropriate reactor coolant system state. Finally, if core heat removal is not carried out, reactor coolant system heat removal is irrelevant. Not only should this hierarchy be kept in mind, but the need for the vital support systems to carry out these safety functions should be recognized.

All safety functions must be accomplished to a degree commensurate with the extent to which they are challenged. Only by doing so can the risk from the hazards of direct or indirect radioactivity release be maintained at an acceptable level. For this reason, safety functions were used in three ways in the probabilistic risk assessment process:

1. To organize the process of determining those initiating events that could threaten the release, either directly or indirectly, of radioactivity as discussed in the Plant Model Report, Section 2.

2. To organize the search for alleviating systems for each initiator, as shown in the event sequence diagrams described in the Plant Model Report, Section 4.

3. To organize an initial set of event tree top events, as described in the Plant Model Report, Section 4.

TABLE 3-1. DEFINITION OF SAFETY FUNCTIONS PURPOSES

SAFETY FUNCTION	PURPOSE
REACTIVITY CONTROL	SHUT REACTOR DOWN TO REDUCE HEAT PRODUCTION
REACTOR COOLANT SYSTEM INVENTORY CONTROL	MAINTAIN A COOLANT MEDIUM AROUND CORE
REACTOR COOLANT SYSTEM PRESSURE CONTROL	MAINTAIN THE COOLANT IN THE PROPER STATE
CORE HEAT REMOVAL	TRANSFER HEAT FROM CORE TO A COOLANT
REACTOR COOLANT SYSTEM HEAT REMOVAL	TRANSFER HEAT FROM THE CORE COOLANT
CONTAINMENT ISOLATION	CLOSE OPENINGS IN CONTAINMENT TO PREVENT RADIATION RELEASES
CONTAINMENT TEMPERATURE AND PRESSURE CONTROL	KEEP FROM DAMAGING CONTAINMENT AND EQUIPMENT
COMBUSTIBLE GAS CONTROL	REMOVE AND REDISTRIBUTE HYDROGEN TO PREVENT EXPLOSION INSIDE CONTAINMENT
MAINTENANCE OF VITAL SUPPORT SYSTEMS	MAINTAIN OPERABILITY OF SYSTEMS NEEDED TO SUPPORT FRONT LINE SYSTEMS
DIRECT RADIOACTIVITY RELEASE CONTROL	CONTAIN MISCELLANEOUS STORED RADIOACTIVITY TO PROTECT PUBLIC AND AVOID DISTRACTING OPERATORS FROM PROTECTION OF LARGER SOURCES

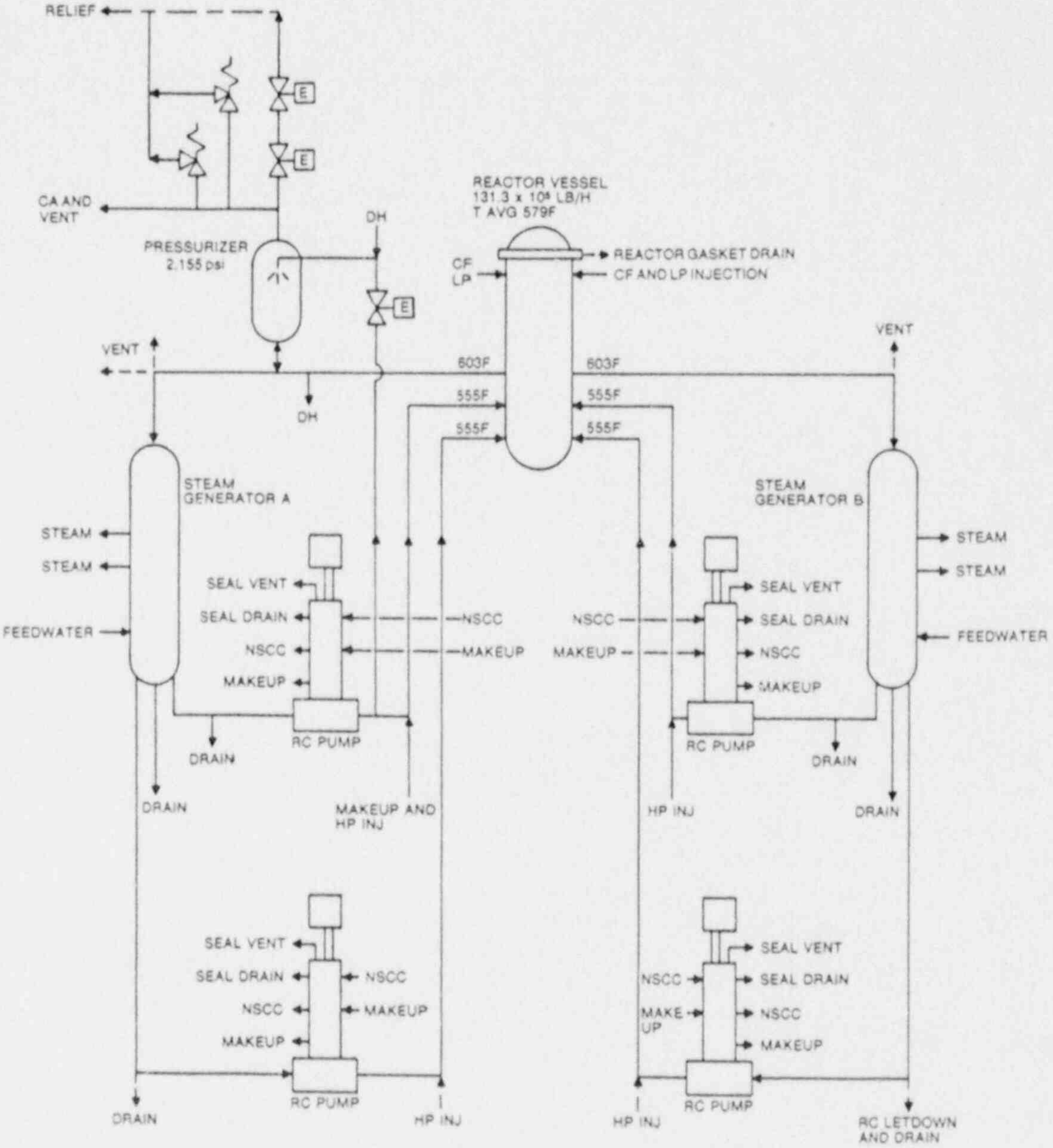


FIGURE 3-1. REACTOR COOLANT SYSTEM ARRANGEMENT FLOW DIAGRAM

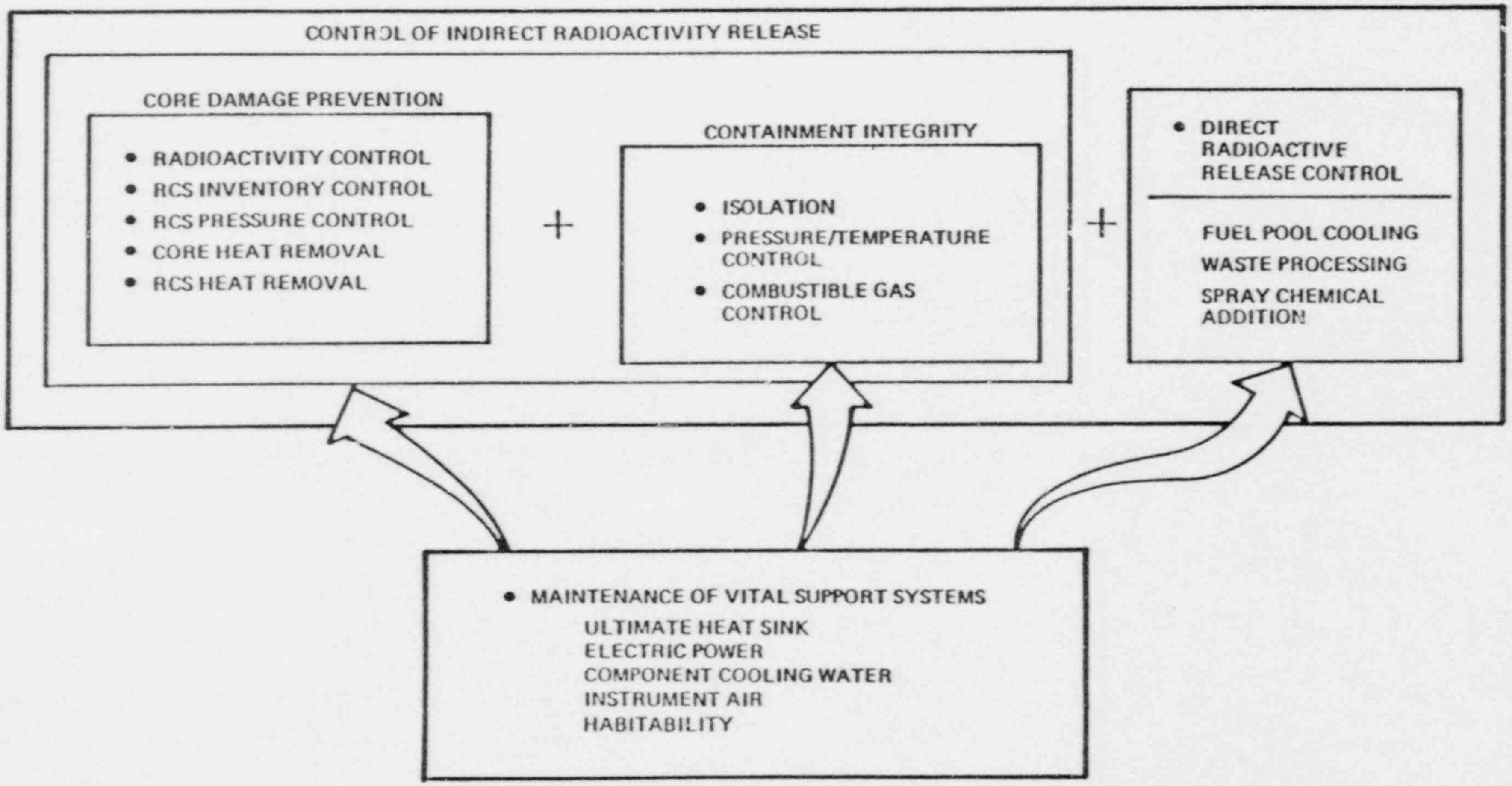


FIGURE 3-2. CLASSES OF SAFETY FUNCTIONS

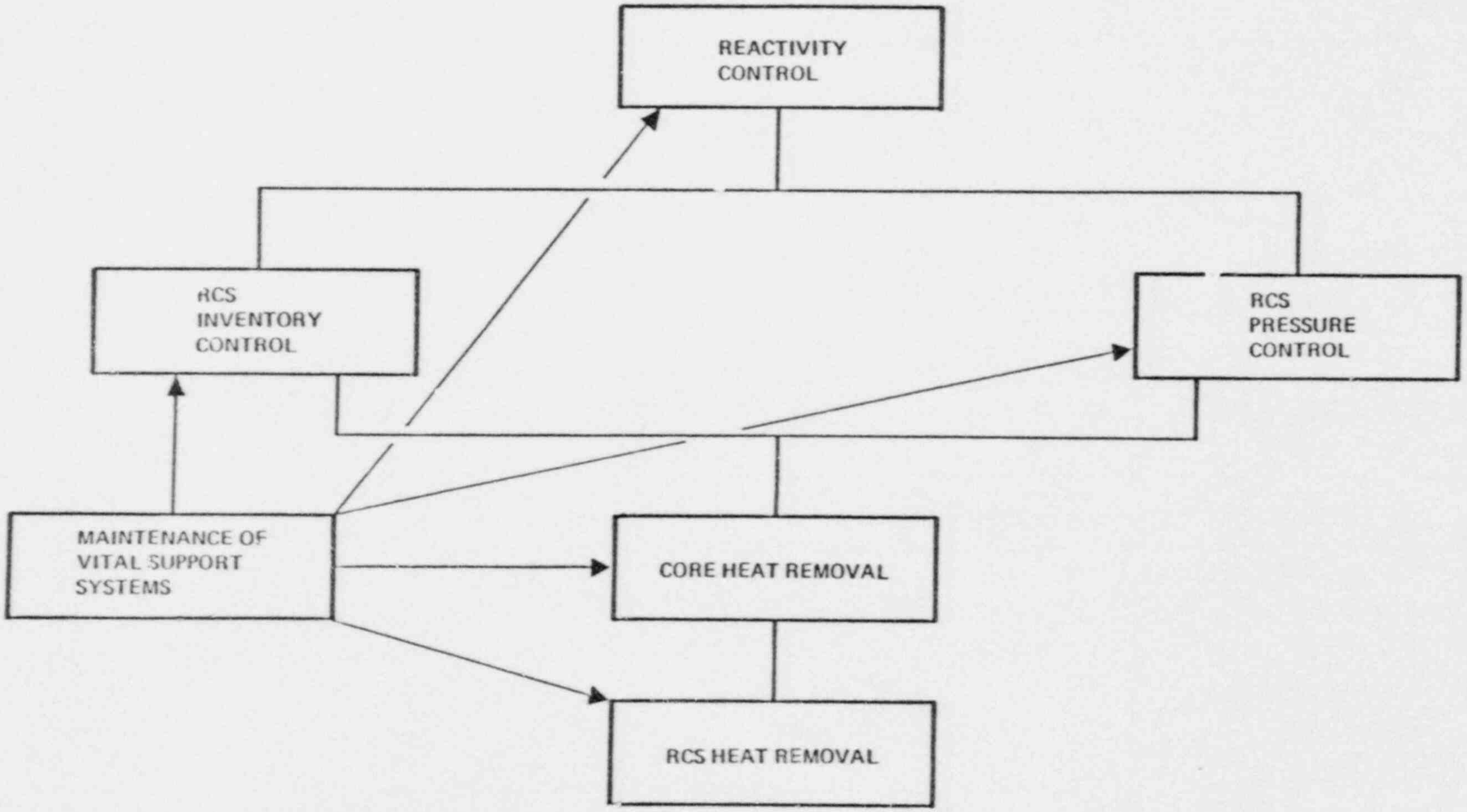


FIGURE 3-3. HIERARCHY OF CORE DAMAGE PREVENTION SAFETY FUNCTIONS

4. PRA METHODOLOGY OVERVIEW

The PRA methodology overview is presented in five sections. In the first four, a presentation is made of the general PLG approach to PRA, highlighting certain aspects of the approach to which we refer in subsequent discussions. These sections are included to agree on terms and thus to facilitate understanding. In general, the methodology described relates to the third level of the three levels of risk assessment defined in the NRC Procedures Guide (Reference 4-1) and presented below:

- Level 1. Corresponds to developing and quantifying the plant systems model with or without considering external events.

- Level 2. Includes both the plant and containment model with or without considering external events.

- Level 3. Includes all three models (plant, containment, and weather-evacuation site) with or without external events.

Section 4.5 describes the PRA process used for TMI-1. This process would be classified, according to the NRC Procedures Guide, as "Level 1, including external events."

4.1 GENERAL PRA PROCESS

In assessing the risk from operating a nuclear power plant, we are attempting to predict the outcome of operating that plant in terms of several measures of damage. Sources of possible damage are called "hazards." Thus, the radioactivity in a nuclear plant may be said to be a hazard to the public. It is not necessarily a "risk," however, since the idea of risk also involves the idea of the likelihood that the hazard will be converted into an actual delivery or realization of damage. Thus, a "risk analysis" can be viewed as consisting of answering the following three questions:

- What can go wrong; i.e., by what scenarios or sequences of events might damage from the hazard be actualized?

- How likely are these scenarios?

- What are the consequences of these scenarios; i.e., how severe is the damage?

To answer these three questions for a nuclear power plant, a structured thinking process was employed that begins with a systematic identification and categorization of all scenarios that might lead to significant damage to the plant or to the public health. Each scenario is then analyzed to determine its frequency of occurrence and magnitude of its consequent damage, as measured by several damage indices.

In calculating these frequencies and damage magnitudes, it is important to explicitly quantify the uncertainty, as any competent scientist does when presenting results. In the case of risk assessment, it is especially important to quantify uncertainty since we are dealing with rare events and with a skeptical audience of regulators, intervenors, and the general public. Therefore, we incorporate uncertainty into the PRA from the beginning, from each piece of input data up to the final results.

The uncertainty in the risk comes from a lack of prior knowledge about exactly how frequently each scenario will occur and exactly what consequences it will produce. Both of these sources of uncertainty are carefully tracked throughout a PRA in order to specify, as accurately as possible, the risk from operating the plant.

Table 4-1 conceptualizes the results of a risk assessment in tabular form, including uncertainty. The likelihood or recurrence interval is expressed as a frequency, ϕ. Consequence magnitude is denoted by X. Uncertainty about frequency and consequences will be expressed by a probability distribution, $P(\phi,X)$. This probability distribution is a function where ϕ and X are the independent variables and P is the dependent variable.

The group of scenarios in Table 4-1 can be represented as a set denoted by braces { }. Each scenario and its risk (i.e., each line in the table) can be put into brackets < >. The total set of scenarios (the risk, R) can then be expressed as

$$R = \{<S_i, P_i(\phi,X)>\}, \text{ for } i = 1,2,\ldots,N \qquad (4.1)$$

where

S_i = a scenario identifier or description.

$P(\phi_i,X_i)$ = joint probability distribution on the frequency of occurrence, (ϕ_i), and the consequences, X_i, of scenario S_i.

The form typically used in presenting risk assessment results today is the cumulative or frequency of exceedance form. In the frequency of exceedance form, the frequencies of all scenarios exceeding a particular level of damage are summed. Curves that are the locus of all ϕ_x^t points for a given damage type, t, and probability, $P(\phi_x^t,X_t)$, are the family of risk curves in frequency of exceedance format for that damage type (see Figures 4-1a through 4-1g).

4.2 QUALITATIVE DEFINITION OF SCENARIOS AND THEIR CONSEQUENCES

Each scenario consists of an initiator or something that starts a sequence of events. This might be a system failing, a pipe breaking, a fire, or a human error (something that perturbs the reactor cooling system). The rest of the scenario consists of manually and automatically actuated actions or passive processes that determine the consequences of the scenario. These actions, or events, consist of systems, working or not; buildings and pipes, remaining intact or not; the direction and speed of the wind when the scenario extends to a release; whether it rains during a release; how people move away from the plume, etc.

In the PRA, all scenarios were defined by a combination of deductive and inductive processes. First, a set of all possible initiating events was deduced. Then, the events that occur in each scenario subsequent to the initiator were characterized inductively, using event trees and a meteorological sampling process.

In principle, it is desirable to make this process as thorough as possible; i.e., to list in great detail all possible scenarios and determine the consequences of each one individually. In a plant such as TMI, however, this could make the list run into millions of scenarios. Methods are used to group similar scenarios into a manageable number of scenario categories.

This grouping will be done by dividing each scenario into four parts:

1. The initiating event.

2. The subsequent events that are determined by the performance of the plant systems.

3. The phenomenological events that occur in the core and containment after the initiation of core damage.

4. The weather and evacuation-related events.

Each of these types of events for each scenario becomes part of a plant or site performance model. All events in the scenario will be modeled either in the plant model, the containment model, or the site (really offsite) model. This means that each scenario when finally assembled consists of three scenario fragments, one from each of these three models. The events in each one of these fragments were defined as being conditional on a certain set of events having previously occurred. Therefore, after a set of interfaces or "pinch points" between models has been agreed on, each model can be developed separately. It also means that the scenarios have to exit each model in one of a certain predefined set of states. After being assigned to this pinch point state, the scenario no longer has its own identity; it is just one member of a group and is treated in the same way as all other members of that group in the succeeding models. These pinch point states define the initiating events, or crucial conditions, for the succeeding model. Therefore, they will contain only the information that must be transferred from the preceding model to the next model because that information is important to what happens in the next model.

4.3 QUANTIFICATION OF SCENARIO FREQUENCY

4.3.1 SCENARIO FRAGMENT FREQUENCIES

Once the possible scenarios have been qualitatively defined, it becomes necessary to calculate the frequency with which they occur. In the simplest terms, this process consists of combining the likelihood of the initiating event with the conditional likelihood that each successive event occurs, given all of the preceding events. The resultinç overall scenario frequency can be expressed by the equation

$$\phi_i = \phi^I \cdot f(1|I) \cdot f(2|I,1) \cdot f(3|I,1,2) \ldots f(M|I,1,2\ldots,M-1) \quad (4.2)$$

where

ϕ^I = the initiating event frequency.

$f(1|I)$ = the conditional frequency of the first subsequent event in the scenario, given that the initiating event, I, has occurred.

.

.

.

$f(M|I,1,2\ldots,M-1)$ = the conditional frequency of the last event, M, in the scenario, given that the initiating event and the first M-1 subsequent events have occurred.

The frequencies, f, are called conditional split fractions of top events because they represent the likelihood that a scenario branches one way or the other in an event tree, given that certain previous events have occurred. The events in event trees are described at the top; thus, they are called top events. A scenario splits and follows either a success or a failure branch. Depending on which branch it follows, a different scenario will evolve.

The conditional split fractions in Equation (4.2) come from the model in which the event is defined. For instance, events 1 and 2 (with frequencies f(1|I) and f(2|I,1)) might be quantified in the plant model, event 3 in the containment model, and event M in the site model. This leads to the establishment of a conditional frequency or split fraction for the whole scenario fragment corresponding to a particular model; e.g., f(PLANT MODEL FRAGMENT|I) = f(1|I) · f(2|I,1). The concept of such scenario fragment frequencies is extremely useful because it allows the overall scenario likelihood to be calculated in three independent parts, which can then be assembled. If one frequency changed, the others would not be affected; only the assembly would have to be redone. Most important, perhaps, is the ability to characterize the dependence of the total risk on interesting intermediate points in the scenario; for instance, to decompose the risk of early fatalities to show how it depends on the responses of the plant systems (the output of the plant model).

4.3.2 THE MATRIX VIEW

The process of decomposing the risk into its contributors is greatly aided by viewing the frequencies in each model in a matrix context. This point of view is illustrated in Figure 4-2.

Each model in this figure may be regarded as a transition operator, or matrix, which defines the likelihood that various entering scenarios will exit in particular states; that is, the likelihood that a given entering scenario will end up passing through a particular set of events in the model. The idea of such a transition matrix is that the identities of the exact events in the scenario are not as important as the condition of the plant when the scenario exits to the next model. This is saying that knowing whether system A or B failed is not as important to the containment model as knowing whether the RCS pressure was high when the plant model scenario resulted in core damage and whether the containment heat removal systems are still operating.

If the initiating events are grouped, their frequencies can be represented by a vector, ϕ^I, where each element ϕ_i^I is the total frequency of that group measured in occurrences per year.

For example, the scenarios enter the plant model after their initiating event, I, and exit in state j with conditional frequency M_{ij}, which is equal to the sum of the frequencies f_j(PLANT MODEL FRAGMENT|I_i) for all plant model fragments going to exit state j from initiator I. The set of these M_{ij} may now be represented as a matrix, which will be called the plant matrix.

The frequencies of the individual scenarios that enter from initiator i and exit in state j are no longer distinct. The product $\phi_i M_{ij}$ is the total frequency of all such scenarios. However, the problem has been considerably simplified. Instead of dealing with hundreds of scenarios that might make this transition, it is only necessary to deal with one group represented by one scenario. The initiating events that were used for TMI entering the plant model are listed in Table 4-2, and the exit states are the plant damage states listed in Table 4-3.

Plant damage states reflect the degree to which plant systems function properly in response to an initiating event. If all systems necessary to prevent core damage during the scenario operate properly, the scenario does not go to a PDS but, rather, to a success state.

The frequencies of the plant damage states have been computed. The next step in the risk assessment/scenario definition process is only performed for a level 2 or level 3 PRA. This step is to translate information on how well the alleviating systems work into information about how radioactive materials may be released. This release will come from the reactor core and go to the area surrounding the plant, depending on the plant system performance. A conditional containment and degraded core model or, simply, containment model will be used to perform this task.

This model treats core damage progression phenomena and the physical processes that are involved. The analysis for the containment model reaches deep into the plant activities, particularly with respect to core behavior and the impact of the containment engineered safety systems following core damage. Many studies, experiments, and analyses are examined to provide a strong technical basis for quantifying containment response. Central to the containment analysis is identifying the response of the containment to the progression of a degraded core accident. Supporting the model are the results of numerous analyses and studies of physical processes. For example, analyses of degraded core phenomena (including in-vessel effects, vessel failure, and ex-vessel effects) and experiments and studies on steam explosions and hydrogen generation and combustion were all used as input to the model.

The containment model can be represented as a containment matrix, C, where the elements, C_{jk}, would represent the conditional frequency of emerging from the containment model in release category k, given that we enter it in plant damage state j.

Typical release categories are listed in Table 4-4. It is expected that similar ones may be developed for TMI-1 if a level 2 or level 3 PRA is performed in the future. These release categories represent different characteristics of releases that impact the extent and kind of damage the releases will inflict on the surrounding population. Among these characteristics are whether the release begins early or late, whether it leaves through the top or side of the containment building or through the basemat, and whether the sprays are operating to scrub radioactivity from the air when the release begins.

The site model estimates the potential for producing a particular level of damage among the surrounding population due to each of the containment release categories. The damage indices that are usually used in PRAs are listed in Table 4-5. To determine the health effects from a release, a distribution of airborne and deposited radioactive material in the environment will be defined as a function of time. There are many factors that determine the nature and extent of health effects. The most important are the evacuation strategy and the weather conditions that exist during the release. The approach that is taken in a PRA is to study a large number of individual weather scenarios for each particular type of release. Any plume that is projected to leave the site area is assumed to be influenced according to weather data taken from the nearest measurement station; i.e., hourly data taken from multiple sites. The models employed permit the plume to vary in direction according to the wind direction. Other important factors are the population distribution and the evacuation conditions. A variable direction evacuation scheme is used to build into the analysis the ability to depict actual emergency planning.

As with the plant and containment, the site model can be represented by a site matrix, S, where the elements S_{k,X_t} represent the conditional frequency of magnitude X of damage type t, given that a release in category k has occurred.

Using these three matrices (M, C, and S), the risk calculation can be symbolically represented by combinations of matrix operations.

Starting at the left side of Figure 4-3, the assembly process then consists of the following steps. The product of the initiating event vector with the plant matrix, M, yields a new vector, $_{\phi}y$:

$$_{\phi}y = {_{\phi}I}M$$

The elements of ϕ^y, are the unconditional frequency of occurrence of each plant damage state, y_j (measured in occurrences per reactor year). ϕ^y is called the unconditional plant damage state frequency vector.

If this vector, in turn, is now multiplied by the containment matrix, C, the vector ϕ^ρ is obtained.

$$\phi^\rho = \phi^y C$$

The elements of ϕ^ρ are the frequency of occurrence of release category k (measured in occurrences per reactor year). ϕ^ρ is referred to as the unconditional release category frequency vector.

Finally, multiplying ϕ^ρ by the site matrix, S, yields

$$\phi^t = \phi^\rho S$$

The elements of ϕ^t are the frequency of occurrence of level X of damage type t (measured in occurrences per reactor year).

Substituting each previous vector equation into the next one, we obtain the relationship between ϕ^t and ϕ^I, as follows:

$$\phi^t = \phi^\rho S = (\phi^y C)S = ((\phi^I M)C)S = \phi^I MCS$$

This equation shows how the results of the plant, containment, and site models are assembled with the initiating event frequencies to yield risk results. The assembly process proposed for TMI-1 only goes through the unconditional plant damage state frequencies.

4.3.3 DECOMPOSING THE SCENARIO FREQUENCIES

An important result of using the matrix formalism is the ability to decompose the final results through matrix manipulations to determine the contributions of each pinch point scenario group to the total risk. For instance, the dominant plant model scenarios contributing to public health risk could be determined by finding the dominant plant damage states contributing to a particular offsite consequence type (e.g., early fatalities) and then finding the highest frequency plant model scenarios going to these PDSs.

The key to this process is the formation of a square diagonal matrix from the frequency vectors for the pinch point groups. In the case of the dominant plant model scenario fragments, the vector ϕ^y is made into a square matrix

$$\phi_D^y = \begin{bmatrix} \phi_1^y & 0 & \ldots & 0 \\ 0 & \phi_2^y & & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ . & . & \ldots & \phi_N^y \end{bmatrix}$$

which, if multiplied by the product of the containment and site matrices, C and S, yields

$$\phi_D^y CS$$

a matrix whose elements are the contributions of each PDS to each damage level (e.g., the frequency with which PDS 3B produces 100 or more early fatalities).

Similarly, the contributions of initiating events to PDS:

Frequency ($\phi_D^I M$)

Release Category Frequency ($\phi_D^I MC$)

and

Offsite Damage Frequency ($\phi_D^I MCS$)

may also be calculated in this way. Also PDS contributions to release category frequency ($\phi_D^Y C$) and release category contributions to offsite damage level exceedance frequency ($\phi_D^\rho S$) may be determined in the same manner. The results of the decomposition process performed in the TMI-1 PRA is described in Section 5 of this report and in even more depth in Section 6 of the Plant Model Report.

4.4 UNCERTAINTY

The process of identifying each member of the scenario list and quantifying its point estimate frequency has now been described. It remains only to describe how to express our state of knowledge about these frequencies. Our state of knowledge about any frequency from that of a basic component on up to core damage frequency is expressed in "probability of frequency" format. This format is defined and described in Section 1.5.6. The following process is used:

1. All possible scenario initiators (initiating events) are identified, and their probability of frequency distributions, $P(\phi_i)$, are calculated.

2. A model of the response of the plant and site to each initiator is developed, and the conditional frequency with which the plant would respond in each specified way (given that the initiating event occurred) is characterized by using probability distributions.

3. All the combinations of initiating event probability of frequency distributions and the conditional plant response probability distributions are then combined to first generate a probability curve characterizing the state of knowledge about the frequency of each scenario and then to find the probability of frequency distribution of the PDS; then, the PDS curves are combined to produce a core damage frequency curve.

Just as in the matrix theory formalism described in Section 4.3.2, the probability of frequency distributions can be combined or grouped to produce a single distribution to represent the frequency of each group at each pinch point. Figure 4-3 shows the process and Figures 4-1a through 4-1g show the probability of frequency curves produced at each pinch point and for each element in the plant, containment, and site matrices. The distributions corresponding to the elements in the plant, site, and containment matrices are progressively combined from initiating event probability of frequency distributions to final risk curves, just as was done with the matrices, but this time including the PRA team's uncertainty. From Equation (4.1), each discrete damage level, X_t, now represents a new subset of grouped scenarios or doublets. The total scenario set of Equation (4.1) is thus represented by the bounding approximation

$$R = \{<S_i, P(\phi_i, X_{i,t})>\} \qquad (4.3)$$

$$\text{for } i = 1,2,\ldots N_t'$$

where N_t' is the total number of scenario groups contributing to damage type t. The total range of damage considered is thus discretized into the intervals $[X_t, X_t + \Delta X_t]$ for ease of computation, then summed and smoothed out in the final risk curves. (See Appendix B, Section 1, for a description of this smoothing process.)

Figure 4-3 shows the probability of frequency curves produced at each pinch point and for each element in the plant, containment, and site matrices. These uncertainties in turn imply uncertainty in the final risk curves of Figure 4-3. This uncertainty is displayed by giving a family of curves with probability or confidence level P as the parameter of the family. Thus, we obtain what we call a "risk curve in probability of frequency format," Figures 4-1c through 4-1g.

These curves are read in the following way. Let Φ_1 be the ordinate over point x_1 of the curve labeled P = .90 (the 90th percentile curve). Then, we would say that we are 90% confident that accidents resulting in damage x_1 or greater occur with a frequency no greater than Φ_1.

One such risk diagram is prepared for each damage type; e.g., fatalities, injuries, population dose, etc. The set of these diagrams thus constitutes the quantification of the public health risk in graphical form. In the case of the TMI-1 PRA, which was a Level 1 PRA including external events, tne risk assessment process consisted of the part shown in Figure 4-4. The output is a figure, such as Figure 4-1a, showing what has been found out about the frequencies of the various plant damage states and their sum, the core damage frequency itself, and a core damage probability of frequency cumulative curve. The curves of this type produced during the TMI-1 PRA are shown in Section 5 in Figures 5-1 and 5-2.

The following sections describe how the distributions corresponding to the elements in the plant are combined to progress from initiating event probability of frequency distributions to plant damage state probability of frequency curves, just as was done with the matrices, but this time representing the uncertainty with its whole curve instead of just with the mean value of the curve.

4.4.1 INITIATING EVENTS

As will be explained in Section 4.5.2.1, the initiating events are first defined and grouped by similar effects; then, a probability of frequency distribution

$$P(\phi_i^I)$$

is calculated for each initiator group i.* This type of distribution is represented by curve Ⓐ at pinch point I in Figure 4-4 and is given by

$$P(\phi_i^I) = \sum_{k=1}^{N_i} P(\phi_{ik}^I)$$

where

N_i = the number of initiating events producing effects to be represented by group i.

ϕ_{ik}^I = the frequency of the kth initiator in initiator group i.

The distribution $P(d_i^I)$ can be calculated from the probability distributions for the individual ϕ_{ik}^I, given by $P(\phi_{ik}^I)$, according to the instructions given in Appendix B, Section B.2.

4.4.2 PLANT SYSTEMS MODEL

The plant model translates the probability of frequency distributions for the initiating event groups given by $P(\phi_i^I)$ (curve Ⓐ at pinch point I in Figure 4-4) into probability of frequency distributions for the plant damage states given by $P(\phi_j^y)$ (curve Ⓒ at pinch point II in Figure 4-4). This process is accomplished using probability distributions for the conditional frequencies of transition from each initiating event group to each plant damage state. The probability

*Throughout this discussion, notation of the form $P(\phi)$ will be used to denote the probability distribution of frequency ϕ. $P(\phi_i^I)$, for instance, refers to the probability of frequency distribution for initiating event group i. It does not refer to the function P evaluated at a specific numerical value of that frequency.

distribution for the frequency of transition from initiator group i to plant damage state j is represented by $F(M_{ij})$ and is shown as curve Ⓑ in Figure 4-4.

Actually, the transition frequency from initiator group i to plant damage state j is calculated by combining the frequencies of all plant model scenarios making this transition. These individual scenarios can be thought of as the plant model doublets,

$$<S^{P}_{im}, P(\tilde{\phi}_{im}, PDS_j)>$$

where

S^{P}_{im} = the mth plant model scenario in initiator group i.

$P(\tilde{\phi}_{im}, PDS_j)$ = the joint probability distribution for the frequency and resulting plant damage state of that scenario.

Hundreds of such scenarios may originate from initiator group i, and their conditional frequencies must be combined to develop the distribution, $F(M_{ij})$. These scenarios are identified on event trees. The probability of frequency distribution for each scenario is developed by combining the distributions for each of the events in that scenario.

The probability of frequency distribution for plant damage state j is given by

$$P(\phi^{y}_{j}) = \sum_{i=1}^{N_j} P(\phi^{I}_{i}) \;\; F \;\; (M_{ij})$$

where N_j is the total number of initiating event groups that can result in plant damage state j. This distribution can be calculated from the individual probability of frequency distributions $P(\phi^{I}_{i})$ and $F(M_{ij})$ according to the procedures spelled out in Appendix B. However, the process will be somewhat more complicated than the process for computing $P(\phi^{I}_{i})$ because $P(\phi^{y}_{j})$ is a sum of products rather than a simple sum.

The plant model was quantified in two steps. The first step was to identify the plant scenarios of highest frequency for each plant damage state. This was done using a single value, usually the mean, to characterize each distribution. (The mean was chosen because it contains information about the high frequency tail of the probability distribution.) These mean values were then combined and propagated through the entire risk model, as described under the matrix formalism above. Based on these point estimate results, the risk dominant plant damage states and the highest frequency scenarios in each were chosen. In the second stage of the analysis, probability distributions were propagated through the plant systems model for these dominant scenarios.

This two-step process necessitated keeping track of all the high frequency scenarios leading to each plant damage state. The identity of these scenarios was maintained to be able to write logical expressions for the probability of frequency distributions of the plant damage states (curve Ⓒ in Figure 4-4) in terms of the probability of frequency distributions for the system failures and initiating events.

With risk defined fundamentally as a list of scenarios or event sequences, the key requirement of a risk assessment methodology is an orderly procedure for defining the scenarios. For this purpose, we use a number of logical methods, most notably the master logic diagram, event sequence diagrams, event trees, fault trees, cause tables, and environmental tables. These methods are described in the Plant Model Report, and their development is described in the tasks in Section 4.5 of this report. Underlying the logical methods used for organizing results are fundamental engineering analyses reflected in the Plant Model Report and in all the other TMI-1 PRA reports.

4.5 TMI-1 PRA PROCESS

Based on our PRA experience, the TMI-1 PRA was conducted in two phases which consist of a "mini" or "focusing" PRA prior to starting detailed work followed by a subsequent detailed risk assessment. This two-phase approach allowed the early use of PRA results and facilitated the development of the detailed risk model.

During Phase I, those systems or initiating events likely to be important to the overall plant risk were identified, thus giving early warning of further required analysis and/or information; the particularly troublesome physical processes that called for more detailed analysis in Phase II were revealed before development of final event trees. The approach adopted in Phase II was based on our findings during Phase I. The Phase I results were documented in a separate report, PLG-0354 (Reference 4-2).

The approach used during the development of the TMI-1 PRA is described in detail in the individual TMI-1 reports that make up the documentation of this PRA and whose tasks are summarized in the following sections.

4.5.1 PHASE I PROCESS

4.5.1.1 Plant Familiarization

This task was conducted to identify information sources and to gather specific plant design and operation information specific to Three Mile Island Unit 1. This information helped in the early identification of major potential risk contributors, which led to the definition of a detailed project schedule and a rational allocation of project resources.

4.5.1.2 Initiating Event Identification

A small set of initiating events was chosen to define scenarios representative of major risk contributors. This effort reduced the number of scenarios considered, while ensuring concentration on issues of major relevance for Phase II. All possible initiating events were included in one of six initiating event groups. The frequency of each group was calculated from the sum of all the initiating events. The initiating event groups used were:

1. Turbine Trip. Used to represent transients with main feedwater available.

2. Loss of Offsite Power.

3. Loss of Main Feedwater.

4. Medium Loss of RCS Inventory. Used to represent small as well as large loss of RCS Inventory.

5. Steam Generator Tube Rupture. Used to represent very small LOCAs also.

6. Loss of River Water to the Pumphouse Intake Basin.

4.5.1.3 Preliminary Systems Analysis

The preliminary systems analysis was conducted in two parts. The first part was an initial screening that encompassed all TMI-1 systems. System summaries were developed to determine the normal and alleviating actions of each system. Alleviating actions are those performed to reduce the consequences of an initiating event. Success requirements were identified for all alleviating actions, as discussed in the next section; i.e., the plant model. Each system was also classified as to whether further analysis was required. Those requiring no further analysis were so noted, and their system summaries were filed. (It is important to understand that although systems analysis is discussed here first, that plant modeling and systems analysis are iterative tasks.)

The second part of the systems analysis task was an analysis of those systems that passed the initial screening and therefore needed to be analyzed in sufficient detail to estimate their availability and to develop event tree top events. The estimation was conducted in one of two ways, depending on the system involved:

1. For those systems that are very similar to their Midland or Seabrook counterparts and whose models were not significantly different (i.e., similar logic, success criteria, and support systems states), the conditional split fractions from the Midland or Seabrook PRA were used.

2. When significant differences in system logic were noted, block diagram logic models were used that included independent hardware failure, maintenance, testing, human error, and common cause failure terms. The unavailability expressions were then quantified using data from either the Midland or Seabrook PRA data bases.

4.5.1.4 Phase I Plant Model

A plant model was developed to represent the scenarios, progressing from the six initiating events through to the plant damage states. For calculational convenience, the plant model was split into three submodels; namely, a frontline systems model for early response, a frontline systems model for late response and for response of the containment safety features, and a support system model. These event trees represented all the important alleviating systems and dependencies between systems.

4.5.1.5 Phase I Analysis of External Events and Spatial Interactions

The objective of this task was to identify externally initiated events (such as aircraft crashes, floods, earthquakes, etc.) and spatial interactions that may result from internally initiated accidents, such as fires, pipe breaks, missiles, etc., that were most relevant to TMI-1 This preliminary study determined the level of study effort in Phase II.

4.5.1.6 Preliminary Plant Damage States

A preliminary set of plant damage states was developed to estimate the severity of each scenario. A plant damage state defines the conditions in the RCS and the availability of the containment safety features at the time of core damage. Such PDSs were developed to perform a containment analysis on the core damage scenarios if it is desired in the future.

4.5.1.7 Assembly Process

The objective of this task was to put together the sequences from the three sets of event trees in the plant model and to estimate the frequencies of occurrence of the most important scenarios for the TMI-1 PRA. These frequencies determined the relative importance of scenarios for their contribution to severe core damage; these frequencies and the scenario PDSs determined their contribution to risk. To a large extent, this task relied on PLG's previous PRA experience.

4.5.2 PHASE II PROCESS

4.5.2.1 Detailed Definition and Grouping of Initiating Events

The dual objective of this task was to complete a list of all the initiating events for consideration in the TMI-1 PRA and, for calculational convenience, to group them into a reduced set according to plant impact.

A detailed definition of initiating events was then performed by means of a master logic diagram, which enabled us to categorize initiating events according to the safety functions threatened, the threatening effect, and the cause of threat. This resulted in identifying 46 initiators. We then further grouped these initiators into 18 groups when their impact on the plant initiated identical plant response sequences within the plant model event trees. The selection of initiating events was based on those initiating events having th greatest number of top events envisioned in the course of developing the event tree for the initiating event in question. A complete treatment of the definition of initiating events may be found in Section 2 of the Plant Model Report, and the calculation of their frequency is found in the Data Analysis Report.

4.5.2.2 Development of Detailed List of Internally Initiated Accident Scenarios

As in Phase I, the internally initiated scenarios were developed by means of three models: the support system event tree model, the frontline system early response models, and the frontline system late response event tree models. This task refined the Phase I plant model in which many issues concerning scenario development were intentionally left undetailed.

The many support system success and failure permutations (6,513) were reduced to a smaller number for calculational and modeling convenience. The reduction was made on the basis of the impact that these sequences would have on the frontline systems. This process yielded 1,104 unique sets of event tree scenarios that produce identical frontline system impacts called impact vectors. These impact vectors were grouped further by putting all very low frequency impact vectors into a single group with an enveloping impact. This effort produced 145 impact vectors. In an effort to further reduce these vectors to a more manageable number of corresponding runs of the frontline system event tree model, we further grouped these impact vectors according to similarity of impact and frequency into 39 common support system states with enveloping impacts.

Although grouping was done conservatively, care was taken to ensure that the degree of conservatism introduced was minimal. This was accomplished by ensuring that impact vectors with little impact on frontline systems, but with relatively high frequencies, were not combined with low frequency impact vectors having substantially more impact on the frontline systems. The support systems event tree and the combining according to impact are both described in Section 3 of the Plant Model Report.

Also, part of this task was the development of event trees for 20 additional initiating events. These event trees included recovery actions and one set of split fractions for each support system state to properly account for the boundary conditions placed on the frontline systems by the support system availability. Fifty unique early and late response frontline event trees were produced. A detailed description of the development of the frontline event trees is contained in Section 4 of the Plant Model Report.

The Phase II plant model consists of three segments, one for all the support systems and one each for the early and late response frontline systems. The early response frontline event trees were called "main" trees, and the late response frontline trees were called subtrees. The scenarios in the main trees resulted in either success or input to subtrees; the end states of the subtrees were success or plant damage states. A version of each main and subtree was made for each support system state. Each plant model scenario was then constructed by combining a scenario fragment from each of the three trees. A scenario fragment is a particular path or sequence in one of these three consecutive trees. The three types of trees are sequential and represent one large plant model event tree that would go from initiating event to plant damage state.

4.5.2.3 Data Analysis

This task was performed to provide failure rates and component repair times required in the conduct of the systems analysis that follows and initiating event frequencies for the quantification of scenario frequencies in the event trees.

The data analysis consisted of the four major work elements described below:

- Definition of Data Requirements. The first step was to ensure compatibility between the data analysis and the systems analysis tasks. Data requirements for each system model were reviewed. A common level of detail was fixed and component failure modes were scoped for each model. This intertask review served to focus both the data base development effort and the systems modeling tasks toward a level of detail commensurate with the available data.

- Generic Data Base Development. PLG had developed a computerized generic data base for probabilistic risk assessments that they have performed in the past. The information in this data base includes data collected for other plants for which PLG has performed PRAs, as well as data from WASH-1400 and other sources. This data base served as the starting point for the TMI-1 plant-specific data analysis. The generic data base was reviewed to ensure applicability to TMI-1, and new failure and success information was incorporated to update the generic data base. The failure rate estimates and the assigned weights were combined to obtain new generic state-of-knowledge distributions. The result was a probability distribution for each parameter that reflects the range of information embodied within the literature. The types of data included in the data base were:

  - Component Failure Rate Data. The available generic data were reviewed to ensure consistency with the needs of the TMI-1 PRA. Subjective weighting factors were assigned to each piece of data, based on the compatibility of the source with the way the data were used in the PRA. In many cases the failure rate data obtained from power plants examined in previous PLG risk assessments provided important input to these relative weights.

  - Component Maintenance Data. Generic component maintenance data were accumulated from other power plants. Information about both frequency and duration of maintenance is necessary to determine component unavailability. The frequency of maintenance defines the rate that components are removed from service; the duration defines the time the components are out of service. Separate distributions were developed to represent the uncertainty in the frequency and duration of maintenance.

- Common Cause Failure Data PLG's data base includes beta factor distributions for several key components. These distributions were based on review and classification of reported nuclear power plant dependent and independent failure incidents.

- Human Error Rates. The chief sources of generic data on human error rates were the NRC Human Reliability Handbook (Reference 4-3). Along with other sources, this document was used to provide human error rates in numerous situations. The uncertainty associated with these data was also represented as a distribution.

- Initiating Event Frequency. The plants included in the generic initiating event data base were selected on the basis of similarity to the TMI-1 plant and on the data availability. The data in Reference 4-4 (EPRI NP-2230) were supplemented by data from monthly operating reports, the Nuclear Regulatory Commission's "Licensed Operating Reactors Status Summary Reports" (the "Grey Books," Reference 4-5), and Nuclear Power Experience reports.

- Plant-Specific Data. Based on our Phase I site visit, a large volume of valuable information about TMI-1 equipment operating history was extracted from plant records. The amount of information available in TMI-1 control room operating logs, test reports, maintenance records, etc., about the number of equipment failures, operating hours, and component demands determined the degree of influence of plant-specific data. This required failure and success event data records.

  Similarly, plant-specific component maintenance frequency and duration data were extracted by reviewing the history of repair and maintenance activities at TMI-1. For initiating events, we sought the number of occurrences and the number of operating years.

- Bayesian Combination of Generic Data Base and Plant-Specific Data. The plant-specific data were combined with generic information, using Bayes' theorem to provide a TMI-1-specific data base that includes all available data and their uncertainty.

The Data Analysis Report offers an in-depth description of all the data base development.

4.5.2.4 Systems Analyses

A system analysis was performed for each of the 17 systems listed in Table 4-6. The objective was to develop a model of system performance to be used for the quantification of each top event conditional frequency, i.e., split fraction. The analysis of each system split fractions is described in the Systems Analysis Report.

In each systems analysis, the first part consisted of a definition of the analysis. In this section, the functions being analyzed were described and a brief presentation was made of the top events and the split fractions pertaining to the analysis. Based on this information, the top events were defined in detail with the success criteria for each of the split fractions. As a final step, the boundaries of the equipment included in the system analysis were described.

The second part of the system analysis was a description of the logic models used for the quantification of top event split fractions. The logic model description consists of:

- Support Systems Needed
- Systems Supported
- Equipment Shared with Other Systems
- Automatic Actions
- Manual Actions
- Operator Emergency/Recovery Actions
- Controlling Station Locations, Indications, and Alarms
- Testing and Maintenance Requirements
- Technical Specifications, Limiting Conditions for Operation, and Surveillance

A block diagram model was constructed showing the success logic for the system in several alignments, including normal, test, maintenance, and misalignments. Based on these block diagrams, fault trees were developed on the block level to convert the success logic of the block to failure logic and to include common cause failures; the main function of the fault trees was to allow computerized sorting of the minimal cutsets to develop algebraic equations for calculation of split fraction frequencies.

Third, an algebraic equation was developed for each alignment, based on the minimal cutsets for that alignment. Each minimal cutset frequency was determined by algebraic equations that combine basic event frequencies; then, by combining the equations for each alignment, an equation for the split fraction frequency was produced. Finally, each split fraction frequency equation was quantified using the computer code RISKMAN3.

4.5.2.5 Human Actions Reliability Analysis

The objective of this task was to evaluate operator performance during accident scenarios. The scope of the analysis was to quantify the effectiveness of selected human actions to delineate the human contribution to the frequency of core damage and plant damage states.

Only selected human actions were analyzed. In the first part of the study, we separated human actions by type to include routine, inadvertent initiators, dynamic human actions, and recovery actions.

- Routine Actions. These include those actions performed prior to the accident initiator, typically involving testing and maintenance, which may result in inadvertent system misalignments. Routine actions may affect the operation of the system in question by way of either partial degradation or complete disablement. In either case, however, the effect of routine actions was included in the system's performance as part of the systems analysis.

- Inadvertent Initiators. These include actions that inadvertently initiate plant events; e.g., cause a reactor trip. These events are an implicit part of the historical data base used for the estimation of initiating event frequencies. Therefore, the quantification of these human actions was not included here.

- Dynamic Human Actions. These include (1) actions performed during a scenario to supplement the automatic response of plant systems to mitigate the event, (2) actions that may change or detract from the automatic response of plant systems, and (3) specific actions that restore previously failed systems by realignment. Dynamic actions were identified when called out by the plant procedures, which were reviewed during the development of the event sequence diagrams.

- Recovery Actions. These refer to more complex activities to restore previously failed systems or to start systems where automatic actuation is not available. Recovery actions were chosen to address accident sequences whose significance became clear only after preliminary rounds of quantification. Recovery actions were evaluated by means of recovery models, which simulate situations of decision making under conditions of high stress and little time for detailed planning. The results from the recovery models were in the form of a frequency of recovery, given a particular set of boundary conditions. This frequency of recovery formed the split fraction of the top event "system recovery" that was incorporated into the system event tree.

The Human Actions Analysis Report describes the methodology, the analysis, and the results of the evaluation for all the types of operator actions described in this section.

4.5.2.6 Environmental and External Hazards Analysis

The objective of the environmental hazards analysis was to establish the risk from internally generated hazards, such as fire, internal flooding, steam, smoke, etc. The objective of the external hazards analysis, on the other hand, was to determine the risk from external hazards, including external floods, tornadoes, aircraft crashes, earthquakes, and the like.

The environmental hazards analysis was divided into two parts: (1) the identification of environmental hazard scenarios in a process called spatial interactions analysis and (2) the assessment of their importance compared to other contributors to risk by inclusion in the PRA assembly process.

To determine the significant spatial interactions, it was necessary to know the component inventory at each location in the plant. The critical equipment, piping, and cables vital to alleviating accident scenarios in each of the "fire locations" from the GPUN analysis (Reference 4-6) for 10CFR50, Appendix R (Reference 4-7), and the possible propagation of hazards among these locations were identified. Then, an exhaustive list was made of the sources of environmental hazards existing at each location.

In the second step, the spatial interaction scenarios were incorporated into the general PRA assembly process. To do this, the spatial interaction scenarios were divided into three categories: those giving rise to an initiating event, those disabling one system, and those giving rise to an initiating event and simultaneously disabling one or more systems. The contribution to risk from the scenarios of the first two categories was accounted for in either the quantification of the initiating event frequency or in the analysis of the split fraction frequency for the particular system being disabled.

The scenarios giving rise to an initiating event, while also impacting one or more of the systems required to alleviate the impact of that initiator, were further subdivided into those leading directly to core damage and those not doing so. For those that did not lead directly to core damage, we developed separate event trees to establish their importance. The event tree for the one such scenario found, a fire, is presented in Section 4 of the Plant Model Report. These spatial interaction scenarios that produced core damage without any other independent systems failure and therefore did not require an event tree for definition or quantification were included directly in the list of core damage scenarios discussed in Section 5 of this report.

The seismic analysis described in Section 2 of the Environmental and External Hazards Report comprised several steps. The objective of this task was to assess the seismicity of the site at Three Mile Island, the fragility of key buildings and equipment when exposed to earthquakes, and the possible consequences of damaging them. First, we determined annual frequency of exceedance for peak ground accelerations at the site on the basis of site-specific seismicity data. Second, for selected plant components particularly susceptible to earthquake damage, we assessed their design and design criteria; i.e., their fragility. Earthquakes can directly fail components by knocking their cabinets over, for instance, or indirectly by dropping block walls on the components. Event trees were developed to describe seismically initiated accident sequences and to determine dominant plant damage states relative to the results of the event trees of other initiating events. The seismic event trees are described in Section 4 of the Plant Model Report.

Winds can affect critical structures at the plant site in at least two ways and are discussed in Section 5 of the Environmental and External Hazards Report. If wind forces exceed the load capacity of a building or another external facility, either the walls or framing might collapse or the structure overturn from the excessive loading. If the wind is strong enough (such as in a tornado), it might be capable of lifting materials and thrusting them against some of these critical facilities. Critical components or other contents of facilities not designed to resist missile penetration might be damaged and lose their function.

The analysis of the risk from aircraft crashes into the TMI-1 plant described in Section 7 was built on analysis previously performed for GPUN as reported in Reference 4-8. The analysis of the risk from toxic chemical accidents at or near the TMI-1 plant described in Section 8 was built on analysis previously performed for GPUN as reported in Reference 4-9.

Missiles generated in the event of turbine failure can potentially damage safety-related systems. The analysis of turbine-generated missiles is described in Section 6. Although highly unlikely, serious damage to a series of pieces of critical equipment in combination with a plant trip may lead to considerable consequences.

4.5.2.7 Plant Damage States

The plant damage states developed and used in Phase II of the TMI-1 PRA are shown in Table 4-3 as a list. Although the TMI-1 PRA did not include a containment and degraded core analysis, PDSs were assigned to each scenario to make an estimate of the importance of the scenario to risk and enable future use of these scenarios with a containment model. The plant model event tree structures are profoundly affected by inclusion of plant damage scenario end states. If core damage were the only end state of importance, with no more information specified, the event tree structures would be much simpler; for instance, no containment safety features would need to appear. However, no information would be gained about the importance of the containment safety features or about the importance of any system to public health risk. Furthermore, if PDSs were not included but were needed later, the event trees would have to be drastically restructured.

As in previous PLG PRAs, the plant damage states were defined by considering the following six factors:

1. Availability of containment heat removal for preventing long-term containment overpressure failure after core damage.

2. Availability of fission product removal to reduce the containment atmosphere source term potentially available for release upon containment failure.

3. Whether the BWST water is accumulated in the containment before or shortly after reactor vessel melt-through. This is to distinguish "wet" containment sequences in which the containment atmosphere is always saturated from "dry" containment sequences in which superheating of the atmosphere and higher temperatures are possible.

4. Whether the vessel penetration takes place at high or low RCS pressure. The pressure in the RCS dictates the distribution of core melt debris following vessel penetration.

5. Whether the containment is isolated at the time of core damage. If the containment is already bypassed by, for instance, a stuck-open containment isolation valve when core damage occurs, the source term cannot be contained and an early release will occur.

6. Whether the opening in containment produces a large or a small leak path. For small leak paths, those of less than 15 square-inch equivalent orifice area, the release duration extends over several hours and would be treated as a continuous release in the offsite consequence model. For larger openings in containment like the 48-inch diameter purge valves, the relese would be treated as a "puff".

The distinction between early and late core damage has been found to not significantly impact offsite health consequences (Reference 4-10, Section 6).

4.5.2.8 Assembly of Results

The objective of this task was to put together the scenarios from the three sets of event trees and calculate the frequencies of all the scenarios for the TMI-1 PRA. By determining these frequencies, judgments were made about the relative importance of specific scenarios and systems for reducing the predicted core damage frequency.

The frequencies of all scenarios were calculated as follows. The conditional probabilities of the top events (i.e., split fractions) that were defined and estimated iteratively by the systems analysis and plant modeling were input to the various event trees, which we evaluated numerically by use of the ETC9 computer program. Results from all event tree runs were input to the MAXIMA program. MAXIMA produced (1) a list of scenarios ordered by their core damage frequency and a separate list to each plant damage state, (2) the conditional probability of going from each initiator to each plant damage states, the plant matrix described in Section 4.2, (3) the total frequency of core damage, and (4) the contribution of particular systems and plant model segmants to overall core damage.

4.6 REFERENCES

4-1. American Nuclear Society and IEEE, "PRA Procedures Guide; A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, NUREG/CR-2300, 1983.

4-2. Pickard, Lowe and Garrick, Inc., "Three Mile Island Unit 1 Probabilistic Risk Assessment, Phase I Report," prepared for GPU Nuclear Corporation, PLG-0354, April 1984.

4-3. Swain, A.D., and H.E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Sandia National Laboratories, prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-1278, SAND80-0200, August 1983.

4-4. Electric Power Research Institute, "ATWS: A Reappraisal, Part III, Frequency of Anticipated Transients," EPRI NP-2230, January 1982.

4-5. U.S. Nuclear Regulatory Commission, "Licensed Operating Reactors, Status Summary Report," NUREG-0020, Grey Book, September 1974 to February 1979.

4-6. GPU Nuclear Corporation, "TMI-1 Fire Hazard Analysis Report for Appendix R Compliance," May 11, 1982.

4-7. Code of Federal Regulations, 10CFR Parts 0 to 199, Revision of January 1, 1986, Office of the Federal Register, National Archives and Records Administration.

4-8. Pickard, Lowe and Garrick, Inc., "Updated Prediction of the Frequency of Aircraft Crashes at the Three Mile Island Unit 1 Site," PLG-0411, April 1985.

4-9. Pickard, Lowe and Garrick, Inc., "Probabilistic Risk Assessment of Offsite Releases Initiated by a Toxic Chemical Release," PLG-0370, July 1984.

4-10. Pickard, Lowe and Garrick, Inc., "Midland Probabilistic Risk Assessment," prepared for the Consumers Power Company, May 1984.

TABLE 4-1. SCENARIO TABLE IN ABSTRACT FORM

What Can Go Wrong?	Frequency	Consequences	Uncertainty
S_1	ϕ_{S_1}	$X_{S_1,t}$	$P(\phi_{S_1}, X_{S_1})$
S_2	ϕ_{S_2}	$X_{S_2,t}$	$P(\phi_{S_2}, X_{S_2})$
.	.	.	.
.	.	.	.
.	.	.	.
S_N	ϕ_{S_N}	$X_{S_N,t}$	$P(\phi_{S_N}, X_{S_N})$

NOTE: From this point forward, ϕ_{S_i} and $X_{S_i,t}$ will be expressed as ϕ_i and $X_{i,t}$.

TABLE 4-2. PINCH POINT I - TMI-1
INITIATING EVENT GROUPS

Initiator I	Initiator Group
1	Large LOCA
2	Medium LOCA
3	Small LOCA
4	Very Small LOCA
5	Inadvertent Opening of DHR Valves
6	Steam Line Break in Intermediate Building
7	Steam Line Break in Turbine Building
8	Steam Generator Tube Rupture
9	Excessive Feedwater Flow
10	Total Loss of Main Feedwater
11	Reactor Trip
12	Turbine Trip
13	Loss of Air System
14	Loss of Control Building Ventilation
15	Loss of ATA Power (ICS)
16	Loss of DC Power Train A
17	Loss of Offsite Power
18	Loss of Nuclear Services Closed Cooling Water
19	Loss of River Water

TABLE 4-3. PINCH POINT II - TMI-1 PLANT DAMAGE STATES

Plant Damage State J	Abbreviation	Description of Conditions at Time of Core Damage				
		RWST Injection Relative to Reactor Vessel Melt-Through	RCS Pressure at Melt-Through	Reactor Building Integrity at Core Melt Initiation	Reactor Building Fission Product Removal	Reactor Building Heat Removal
1	1A	Never	Low	Yes	Yes	Yes
2	1C	Never	Low	Yes	No	No
3	1D	Never	Low	Small	Yes	Yes
4	1F	Never	Low	Small	No	No
5	1H	Never	Low	Large	No	--
6	2A	Before	Low	Yes	Yes	Yes
7	2B	Before	Low	Yes	Yes	No
8	2C	Before	Low	Yes	No	No
9	2D	Before	Low	Small	Yes	Yes
10	2E	Before	Low	Small	Yes	No
11	2F	Before	Low	Small	No	No
12	2G	Before	Low	Large	Yes	--
13	2H	Before	Low	Large	No	--
14	3A	Never	High	Yes	Yes	Yes
15	3C	Never	High	Yes	No	No
16	3D	Never	High	Small	Yes	Yes
17	3F	Never	High	Small	No	No
18	3H	Never	High	Large	No	--
19	4A	After	High	Yes	Yes	Yes
20	4B	After	High	Yes	Yes	No
21	4C	After	High	Yes	No	No
22	4D	After	High	Small	Yes	Yes
23	4E	After	High	Small	Yes	No
24	4F	After	High	Small	No	No
25	4G	After	High	Large	Yes	--
26	4H	After	High	Large	No	--
27	5A	Before	High	Yes	Yes	Yes
28	5B	Before	High	Yes	Yes	No
29	5C	Before	High	Yes	No	No
30	5D	Before	High	Small	Yes	Yes
31	5E	Before	High	Small	Yes	No
32	5F	Before	High	Small	No	No
33	5G	Before	High	Large	Yes	--
34	5H	Before	High	Large	No	--

Legend:

"--" indicates that heat removal takes place through the large hole in the reactor building.

High RCS pressure at melt-through means > 400 psig; low pressure means < 400 psig.

"Large" means hole of > 15 square-inch equivalent orifice area produced only by leaving the containment purge valve(s) open; "small" means a hole < 15 square inches produced by leaving any other penetration or combination of penetrations unisolated; "yes" means the containment is intact.

TABLE 4-4. PINCH POINT III - EXAMPLE RELEASE CATEGORIES

Release Category K	Description of Release Conditions
1	Steam Explosion with Containment Spray
2	Steam Explosion without Containment Spray
3	Early Overpressure with Containment Spray
4	Early Overpressure without Containment Spray
5	Delayed Overpressure with Containment Spray
6	Delayed Overpressure without Containment Spray
7	Basemat Melt-Through with Containment Spray
8	Basemat Melt-Through without Containment Spray
9	Containment Intact with Containment Spray
10	Containment Intact without Containment Spray

TABLE 4-5. PINCH POINT IV - EXAMPLE DAMAGE TYPES

Damage Type L	Description
1	Acute Fatalities
2	Injuries
3	Thyroid Cancer Cases
4	Cancer Fatalities (other than thyroid)
5	Whole Body Man-Rem Exposure

TABLE 4-6. SYSTEMS ANALYZED

1. Electric Power System
2. Engineered Safeguards Actuation System
3. Nuclear Services River Water and Closed Cooling Water Systems
4. Decay Heat River Water and Closed Cooling Water Systems
5. Control Building Ventilation System
6. Reactor Protection System
7. Turbine Trip System
8. Main Steam System
9. Main Feedwater and Integrated Control Systems
10. Emergency Feedwater System
11. Pressure Control System
12. High Pressure Injection System
13. Low Pressure Injection/Decay Heat Removal System
14. Reactor Building Isolation System
15. Reactor Building Emergency Cooling System
16. Reactor Building Spray System
17. Instrument Air System

TABLE 4-6. SYSTEMS ANALYZED

1. Electric Power System
2. Engineered Safeguards Actuation System
3. Nuclear Services River Water and Closed Cooling Water Systems
4. Decay Heat River Water and Closed Cooling Water Systems
5. Control Building Ventilation System
6. Reactor Protection System
7. Turbine Trip System
8. Main Steam System
9. Main Feedwater and Integrated Control Systems
10. Emergency Feedwater System
11. Pressure Control System
12. High Pressure Injection System
13. Low Pressure Injection/Decay Heat Removal System
14. Reactor Building Isolation System
15. Reactor Building Emergency Cooling System
16. Reactor Building Spray System
17. Instrument Air System

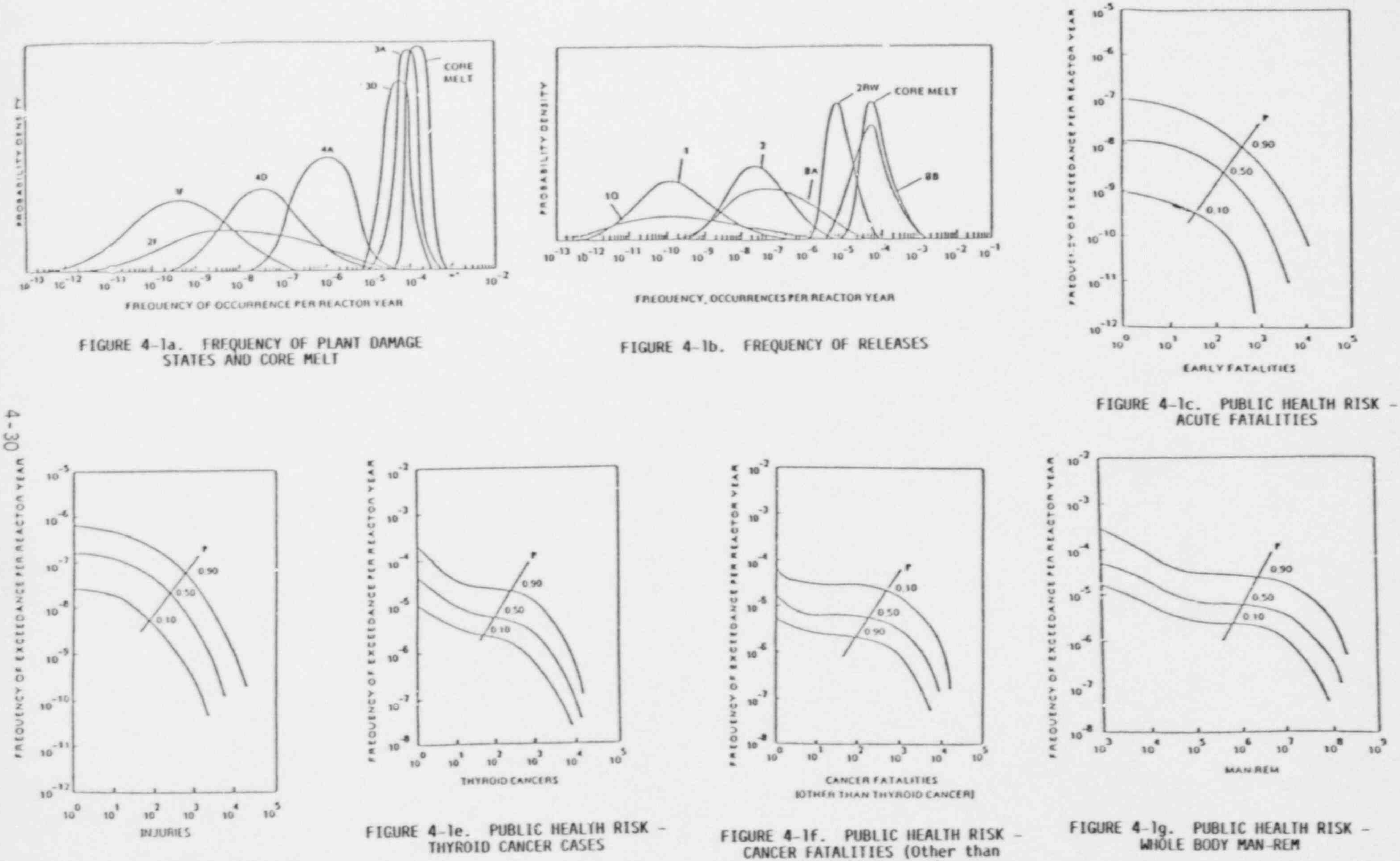


FIGURE 4-1a. FREQUENCY OF PLANT DAMAGE STATES AND CORE MELT

FIGURE 4-1b. FREQUENCY OF RELEASES

FIGURE 4-1c. PUBLIC HEALTH RISK - ACUTE FATALITIES

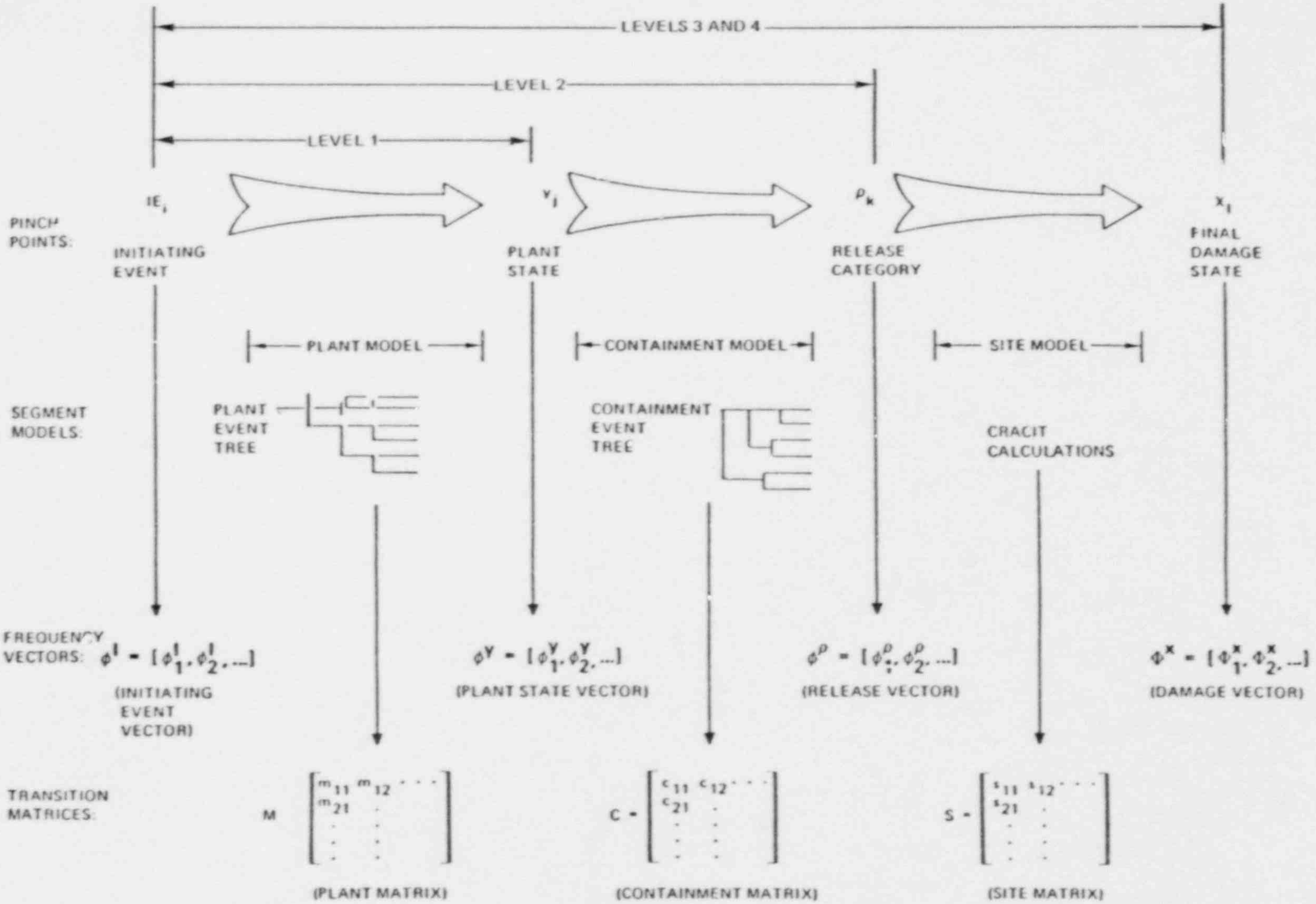
FIGURE 4-1d. PUBLIC HEALTH RISK - INJURIES

FIGURE 4-1e. PUBLIC HEALTH RISK - THYROID CANCER CASES

FIGURE 4-1f. PUBLIC HEALTH RISK - CANCER FATALITIES (Other than Thyroid Cancers)

FIGURE 4-1g. PUBLIC HEALTH RISK - WHOLE BODY MAN-REM

FIGURE 4-1. REPRESENTATIVE NUMERICAL RESULTS FROM A PRA


LEVELS 3 AND 4
LEVEL 2
LEVEL 1
PINCH POINTS:
IE_i
INITIATING EVENT
Y_j
PLANT STATE
ρ_k
RELEASE CATEGORY
X_l
FINAL DAMAGE STATE
PLANT MODEL
CONTAINMENT MODEL
SITE MODEL
SEGMENT MODELS:
PLANT EVENT TREE
CONTAINMENT EVENT TREE
CRACIT CALCULATIONS
FREQUENCY VECTORS:
$\phi^I = [\phi^I_1, \phi^I_2, \ldots]$
(INITIATING EVENT VECTOR)
$\phi^Y = [\phi^Y_1, \phi^Y_2, \ldots]$
(PLANT STATE VECTOR)
$\phi^\rho = [\phi^\rho_1, \phi^\rho_2, \ldots]$
(RELEASE VECTOR)
$\Phi^X = [\Phi^X_1, \Phi^X_2, \ldots]$
(DAMAGE VECTOR)
TRANSITION MATRICES:
$M \begin{bmatrix} m_{11} & m_{12} & \cdots \\ m_{21} & \cdot & \\ \vdots & \vdots & \end{bmatrix}$
(PLANT MATRIX)
$C = \begin{bmatrix} c_{11} & c_{12} & \cdots \\ c_{21} & \cdot & \\ \vdots & \vdots & \end{bmatrix}$
(CONTAINMENT MATRIX)
$S = \begin{bmatrix} s_{11} & s_{12} & \cdots \\ s_{21} & \cdot & \\ \vdots & \vdots & \end{bmatrix}$
(SITE MATRIX)

ASSEMBLY PROCESS:

$\phi^Y = \phi^I M$

$\phi^\rho = \phi^Y C = \phi^I MC$

$\Phi^X = \phi^\rho S = \phi^Y CS = \phi^I MCS$

FIGURE 4-2. OVERVIEW OF THE ASSEMBLY PROCESS, SHOWING RELATIONSHIPS OF PINCH POINTS, EVENT TREES, FREQUENCY VECTORS, AND TRANSITION MATRICES

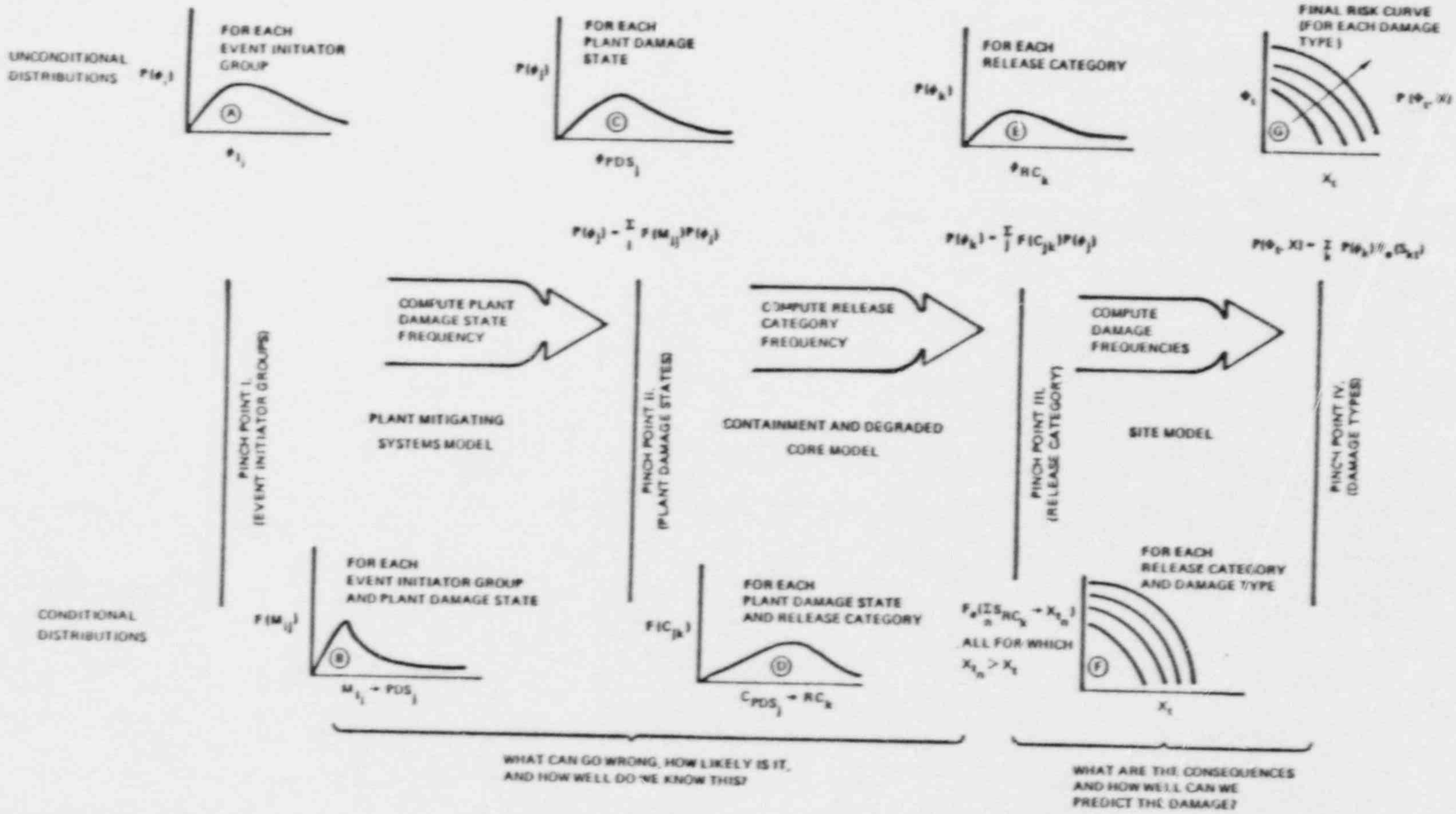

UNCONDITIONAL DISTRIBUTIONS
$P(\phi_I)$
FOR EACH EVENT INITIATOR GROUP
A
ϕ_{I_i}
FOR EACH PLANT DAMAGE STATE
$P(\phi_j)$
C
ϕ_{PDS_j}
FOR EACH RELEASE CATEGORY
$P(\phi_k)$
E
ϕ_{RC_k}
FINAL RISK CURVE (FOR EACH DAMAGE TYPE)
ϕ_t
G
$P(\phi_t, X)$
X_t
$P(\phi_j) = \sum_i F(M_{ij}) P(\phi_i)$
$P(\phi_k) = \sum_j F(C_{jk}) P(\phi_j)$
$P(\phi_t, X) = \sum_k P(\phi_k) ///_\phi (S_{kt})$
PINCH POINT I. (EVENT INITIATOR GROUPS)
COMPUTE PLANT DAMAGE STATE FREQUENCY
PLANT MITIGATING SYSTEMS MODEL
PINCH POINT II. (PLANT DAMAGE STATES)
COMPUTE RELEASE CATEGORY FREQUENCY
CONTAINMENT AND DEGRADED CORE MODEL
PINCH POINT III. (RELEASE CATEGORY)
COMPUTE DAMAGE FREQUENCIES
SITE MODEL
PINCH POINT IV. (DAMAGE TYPES)
CONDITIONAL DISTRIBUTIONS
$F(M_{ij})$
FOR EACH EVENT INITIATOR GROUP AND PLANT DAMAGE STATE
B
$M_{I_i} \rightarrow PDS_j$
$F(C_{jk})$
FOR EACH PLANT DAMAGE STATE AND RELEASE CATEGORY
D
$C_{PDS_j} \rightarrow RC_k$
$F_\phi(\sum_n S_{RC_k} \rightarrow X_{t_n})$
ALL FOR WHICH
$X_{t_n} > X_t$
FOR EACH RELEASE CATEGORY AND DAMAGE TYPE
F
X_t
WHAT CAN GO WRONG, HOW LIKELY IS IT, AND HOW WELL DO WE KNOW THIS?
WHAT ARE THE CONSEQUENCES AND HOW WELL CAN WE PREDICT THE DAMAGE?

FIGURE 4-3. RISK ASSESSMENT PROCESS

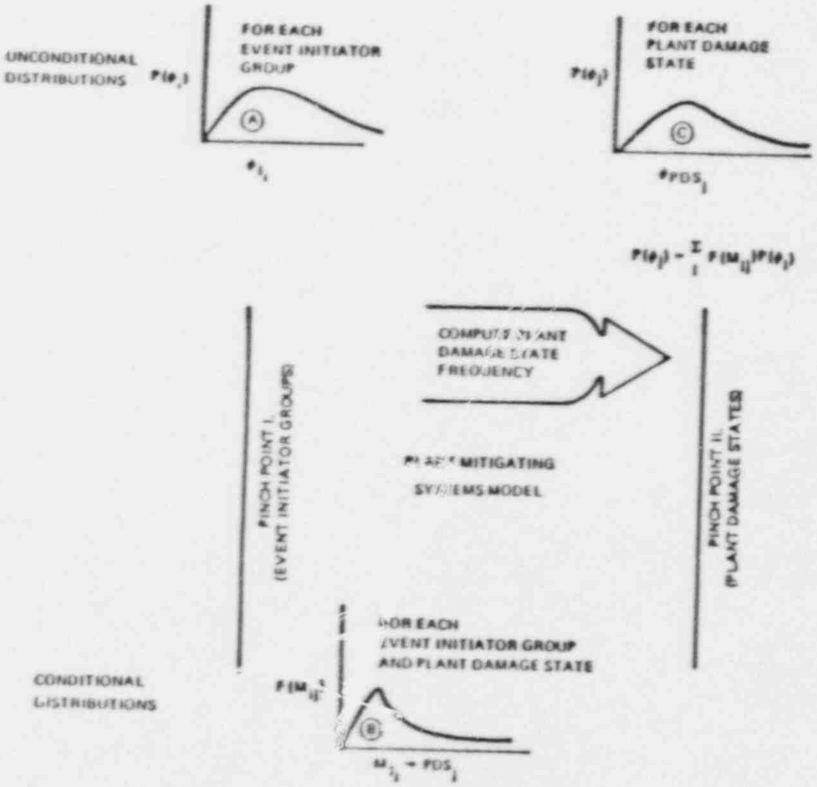

UNCONDITIONAL DISTRIBUTIONS
$P(\phi_i)$
FOR EACH EVENT INITIATOR GROUP
Ⓐ
ϕ_{I_i}
$P(\phi_j)$
FOR EACH PLANT DAMAGE STATE
Ⓒ
ϕ_{PDS_j}
$P(\phi_j) = \sum_i P(M_{ij})P(\phi_i)$
COMPUTE PLANT DAMAGE STATE FREQUENCY
PINCH POINT I. (EVENT INITIATOR GROUPS)
PLANT MITIGATING SYSTEMS MODEL
PINCH POINT II. (PLANT DAMAGE STATES)
CONDITIONAL DISTRIBUTIONS
$P(M_{ij})$
FOR EACH EVENT INITIATOR GROUP AND PLANT DAMAGE STATE
Ⓑ
$M_{ij} \rightarrow PDS_j$

FIGURE 4-4. RISK ASSESSMENT PROCESS SPECIFIC TO THE TMI-1 PRA

5. SUMMARY OF RESULTS

Section 4.1 described how the risk from operating TMI-1 could be characterized by a set of risk curves, as shown in Figures 4-1 and 4-4. The assembly process for TPRA consisted of using unconditional initiating event frequency curves like curve A in Figure 4-4 and combining them with conditional scenario frequency curves like curve B to produce unconditional plant damage state frequency curves like curve C.

This section summarizes the results of the PRA by first showing the core damage frequency curve and then working backward to unravel the contributors to this curve (more detailed results are presented in Section 6 of the Plant Model Report). The contributors to be examined first will be the initiating event groups (Section 5.2), which are pinch point I in Figure 4-4. Next, these results will be unraveled further in Section 5.3 to examine the scenarios contributing to core damage frequency. In Section 5.4, the scenarios will be summed down the event tree top events to find the most important systems. Finally, each of these important systems will be further unraveled in Section 5.5 to identify the most important component failures contributing to the unavailability of each important system. Operator-initiated system actions are described in Section 5.6.

All of the sequences described in this section contribute signficantly to the core damage frequency, but they would not all necessarily contribute significantly to the public health risk of operating TMI-1. All core damage scenarios contribute to the economic risk to GPUN of operating TMI-1, but some do not contribute to the risk of offsite consequences. Some information about the contribution of each scenario to public health risk may be gleaned from the plant damage state of the scenario. Plant damage states are discussed in Section 5 of the Plant Model Report.

5.1 CORE DAMAGE FREQUENCY

Figures 5-1 and 5-2 present the probability of frequency curve for core damage. This is one of the key results of the TPRA. The frequency of core damage represents the likelihood that some scenarios could get sufficiently out of control to damage the core.

The core damage frequency curve is presented in probability of frequency format. This format was used to express our state of knowledge about this frequency. As explained in Section 4.4, each parameter involved in the calculation of the core damage frequency has uncertainty associated with it. All of the uncertainties that went into calculating the frequency of each scenario were combined to calculate a frequency distribution for the scenario. Then, the probability of frequency distribution for each scenario was combined to calculate the uncertainty associated with the core damage frequency.

Figures 5-1 and 5-2 divide the core damage frequency into broad categories according to the source of the initiating event. The "total externals" curve represents the contribution from all externally initiated scenarios and the "total internals" from all internally initiated scenarios. The "total" curves represent the sum of these two.

The probability of core damage frequency curves in Figure 5-1 expresses uncertainty using the cumulative frequency format. Figure 5-2 expresses the same information in the probability density format. These figures both say that the TMI-1 PRA team is 95% confident that the total core damage frequency from all sources (both internal and external; see next section) is no more than 9.4×10^{-4} and 95% confident that it is really greater than 2.6×10^{-4}. These figures also indicate that our best estimate of the core damage frequency, the median (or 50th percentile), is 4.5×10^{-4}. The mean of the total core damage frequency distribution is $5.5 \times 1C^{-4}$.

The greater range between the 5th and 95th percentile values "total external" curve in Figures 5-1 and 5-2 indicates the greater uncertainty in calculating the frequency of externally initiated scenarios compared to that involved with calculating the frequency of the internally initiated scenarios. The span is about an order of magnitude for the externals as compared to about half that for the internals.

The point estimate mean value shown in Figure 5-1, 5.5×10^{-4}, has a special significance to the results presented for this study. This mean value is the product of the means of the system reliability and initiating event frequencies used for choosing the most important scenarios. Most results presented in the first three volumes of this study are presented in terms of products of means, and their contribution or importance is compared to 5.5×10^{-4}. The most important use of the product of the means was in determining which scenarios were sufficiently important to have their own mean and distribution calculated. The most important scenarios were chosen from the event tree calculations using mean values for the split fractions. The split fraction mean values were used for screening because they are single values that characterize the shape of the probability of frequency distribution and therefore help ensure that the correct "important" scenarios were chosen.

5.2 INITIATING EVENTS CONTRIBUTING TO CORE DAMAGE FREQUENCY

This section discusses the initiating events that contributed the highest frequency scenarios to the total probability of core damage frequency curve presented in Figures 5-1 and 5-2. All of the initiating event groups used in the TPRA are shown in Table 5-1. Table 5-2 shows the contribution of the initiating events in Table 5-1 grouped according to whether they originate within, internal, or outside the plant systems, external. All the internal initiating events contribute 81% of the core damage frequency, while the external contribute 19%. Most of the contributions (16%) from external events come from the six fires listed in Table 5-1. The calculation of the fire and other external event frequencies is presented in the Environmental and External Hazards Report. One fire, F04, and the four earthquakes, E15, E25, E40, and E60, were analysed using event trees as described in the Plant Model Report. As seen in Table 5-1, core damage results 36% of the time from scenarios initiated by loss of control building ventilation, 7% of the time from steam generator tube rupture, 6% of the time from fires in the auxiliary building MCC area (AB-FZ-6) and 5% of the time from loss of offsite power, 4% of the time from reactor trip, fires in switchgear room 1S (CB-FA-2b), fires in the ESAS cabinet area (CB-FA-3c), loss of instrument air, medium LOCA, and excessive main feedwater and very small break LOCA. No other initiators contribute more than 3%.

The fire-initiating events listed in Table 5-1, except for the fire in the 1D switchgear room (CB-FA-3a, hazard scenario 2), lead directly to core damage because none of the alleviating systems that are still available after the fire can prevent core damage. In most of these fires, loss of the RCP seal cooling and unavailability of the high pressure injection pumps produces core damage. The core uncovers because the RCP seals fail and water is then lost through the seals. There is no way to replace the lost reactor coolant since the high pressure injection pumps do not work. It will not happen right away, but core damage is inevitable unless either power is recovered to the HPI pumps or, in fact, the seals somehow remain intact.

In all of these fires, power or control cables are burnt in low probability fires of higher intensity than those for which 10CFR50, Appendix R (Reference 5-1) protection was designed. The frequency of such fires is very low, but the possible impact on the plant is so great that they became important risk contributors. The fire in the control building 1D switchgear room (CB-FA-3a), hazard scenario 2 shown in Table 5-1 required an additional nonfire-related failure to produce core damage and did not produce any important scenarios. Therefore, this initiating event contributed relatively little to the total core damage frequency (<1%).

5.3 SCENARIOS CONTRIBUTING TO CORE DAMAGE FREQUENCY

This section discusses the plant model scenarios which dominate the total frequency of core damage curve presented in Figure 5-1. As listed in Table 5-3, the core damage scenario with the highest frequency (33%) is one initiated by loss of control building ventilation. The next three highest frequency scenarios at 6%, 4%, and 4%, respectively, are fires in three different areas of the plant. The first one is in the auxiliary building and the next two are in two different areas of the control building. The next highest frequency scenario at 2.4% is a medium LOCA scenario in which the operator fails to establish recirculation flow from the reactor building sump. The next scenario at 2% is initiated by excessive main feedwater, which actuates high pressure injection. The operator fails to reestablish minimum-flow recirculation when he throttles the HPI flow, which fails the operating high pressure injection pumps. Then, the RCP seal cooling fails independently. Failure of seal injection from the HPI pumps and of seal cooling together result in extensive leakage from the RCP seals. The seventh scenario at 2% is another fire, this one in the 1E switchgear room in the control building. The next scenario at 1% also is a seal LOCA but initiated by a loss of air with subsequent failure of the seal injection valves and of seal cooling. The eighth most frequent scenario is like the fifth, a failure of sump recirculation, but, in this case, following a large instead of a medium LOCA. The next 3 scenarios and the 14th, all at about 1% each, result in core damage because of failures of decay heat removal either by failing the DHR system itself or by failing the decay heat cooling water system or combinations of one train of each. All other scenarios contribute less than 1% each. These scenarios are the first of an almost continuous series of scenarios. In fact, in this continuum of scenarios closely spaced in frequency, the first 10 contain only 55% and the first 100 only 74% of the total likelihood of core damage.

Based on the scenarios shown in Table 5-3 with "*" and "**," approximately 54% of the core damage frequency involves scenarios in which reactor coolant is being lost through the reactor coolant pump seals because neither seal cooling from the intermediate closed cooling water system nor seal injection is available from the makeup system. In addition, this loss of reactor coolant cannot be properly alleviated since high pressure injection is also unavailable. In some of these cases, long-term decay heat removal is also not available (those marked with "*"). The loss of inventory through the seals dictates the time available for recovering support systems that are lost. If seal cooling and injection failures did not lead to large losses of RCS coolant, as assumed in this PRA, then the TMI-1 core damage frequency would be only 4.5×10^{-4} instead of 5.5×10^{-4} in the "**" cases and, in the "*" cases, the likelihood of recovering DHR capability would be higher.

Another interesting conclusion from looking down the list of scenarios is that 42% of the core damage frequency comes from scenarios in which long-term core heat removal/inventory control is involved. Failures in sump recirculation and decay heat removal are included in this group. This means that core uncovery would take a relatively long time to occur; therefore, more time is available to fix damaged systems. Some advantage has already been taken of these enhanced repair and recovery opportunities in this PRA. LOCAs (other than seal LOCAs) with failure of the HPI are not important contributors in this plant.

5.4 PLANT SYSTEMS CONTRIBUTING TO CORE DAMAGE FREQUENCY

This section discusses the plant systems that are most important to the total frequency of core damage curve presented in Figure 5-1. The scenarios in Table 5-3 were further decomposed to find the system action failures that dominate the frequency of severe core damage; these syste action failures are shown in Table 5-4. The systems in Table 5-4 are indicated by underlined uppercase letters that correspond to individual systems analyses in the Systems Analysis Report. The appropriate section numbers are indicated in this table. Under each systems analysis heading, the actions that each system performs are grouped by categories that correspond to the event tree top events. Under each category title indicated by a bullet ("o") are specific system actions or events initiated by failures with the system. (These specific system actions are referred to above as split fractions in Section 4.) The first numerical column to the right of the titles is the decomposition of the total core damage frequency into contributors. This decomposition is made by adding the frequency of all scenarios in which each system failure occurs. The total percentage of all contributing systems may exceed 100% because more than one system failure may occur in each core damage scenario.* Such a "vertical cut" measures the cumulative effect of many low frequency scenarios that, due to their large number, would be prohibitive to examine individually.

The second column to the right in Table 5-4 represents the system contribution that comes from each system action category. The numbers in the second column in square brackets ("[ ]") indicate the contributions from split fractions other than 0.0 or 1.0. The numbers in curly braces, "{ }" indicate the contribution of scenarios that have both of two redundant trains failed (the so-called "cross terms"). The contribution from these two train failure cases have been subtracted from the total system contribution in the first numerical column because, otherwise, the system actions would be double counted when compared to an action that contains both trains. The third column represents the fraction of the system action category contribution that comes from each specific action.

When failures that initiate events, as well as those that alleviate the consequences of initiating events, are considered, the control building ventilation system at 43% is seen to be very important. Most of the scenarios that lead to core damage and have CBVS failures (98%) are initiated by loss of control building ventilation.

Failures of the decay heat removal system appears in scenarios sustaining 37% of the core damage frequency. Failure of this system is important because it is necessary for the long-term success of core heat removal through either open (sump) or closed loop recirculation. Recirculation from the reactor building sump is an important part of this system. This system also contains low pressure injection actions. The decay heat cooling water system that cools the DHR heat exchangers is also important figuring in 21% of the core damage scenarios.

The high pressure injection system also figures in scenarios with 37% of the core damage frequency. As can be seen by the square bracket terms, however, the HPI system is usually important not because of failures within itself but because support system failures make it unavailable. The important exceptions to this are the throttling and minimum-flow recirculation system action categories.

*The importance percentage calculated in this way usually indicates the percentage reduction in core damage frequency that would result if the system were made perfect; i.e., unable to fail. For instance, if system A (which contributes to 10% of the core damage frequency) were made perfect, the total core damage frequency would be reduced by 10%. An exception to this rule is for cases for which the system does not contribute to core damage but merely to the PDS damage state in which the scenario appears. Fixing a containment safety feature will not reduce core damage frequency; therefore, when such a system is made perfect, the frequency of one PDS is decreased, while that of another is increased by the same amount, leaving total core damage frequency unchanged. Another exception is when there are two systems failed in the scenario, either one of which would in itself lead to core damage. Fixing one such system would reduce the frequency of the scenario with the pair of failures and increase the frequency of the scenario containing failure of the unfixed system.

Electric power systems failures account for 24% of the core damage frequency. These include all of the AC and DC power and offsite power systems that are important to accident initiation or alleviation.

Main steam and feedwater system failures, although they do not lead directly to core damage, occur in scenarios that have 23% of the core damage frequency.

RCS pressure control system failures appear in about 22% of the core damage frequency. These are system actions to open and close RCS relief valves and to use the RCS sprays to depressurize the RCS during cooldown. Again, only failure of the cooldown actions would lead directly to core damage, but the other pressure control system failures, if eliminated, would reduce the core damage frequency.

No other systems contribute to in more than 10% of the core damage frequency.

5.5 SYSTEM COMPONENT FAILURES CONTRIBUTING TO CORE DAMAGE FREQUENCY

The most important of the system action categories in Table 5-4 were further decomposed to show the most important specific system actions that contributed to each category and the system component failures that contribute to the failure of each specific action. This further decomposition is shown in Table 5-5. Each page of Table 5-5 contains the most important of the action categories as they appeared in Table 5-4 for a particular system. Use Table 5-4 as a guide for plowing through the more extensive and complicated Table 5-5.

The left-hand three columns in Table 5-5 are the same as those in Table 5-4. The three right-hand numerical columns are different. The first numerical column in Table 5-5 is the same as the second one in Table 5-4. It is the system action category (top event) contribution to core damage frequency. The second column in Table 5-5 is the same as the third in Table 5-4, it is the fraction of the total contribution to the category from each specific system action (split fraction). The third right-hand column in Table 5-5 is the fraction of each system action failure that is caused by a particular component or set of components (blocks in the reliability block diagram for the system). Only the most important component failures are shown, not all of them. Extreme caution should be used if one is tempted to multiply these three columns together, but they do give some idea of which components to work on to reduce the core damage frequency. This table also indicates the contribution from initiating events and the cases in which the system unavailability was dictated by dependence on support system or other preceding failures instead of failures within the system itself. Such cases are indicated by specific system actions that are labeled "guaranteed failure." An example of this is DHR system specific action SA-1.0 (SAE). The number in the second column to the right of SA-1.0, 8%, indicates that 8% of the 15% contribution to the SA system action category or about 1% of the 15% is not due to failure of the sump or operator, but due to dependence on the failure of some preceding system.

No attempt has been made to sum across components of a particular type except for operator actions. The operator actions extracted from Table 5-5 are discussed in the next section.

5.6 OPERATOR ACTIONS CONTRIBUTING TO CORE DAMAGE FREQUENCY

Many operator actions are important in the TMI-1 PRA, and contribute significantly to reducing the calculated core damage frequency. However, the failure of the operators to successfully perform certain actions contributes to core damage in some of the scenarios. Table 5-6 summarizes the contribution of the most important of the operator actions to core damage frequency. The actions in Table 5-6 are grouped into three categories:

- Operator Restoration and Recovery Actions
- Manual Actions To Actuate Systems
- Manual Backups To Automatic Actions

Inclusion in these categories is somewhat arbitrary; some actions might logically fit into two categories, but have only been put into one. All of the operator actions in Table 5-5 were put into one of these three categories. These actions included those from recovery (RE) top events, from initiating events that had operator actions to prevent the plant tripping, and from systems analyses, but no maintenance contribution was included. The numbers in the second right-hand column have had the specific system action contribution to core damage frequency multiplied by the fraction of that failure that was estimated to be attributable to the operator. All such products were summed to get the number in the first right-hand column; then, the first right-hand column was divided into each specific action contribution to get the fractions in the second column. Table 5-6 had to be prepared at the level of specific operator actions because only at this level could the operator's contribution be calculated. No generalities could be made about his contribution across all operator actions in any particular action category.

The most important category of operator actions were those classified as restoration and recovery (38%). By far the most important action of these was what the operator did after losing the control building fans or chillers to restore ventilation before plant trip (58% of the 38%).

The next most important category comprised the manual actions to actuate systems (12%). In this category, the operator was almost equally important to reestablishing minimum-flow recirculation after throttling HPI flow (47% of 12%) and switching low pressure pump suction from the BWST to the sump following a large LOCA (39% of 12%).

The last category, manual backup to automatic actuations, was less important at 8% and contained no single important action that contributed more than 25% of this 8%.

5.7. REFERENCES

5-1. Code of Federal Regulations, 10CFR Parts 0 to 199, Revision of January 1, 1986, Office of the Federal Register, National Archives and Records Administration.

TABLE 5-1. INITIATING EVENT CONTRIBUTIONS TO CORE DAMAGE FREQUENCY

Sheet 1 of 2

Abbreviation	Description	Contribution to Severe Core Damage Frequency, Percent of 5.5×10^{-4}	Mean Frequency per Reactor Year
LC	Loss of Control Building Ventilation	36.4	2.00×10^{-4}
TR	Steam Generator Tube Rupture	7.0	3.84×10^{-5}
F01	Fire in Auxiliary Building MCC Area (AB-FZ-6, hazard [illegible] 1)	5.5	3.00×10^{-5}
AC	Loss of Offsite Power	5.3	2.90×10^{-5}
RT	Reactor Trip	3.8	2.10×10^{-5}
F02	Fire in Control Building Switchgear Room 1S (CB-FA-2b; hazard scenario 1a)	3.6	2.00×10^{-5}
F06	Fire in Control Building ESAS Cabinet Area (CB-FA-3c; hazard scenario 1)	3.6	2.00×10^{-5}
LA	Loss of Instrument Air	3.6	1.98×10^{-5}
ML	Medium LOCA	3.6	1.97×10^{-5}
EXC	Excessive Main Feedwater	3.3	1.80×10^{-5}
VSB	Very Small LOCA	3.2	1.74×10^{-5}
LR	Loss of River Water to the Pump House	2.9	1.58×10^{-5}
TT	Turbine Trip	2.4	1.28×10^{-5}
ATA	Loss of ATA Power	2.3	1.22×10^{-5}
F05	Fire in Control Building Switchgear Room 1E (CB-FA-3b; hazard scenario 1)	1.8	1.00×10^{-5}
	All Other Fires and Floods	< 2.0	$< 1.00 \times 10^{-5}$
LD	Loss of One Train of DC Power	1.8	9.80×10^{-6}
LL	Large LOCA	1.6	8.84×10^{-6}
SB	Small LOCA	1.4	7.27×10^{-6}
	Large External Floods	1.4	7.50×10^{-6}
SLI	Steam or Feedwater Line Breaks in the Turbine or Intermediate Building	1.1	6.32×10^{-6}
F03	Fire in Control Building Battery Room B (CB-FA-2d; hazard scenario 1)	1.0	5.00×10^{-6}
LNS	Loss of Nuclear Services Cooling Water	0.7	3.54×10^{-6}
F04	Fire in Control Building Switchgear Room 1D (CB-FA-3a; hazard scenario 2)	0.3	1.36×10^{-6}
FW	Total Loss of Main Feedwater	0.6	3.16×10^{-6}
E60	0.6g Earthquake	0.5	2.48×10^{-6}

TABLE 5-1 (continued)

Sheet 2 of 2

Abbre-viation	Description	Contribution to Severe Core Damage Frequency, Percent of 5.5×10^{-4}	Mean Frequency per Reactor Year
E25	[illegible] quake	< 0.1	1.22×10^{-7}
VS	[illegible] Opening of the DHR solation Valves	< 0.1	1.00×10^{-7}
E40	[illegible] nquake	< 0.1	7.52×10^{-8}
E15	0.15g Earthquake	< 0.1	2.76×10^{-8}

TABLE 5-2. INITIATING EVENT CATEGORIES CONTRIBUTING SIGNIFICANTLY TO CORE DAMAGE FREQUENCY

Description	Contribution, Percent of 5.5 x 10^{-4}	Mean Frequency per Reactor Year
INTERNAL	80.6	4.43 x 10^{-4}
Loss of Support Systems:	52.8	
Loss of CBV	36.4	2.00 x 10^{-4}
Others	8.2	4.53 x 10^{-5}
Loss of Offsite Power*	5.3	2.90 x 10^{-5}
Loss of River Water to Pumphouse	2.9	1.58 x 10^{-5}
All Other Transients	11.1	6.09 x 10^{-5}
Very Small LOCAs (including steam generator tube rupture)	10.1	5.58 x 10^{-5}
All Larger LOCAs	6.5	3.58 x 10^{-5}
LOCA outside Containment	< 0.1	1.00 x 10^{-7}
EXTERNAL	19.4	1.07 x 10^{-4}
Fires Explicitly Modeled**	15.7	8.64 x 10^{-5}
All Other Fires and All Internal Floods	< 2	< 1.00 x 10^{-5}
Earthquakes	0.5	2.70 x 10^{-6}
External Flood	1.4	7.5 x 10^{-6}
Tornado	<< 0.1	1.2 x 10^{-8}
Turbine Missile	< 0.1	2.3 x 10^{-7}
Aircraft Crash	< 0.1	1.0 x 10^{-7}
Toxic Chemical	< 0.1	2.6 x 10^{-7}

*Loss of offsite power could also be included in the external category.
**Fires, though internal to the plant, are usually categorized as external events.

TABLE 5-3. SCENARIOS CONTRIBUTING SIGNIFICANTLY TO CORE DAMAGE FREQUENCY

Sheet 1 of 4

Order Number	Description	RCP Seal Fail-ure	Contribution to Severe Core Damage Frequency, Percent of 5.5 x 10-4	Mean Frequency per Reactor Year
1	Loss of control building ventilation and failure to establish alternate room cooling.	*	33.3	1.83×10^{-4}
2	Fire in auxiliary building MCC area (AB-FZ-6; hazard scenario 1).	**	5.5	3.00×10^{-5}
3	Fire in control building switchgear room 1S (CB-FA-2b; hazard scenario 1a).	**	3.6	2.00×10^{-5}
4	Fire in control building ESAS cabinet area (CB-FA-3c; hazard scenario 1), and the operator fails to use the alternative shutdown system correctly.	**	3.6	2.00×10^{-5}
5	Medium LOCA and failure to establish sump recirculation.		2.4	1.30×10^{-5}
6	Excessive main feedwater, leading to HPI actuation; failure to provide HPI minimum-flow recirculation after HPI flow throttling, leading to HPI pump failure; and failure of RCP seal cooling leading to seal LOCA with no HPI available.	**	1.9	1.02×10^{-5}
7	Fire in control building 1E switchgear room (CB-FA-3b; hazard scenario 1).	**	1.8	1.00×10^{-5}

*Long-term DHR heat removal is also unavailable.
**Seal cooling and injection are both failed.

TABLE 5-3 (continued)

Sheet 2 of 4

Order Number	Description	RCP Seal Fail-ure	Contribution to Severe Core Damage Frequency, Percent of 5.5 x 10-4	Mean Frequency per Reactor Year
8	Loss of air; failure of RCP seal injection and cooling.	**	1.1	6.26×10^{-6}
9	Large LOCA and failure to establish sump recirculation.		1.1	5.95×10^{-6}
10	Steam generator tube rupture and failure of one train of decay heat removal and the opposite train of decay heat cooling water, leading to loss of long-term decay heat removal capability.		1.1	5.88×10^{-6}
11	Very small LOCA and failure of both trains of decay heat cooling water, leading to loss of long-term decay heat removal capability.		1.1	5.78×10^{-6}
12	Steam generator tube rupture and one train of electric power leading to failure to cool down RCS and stop RCS inventory loss so that recirculation is not needed.		1.0	5.36×10^{-6}
13	Fire in control building battery room B (CB-FA-2d; hazard scenario 1), leading to seal LOCA with no HPI.	**	1.0	5.00×10^{-6}

*Long-term DHR heat removal is also unavailable.
**Seal cooling and injection are both failed.

TABLE 5-3 (continued)

Sheet 3 of 4

Order Number	Description	RCP Seal Fail-ure	Contribution to Severe Core Damage Frequency, Percent of 5.5 x 10-4	Mean Frequency per Reactor Year
14	Very small continued loss of RCS inventory, failure of one train of decay heat cooling, and failure to align other train of decay heat removal.		0.7	3.90×10^{-6}
15	Loss of river water; loss of EFW, thus reducing available recovery time; and failure to recover river water prior to core damage.	*	0.7	3.90×10^{-6}
16	Loss of river water with EFW available and failure to recover river water, even with more time available.	*	0.6	3.51×10^{-6}
17	Steam generator tube rupture and failure of decay heat removal.		0.6	3.21×10^{-6}
18	Steam generator tube rupture and failure of the necessary closed-loop recirculation because there is no water in the sump.		0.6	3.12×10^{-6}
19	Station blackout; failure of EFW, thus reducing available recovery time; and failure to recover AC power prior to core damage.	*	0.5	2.77×10^{-6}
20	Small LOCA and failure of both trains of decay heat cooling water.		0.5	2.70×10^{-6}

*Long-term DHR heat removal is also unavailable

**Seal cooling and injection are both failed.

TABLE 5-3 (continued)

Sheet 4 of 4

Order Number	Description	RCP Seal Fail-ure	Contribution to Severe Core Damage Frequency, Percent of 5.5 x 10-4	Mean Frequency per Reactor Year
21	Steam generator tube rupture and failure to cool down prior to BWST exhaustion, leading to continuing inventory loss with no makeup available.		0.4	2.44×10^{-6}
22	Loss of one train of DC power, failure of EFW, and failure of operator to start HPI cooling.		0.4	2.09×10^{-6}
23	Reactor trip, continued small RCS inventory loss, failure of both trains of decay heat cooling water, and failure of the operator to get decay heat removal back prior to core damage.		0.4	1.88×10^{-6}
24	Loss of one train of DC power, failure of EFW, failure of the opposite train of decay heat cooling water, leading to unavailability of high pressure recirculation.		0.4	1.88×10^{-6}
25	Very small break and failure to establish high pressure sump recirculation.		0.4	1.86×10^{-6}

TABLE 5-4. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE

Sheet 1 of 5

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	System (SAR Section; Component Table Number) System Action Category • Specific System Action	Total System Contribution to Core Damage Frequency	System* Action Category Contribution to Core Damage Frequency	Specific System Action Contribution to Top Event
			Control Building Ventilation (6; 5-5A)	43%		
CV			Control Building Ventilation		43% [1%]	
	I.E.	LC	• Loss of CBV Initiating Event			98%
	CV-1(NS)	CVD	• Control Building Ventilation Failure			2%
			Decay Heat Removal (6; 5-7B)	37%		
SA			Decay Heat Removal - Reactor Building Sump Train A		15% [5%]	
SB			Decay Heat Removal - Reactor Building Sump Train B		12% [5%] {5%}	
DH			Decay Heat Removal - Pumps and Heat Exchangers		8% [8%]	
HL			Decay Heat Removal - High Pressure Recirculation		4% [2%]	
LP			Low Pressure Injection Mode		2% [.2%]	
BW			Borated Water Storage Tank		1%	
			High Pressure Injection (13; 5-5C)	37%		
HPB			High Pressure Injection Train B - Pump C		16% [.3%] {0%}	
HPA			High Pressure Injection Train A - Pumps A and B		9% [1%]	
TH			Throttle High Pressure Injection Flow		8% [5%]	
MR			Minimum-Flow Recirculation		7% [6%]	
HI			High Pressure Injection Valves		2% [.2%]	
INJ			RCP Seal Injection Valves		2%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-4 (continued)

Sheet 2 of 5

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	System (SAR Section; Component Table Number) System Action Category • Specific System Action	Total System Contribution to Core Damage Frequency	System* Action Category Contribution to Core Damage Frequency	Specific System Action Contribution to Top Event
			Electric Power (2; 5-5E)	24%		
OP			Offsite Power		6% [.2%]	
	I.E.	AC	• Loss of Offsite Power Initiating Event from Operating History Data			96%
	OP-1	OPA	• Loss of Offsite Power after Plant Trip			4%
GA			Emergency AC Power - Train A		5%	
GB			Emergency AC Power - Train B		4% {1%}	
1C			480V AC Motor Control Center-1C ESV		3%	
DB			Emergency DC Power - Train B		3%	
AA			ATA bus		2% [.1%]	
DA			Emergency DC Power - Train A		2%	
			Main Steam and Feedwater	23%		
			(8, 9, 10; none)			
MF-			Main Feedwater - Enough		14% [.1%]	
TC			Main Steam Safety Valves Reclose		8% [6%]	
MF+			Main Feedwater - Too Much		1%	
TT			Turbine Trip		< .02%	
SD			Secondary System Relief Valves Open		< .02%	
SL			Steam Line Rupture Detection System		< .02%	
SI			Main Steam Isolation Valves Close		< .02%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-4 (continued)

Sheet 3 of 5

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	System (SAR Section; Component Table Number) System Action Category • Specific System Action	Total System Contribution to Core Damage Frequency	System* Action Category Contribution to Core Damage Frequency	Specific System Action Contribution to Top Event
			RCS Pressure Control (12; none)	22%		
PO			PORV Opens		11% [.2%]	
RC			Primary Relief Valves Reclose		8%	
CE			Cooldown during an SGTR		3% [1%]	
CD			Cooldown after a Small Leak		2%	
PV			Primary Relief Valves Open		< .02%	
			Decay Heat Cooling Water (5; 5-5B)	21%		
HA			Decay Heat Cooling Water - Train A		12% [9%]	
HB			Decay Heat Cooling Water - Train B		11% [8%] (2%)	
			Intermediate Closed Cooling Water (13; 5-5D)	9%		
SE			Intermediate Closed Cooling Water		9% [5%]	
			Emergency Feedwater (11; 5-5F)	6%		
EF-			Emergency Feedwater - Not Enough		6%	
EF+			Emergency Feedwater - Too Much		< .02%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-4 (continued)

Sheet 4 of 5

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	System (SAR Section; Component Table Number) System Action Category • Specific System Action	Total System Contribution to Core Damage Frequency	System* Action Category Contribution to Core Damage Frequency	Specific System Action Contribution to Top Event
			Instrument Air (18; 5-5G)	4%		
AM			Instrument Air		4% [.2%]	
	I.E.	LA	• Loss of Instrument Air Initiating Event - From Operating History Data			95%
	AM-1(OP.GA/GB)	AMD	• Given Emergency AC Train A or B and Offsite Power Unavailable			4%
			Nuclear Services Cooling Water (4; 5-5H)	4%		
NS			Nuclear Services Cooling Water		4% [.2%]	
	I.E.	LR	• Loss of River Water Initiating Event From Operating History Data			76%
	I.E.	LNS	• Loss of Nuclear Services Cooling Water Initiating Event			17%
	NS-1	NSA	• One Train Operates for 24 Hours			4%
	NS-1.0	NSG	• Guaranteed Failure Cooling Water Initiating Event			2%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-4 (continued)

Sheet 5 of 5

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	System (SAR Section; Component Table Number) System Action Category ● Specific System Action	Total System Contribution to Core Damage Frequency	System* Action Category Contribution to Core Damage Frequency	Specific System Action Contribution to Top Event
			Engineered Safeguards Actuation (3; none)	2%		
EA			ESAS - Train A		1%	
EB			ESAS - Train B		1%	
			Reactor Protection (7; none)	1%		
RT			Reactor Trip		1%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5a. SYSTEMS ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM THE CONTROL BUILDING VENTILATION SYSTEM

Sheet 1 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) ● Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
CV			Control Building Ventilation	43% [1%]		
	I.E.	LC	● Loss of CBV Initiating Event		98%	
			- CCF of Chillers or Chilled Water Pumps and Outside Air Temperature > 95°F			44%
			- CCF of Ventilation Booster or Exhaust Fans and Failure of Operator To Establish Alternate Cooling			19%
			- Chilled Water Train Maintenance and Failure of Operator To Establish Alternate Cooling			10%
			- Failure of Both Trains of Chilled Water and Outside Air Temperature > 95°F			8%
			- Failure Closed of 1 of 19 Fire Dampers and of Operator To Establish Alternate Cooling			4%

Key: CCF = common cause failure.
[ ] = contribution from failures within the system itself.

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see FMR, Section 1). Contributors to other results were not included.

TABLE 5-5a (continued)

Sheet 2 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
			- Failure of Both Ventilation Booster or Exhaust Fans and Failure of Operator To Establish Alternate Cooling			3%
			- Exhaust Fan Maintenance and Failure of Operator To Establish Alternate Cooling			3%
			- Booster Fan Maintenance and Failure of Operator To Establish Alternate Cooling			3%
	CV-1(NS)	CVD	• Control Building Ventilation Failure, Given Failure of Nuclear Services Water		2%	
			- Outside Air Temperature > 95°F			94%
			- Operator Fails To Realign Once-Through Cooling or Establish Alternate Ventilation			3%
			- Maintenance			2%

Key: CCF = common cause failure.
[ ] = contribution from failures within the system itself.

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5b. SYSTEMS ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM THE DECAY HEAT REMOVAL SYSTEM

Sheet 1 of 3

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
SA			Decay Heat Removal - Reactor Building Sump Train A	15% [6%]		
	SA-1(GA)=1	SAB	• Guaranteed Failure due to Failure of Electric Power Train A		53%	
	SA-1	SAA	• Recirculation Available and Initiated within 1 Minute during a Large LOCA		32%	
			- Operator Fails To Initiate			93%
			- Sump Clogs or DH-V6 Fails To Open			6%
	SA-1.0	SAE	• Guaranteed Failure		8%	
	SA-2	SAC	• Recirculation Available and Initiated within 10 Minutes during a Small or Very Small LOCA		7%	
			- DH-V6 Fails To Open			82%
			- CCF Failure			7%
			- Sump Clogs			3%
			- Operator Fails To Initiate			3%
DH			Decay Heat Removal - Pumps and Heat Exchangers	8% [8%]		
	DH-1	DHA	• At Least One Train Starts and Runs		20%	
			- CCF of Both Pumps To Start			77%
			- Pump Maintenance			8%
			- Piggy-Back Strainer Maintenance			4%
			- Pump Operability Testing			3%

Key: CCF = common cause failure.
[ ] = contribution from failures within the system itself.

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5b (continued)

Sheet 2 of 3

System Action Category (top event)	Specific System Action [split fraction/initiating event (I.E.)]	Split Fraction/Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/Initiating Event Contribution to Top Event	Component/Operator Action Contribution to Split Fraction/Initiating Event
	DH-1(HA.HB)	DHF	• At Least One Train Starts and Runs, and One Train of Decay Heat Cooling Is Recovered in 6 Hours		14%	
	DH-1(GA)	DHK	• At Least One Train Starts and Runs, and One Train of Onsite AC Power is Recovered in 6 Hours		14%	
HL			Decay Heat Removal - High Pressure Recirculation	4% [2%]		
	HL-1.0	HLC	• Guaranteed Failure		42%	
	HL-1	HLA	• Align Closed Loop		20%	
			- Maintenance on DH-V3			35%
			- Operator Fails To Open Valves			29%
			- Misalignment after Testing			26%
	HL-2(SA)	HLE	• Align from Reactor Building Sump, Given Sump Suction Train A Failed		20%	
			- Failure of DH-V7B To Open and Remain Open			90%
			- CCF of Two Motor-Operated Valves			8%
			- Failure of Y-Strainer			2%
	HL-2	HLB	• Align from Reactor Building Sump		18%	
			- CCF of DH-V7A and DH-V7B			96%
			- Failure of Y-Strainer and Opposite DH-V7 Valve			2%

Key: CCF = common cause failure.
[ ] = contribution from failures within the system itself.

*These are percentages of the total core damage frequency calculated from the internal evente plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5b (continued)

Sheet 3 of 3

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
HA			Decay Heat Cooling Water - Train A	12% [9%]		
			• Available to Decay Heat Exchange		74%	
			- Maintenance of Decay Heat River Water Pump			48%
			- Failure of Standby River Water Pump To Start and Run			13%
			- Failure of Motor-Operated Water Pump Discharge Valve			9%
			- Maintenance of Decay Heat Closed Cooling Water Pump			8%
			- Maintenance of River Water Strainer			6%
			- Maintenance of Decay Heat Service Cooler			4%

Key: CCF = common cause failure
[ ] = contribution from failures within the system itself.

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5c. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM HIGH PRESSURE INJECTION SYSTEM

Sheet 1 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
HPA			High Pressure Injection Train A - Pumps A and B	9% [1%]		
	HP-1.0	HPI	• Guaranteed failure		84%	
	HP-1(OP/NS)	HPK	• One of Two Pumps Work after Offsite Power or Nuclear Services Fail		10%	
			- Unscheduled Maintenance of Both Pumps			49%
			- Failure of Pump C To Start			19%
			- Failure of Pump C To Run for 24 Hours			13%
			- Failure of One of Seven Isolation Check Valves To Open			10%
			- CCF of Pump C To Start and Run for 24 Hours			4%
			- Failure of Discharge Check Valve MU-V74C To Open			3%
	HP-1	HPA	• One of Two Pumps Work To Provide Flow		3%	
			- Failure of Suction Valve MU-V14A			54%
			- Unscheduled Maintenance of Both Pumps			38%
			- CCF of Both Motor-Operated Suction Valves (MU-V14s)			5%
			- CCF of Both Makeup Pumps			6%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5c (continued)

Sheet 2 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
MR			High Pressure Injection	7% [6%]		
	MR-1	MRA	• Minimum-Flow Recirculation Is Established after Successful Throttling		81%	
			- Failure of Operator			98%
			- Failure of Either Motor-Operated Valve To Open			2%
	MR-1.0	MRB	• Guaranteed Failure		19%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5d. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM INTERMEDIATE CLOSED COOLING WATER SYSTEM

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
SE			Intermediate Closed Cooling Water	9% [5%]		
	SE-1	SEA	• Seal Cooling Is Maintained to all Four RCPs		34%	
			- Failure of Either Air-Operated Valve			44%
			- Failure of Seal Cooling Heat Exchanger			31%
			- Failure of Both ICCW Pumps			11%
			- Unscheduled Pump Maintenance			8%
			- Failure of One of Five Motor-Operated Valves			3%
	SE-1.0	SEC	• Guaranteed Failure		41%	
	SE-1(OP. AM.GA)	SEE	• Seal Cooling Is Maintained to All Four RCPs, Given Offsite Power and Diesel A Failure and Instrument Air Success		21%	
			- Reverse Leakage of Check Valve			44%
			- Unscheduled Pump Maintenance			27%
			- Failure of Pumps To Start			18%
			- Failure of Check Valves To Open			5%
			- Failure of RCP Seal Cooler			3%
	SE-1 (GA/GB)	SEB	• Seal Cooling Is Maintained to All Four RCPs, Given One Train of AC Power Is Failed		4%	
			- Reverse Leakage of Check Valve			44%
			- Unscheduled Pump Maintenance			27%
			- Failure of Pumps To Start			18%
			- Failure of Check Valves To Open			5%
			- Failure of RCP Seal Cooler			3%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5e. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM THE ELECTRIC POWER SYSTEM

Sheet 1 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
OP			Offsite Power	6% [.2%]		
	I.E.	AC	• Loss of Offsite Power Initiating Event - From Operating History Data		96%	
	OP-1	OPA	• Loss of Offsite Power after Plant Trip		4%	
			- Failure of Offsite Grid on Demand			46%
			- Failure of Offsite Grid during 24-Hour Mission Time			33%
			- Failure of Either of Two Auxiliary Power Transformers			10%
			- Failure of Either of Two Circuit Breakers			7%
			- Failure of Either of Two Buses during Operation			4%
GA			Emergency AC Power - Train A	5% [%]		
	GA-1(OP)	GAB	• Provide AC Power from Diesel Generator A for 6 Hours		57%	
			- Unscheduled Maintenance of Diesel Generator Set			47%
			- Failure of Diesel To Start on Demand			21%
			- Failure of Diesel Generator To Continue To Run After First Hour			17%
			- Failure of Diesel Generator To Run for the First Hour			9%
			- Diesel Generator Breaker Failure			4%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5e (continued)

Sheet 2 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
	GA-1	GAA	• Provide AC Power From Diesel Generator A or From Offsite		38%	
			- One of Nine Circuit Breakers Transfers Open			57%
			- Failure of One of Seven Electric Buses			27%
			- Failure of One of Three Transformers during Operation			10%
			- Circuit Breaker 1SB-D2 Transfers Open			6%
	GA-1.0	GAC	• Guaranteed failure		5%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5f. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM THE EMERGENCY FEEDWATER SYSTEM

Sheet 1 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
EF-			Emergency Feedwater - Not Enough	6%		
	EF-1(OP. AM.GA/GB)	EFE	• At Least One Pump Started, Given No Offsite Power, No Instrument Air, and Only One Train of Emergency AC Power Available		41%	
			- Failure of Operator To Replenish the 2-Hour Air Bottles and To Locally Control the EFW Flow			63%
			- Failure of the 2-Hour Air and of the Operator To Locally Control The EFW Flow			18%
			- Failure of the Turbine-Driven Pump and of the Remaining Motor-Driven Pump To Start or Run			9%
			- Failure of the Turbine-Driven Pump, while the Remaining Motor-Driven Pump Is in Maintenance			8%
	EF-1(OP. GA/GB)	EFF	• At Least One Pump Started, Given No Offsite Power, and Only One Train of Emergency AC Power Available		33%	

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5f (continued)

Sheet 2 of 2

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
	EF-1(OP .AM)	EFD	• At Least One Pump Started, Given No Offsite Power and No Instrument air		20%	
			- Failure of Operator To Replenish the 2-Hour Air Bottles and To Locally Control the EFW Flow			96%
			- Failure of the Turbine-Driven Pump and CCF of the Two Motor-Driven Pumps or CCF of All Three			1%
	EF-1(OP. AM.VA/VB)	EFH	• At least One Pump Started, Given No Offsite Power, No Instrument Air, and Only One Train of Vital Instrument AC Power Available		6%	
			- Failure of Operator To Replenish the 2-Hour Air Bottles and To Locally Control the EFW Flow			75%
			- Failure of the 2-Hour Air and of the Operator To Locally Control the EFW Flow			22%
			- Failure of the Turbine-Driven Pump and CCF of the Two Motor-Driven Pumps			1%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5g. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM THE INSTRUMENT AIR SYSTEM

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
AM			Instrument Air	4% [.2%]		
	I.E.	LA	• Loss of Instrument Air Initiating Event - From Operating History Data		95%	
	AM-1(OP. GA/GB)	AMD	• Given Emergency AC Train A or B and Offsite Power Unavailable:		4%	
			- Failure of Operator To Restart Air Compressors after Loss of Offsite Power			84%
			- Failure of Air Compressors To Start and Run			8%
			- CCF of Air Compressors To Start and Run			4%
			- Maintenance on The Air Compressors			4%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-5h. SYSTEMS AND ACTIONS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM THE NUCLEAR SERVICES COOLING WATER SYSTEM

System Action Category (top event)	Specific System Action [split fraction/ initiating event (I.E.)]	Split Fraction/ Initiating Event Abbreviation	Description of: System Action Category (top event) • Specific System Action (initiating event/split fraction) - Component or Operator Action	System* Action Category (top event) Contribution to Core Damage Frequency	Specific System Action Split Fraction/ Initiating Event Contribution to Top Event	Component/ Operator Action Contribution to Split Fraction/ Initiating Event
NS			Nuclear Services Cooling Water	4% [.2%]		
	I. E.	LR	• Loss of River Water Initiating Event - From Operating History Data		76%	
	I. E.		• Loss of Nuclear Services Cooling Water Initiating Event		17%	
	NS-1	NSA	• One Train Operates for 24 Hours		4%	
			- Rupture of Heat Exchanger, and Operator Fails To Isolate			56%
			- Failure of Closed Cooling Water Pump To Operate and Its Discharge Check Valve To Reseat			8%
			- Maintenance on One River Water Pump and Other Two River Water Pumps Fail			7%
			- River Water Header Isolation Valve Transfers Closed			6%
			- CCF of All Three River Water Pumps			5%
			- Maintenance on One Closed Pump and Other Two Closed Pumps Fail			5%
	NS-1.0	NSG	• Guaranteed Failure Cooling Water Initiating Event		2%	
			- Maintenance on DH-V3			35%

*These are percentages of the total core damage frequency calculated from the internal events plus one fire contained in the event tree results assembled with MAXIMA (see PMR, Section 1). Contributors to other results were not included.

TABLE 5-6. OPERATOR ACTION FAILURES CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE

Sheet 1 of 3

Specific Operator Action [split fraction (I.E.)]	Split Fraction Abbreviation	Operator Action Category • Specific Operator Action*	Operator Action Category Contribution to Core Damage Frequency	Specific Operator Action Contribution to Total Contribution of Category
		Operator Restoration and Recovery:	30%	
I.E.	LC	• Loss of CBV Initiating Event (includes operator failure to establish alternate cooling)		42%
DH-1(GA)	DHK	• At Least One Train of DHR Starts and Runs, and One Train of Onsite AC Power Is Recovered in 6 Hours		18%
I.E.	LR	• Loss of River Water Initiating Event - From Operator History Data (includes operator failure to clear the screen before plant trip)		10%
RE-2	REB	• Recover River Water		5%
RE-2(EF)	REF	• Recover River Water with Steam-Driven EFW Pump Failed		4%
RE-1(EF)	REC	• Recover Onsite or Offsite Power during a Station Blackout with Steam-Driven EFW Pump Failed		3%
RE-3	REG	• Recover Single Train of Onsite Power or Offsite Power		.3%
CV-1(NS)	CVD	• Provide Alternate Ventilation after Control Building Ventilation Failure, Given Failure of Nuclear Services Water		.3%
RE-3(EF)	REH	• Recover Single Train of Onsite Power or Offsite Power With Steam-Driven EFW Pump Failed		.1%
RE-1	REA	• Recover Onsite or Offsite Power during a Station Blackout		.1%
		Manual Actions To Actuate Systems	13%	
MR-1	MRA	• Minimum-Flow Recirculation Is Established after Successfully Throttling HPI		47%

*Indicates failure of the action described.

TABLE 5-6 (continued)

Sheet 2 of 3

Specific Operator Action [split fraction (I.E.)]	Split Fraction Abbreviation	Operator Action Category • Specific Operator Action*	Operator Action Category Contribution to Core Damage Frequency	Specific Operator Action Contribution to Total Contribution of Category
SA-1	SAA	• Recirculation Available and Initiated within 1 Minute of BWST Low Level Alarm during a Large or Medium LOCA		39%
BW-2	BWB	• Operator Initiates HPI Cooling		6%
TH-2(GA)	THG	• Throttle Makeup Flow Using MU-V16s before Diesel Generator Train A Fails		6%
ID-1	IDA	• Operator Identifies SGTR		2%
TH-2	THB	• Throttle Makeup Flow Using MU-V16s		2%
CD-1	CDA	• Operator Cools Down To Repair Small Leak		.6%
TH-1	THA	• Throttle Makeup Flow Using MU-V217		.4%
SA-2	SAC	• Recirculation Available and Initiated within 10 Minutes of BWST Low Level Alarm during a Small or Very Small LOCA		.3%
TH-1(OP)	THF	• Throttle Makeup Flow Using MU-V217, Given that Offsite Power Is Lost after Plant Trip		.06%
CE-1	CEG	• Operator Cools Down during an SGTR Leak in RCS		.06%
		Manual Backup To Automatic Actuations	8%	
EF-1(OP.AM.GA/GB)	EFE	• At Least One Pump Started, Given No Offsite Power, No Instrument Air, and Only One Train of Emergency AC Power Available		23%
RC-3	RCC	• Primary Safety Valves Reclose after Passing Water and Operator Throttles HPI Flow		19%
EF-1(OP.GA/GB)	EFF	• At Least One Pump Started, Given No Offsite Power and Only One Train of Emergency AC Power Available		18%
EF-1(OP.AM)	EFD	• At Least One Pump Started, Given No Offsite Power and No Instrument Air		13%

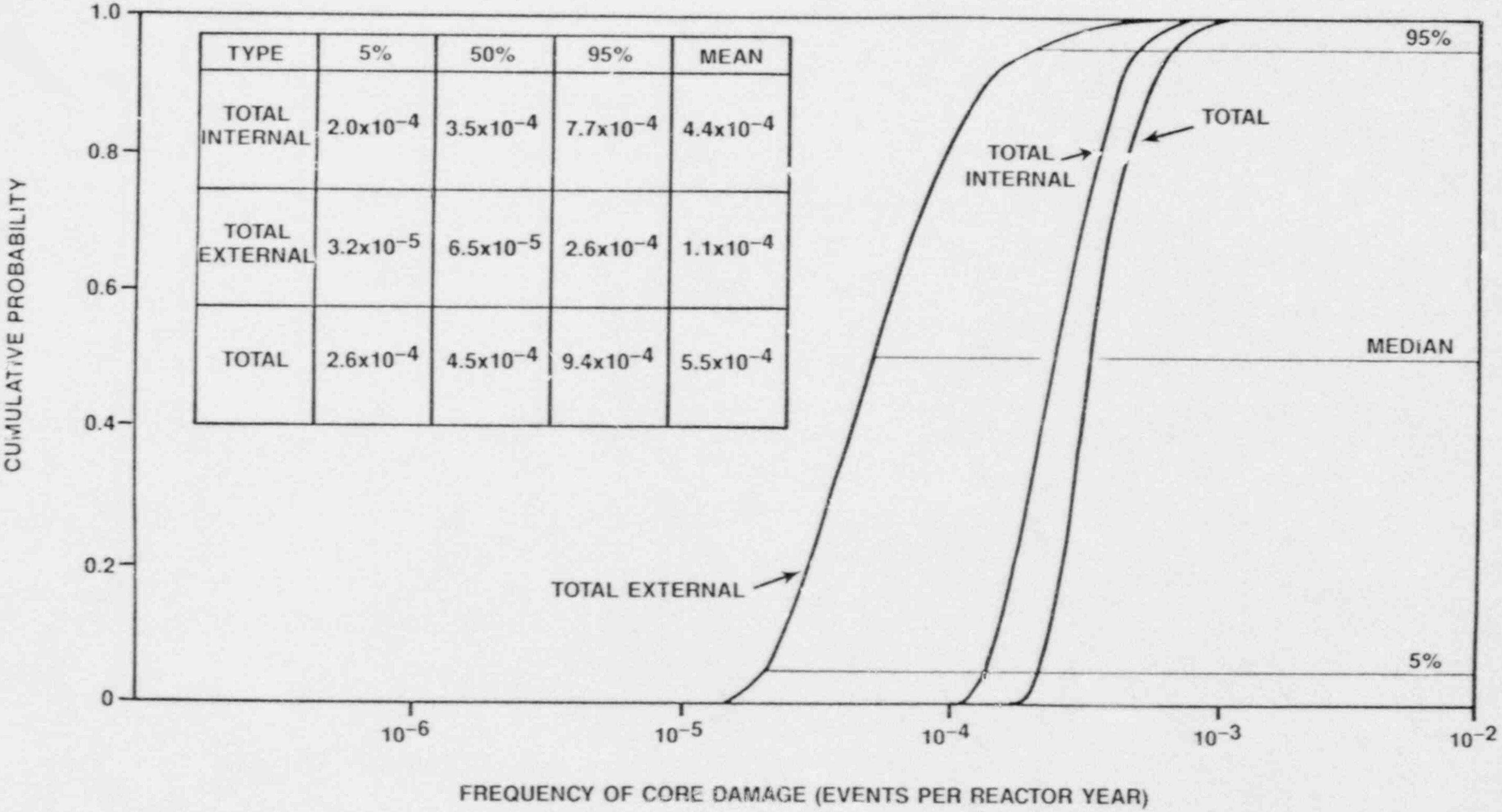
*Indicates failure of the action described.

TABLE 5-6 (continued)

Sheet 3 of 3

Specific Operator Action [split fraction (I.E.)]	Split Fraction Abbreviation	Operator Action Category • Specific Operator Action*	Operator Action Category Contribution to Core Damage Frequency	Specific Operator Action Contribution to Total Contribution of Category
RC-6	RCF	• PORV Recloses after Passing Water, and Operator Throttles HPI Flow		9%
AM-1(OP. GA/GB)	AMD	• Given Emergency AC Train A or B and Offsite Power Not Available		2%
Total Contribution of All Manual Actions to Core Damage Frequency			50%	

*Indicates failure of the action described.



TYPE	5%	50%	95%	MEAN
TOTAL INTERNAL	2.0×10^{-4}	3.5×10^{-4}	7.7×10^{-4}	4.4×10^{-4}
TOTAL EXTERNAL	3.2×10^{-5}	6.5×10^{-5}	2.6×10^{-4}	1.1×10^{-4}
TOTAL	2.6×10^{-4}	4.5×10^{-4}	9.4×10^{-4}	5.5×10^{-4}

FIGURE 5-1. TMI-1 PRA PROBABILITY OF CORE DAMAGE FREQUENCY DISTRIBUTIONS
(CUMULATIVE PROBABILITY FORMAT)

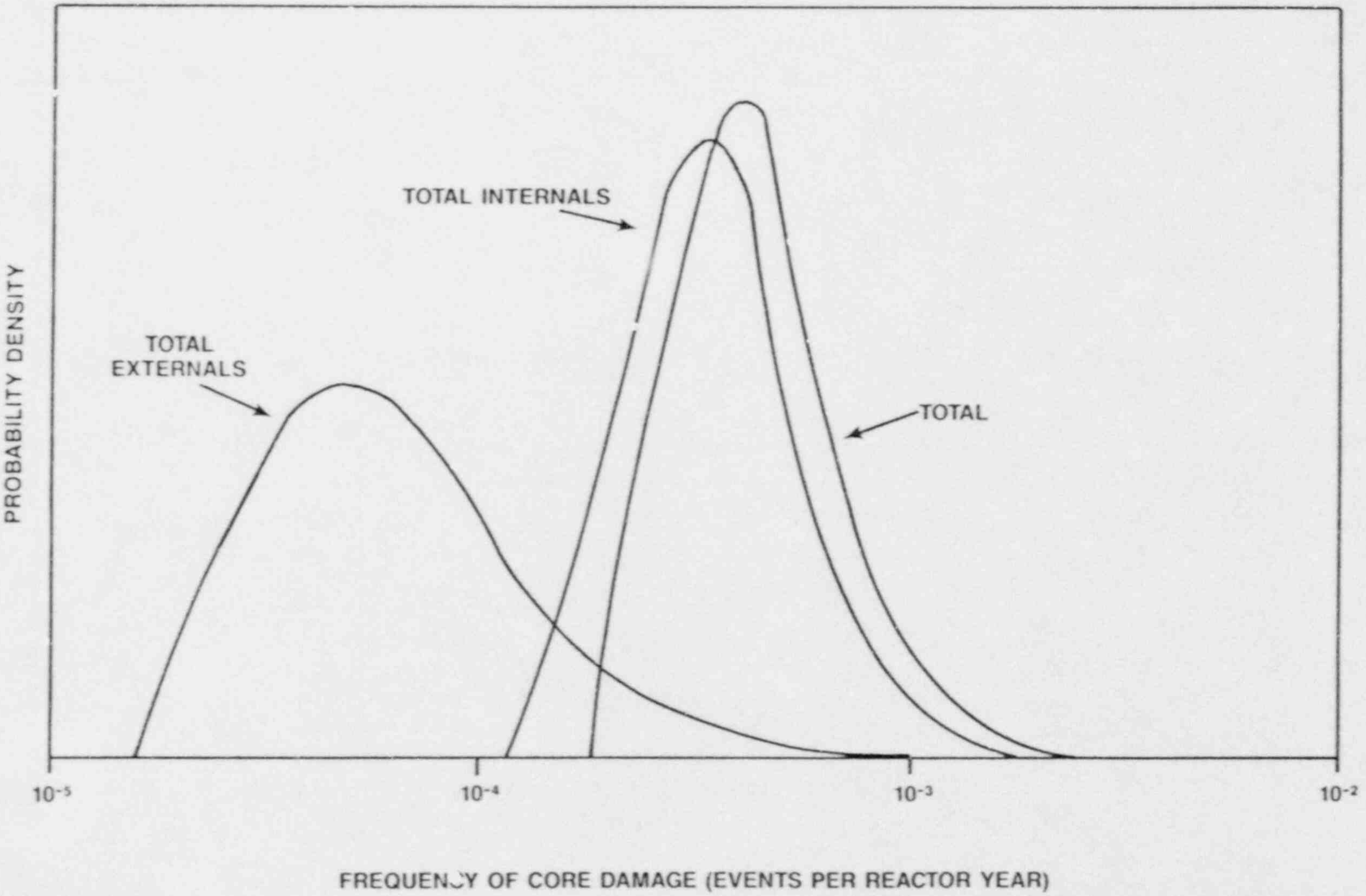


FIGURE 5-2. TMI-1 PRA PROBABILITY OF CORE DAMAGE FREQUENCY DISTRIBUTIONS (PROBABILITY DENSITY FORMAT)

APPENDIX A

SYSTEMS DESCRIPTION

This section provides a summary description of the 17 systems that were analyzed and included in the TMI-1 PRA plant model. More details of each system can be found in each system's section of the Systems Analysis Report.

A.1 ELECTRIC POWER SYSTEM

The primary function of the electric power system is to provide a source of motive, control, and instrument power to various plant equipment. This function is normally accomplished by supplying power from the offsite network to the 230-kV electrical substation, which in turn supplies power to plant loads through two auxiliary transformers.

All plant loads are normally supplied from offsite power through the auxiliary transformers and not directly from the Unit 1 main turbine-generator and transformers. Therefore, when a plant trip occurs due to an initiating event other than a loss of offsite power, a fast transfer from the main generator output to offsite power is not required. If that power is lost from the output of an auxiliary transformer, the nonengineered safeguards loads being supplied from that auxiliary transformer will automatically transfer to the other auxiliary transformer if power is available from it. At the same time, a diesel generator will start and supply power to the train of engineered safeguards loads that lost power.

If offsite power is lost, power will be supplied from two automatic, fast-startup diesel engine generators. These are sized so that either one can carry the required engineered safeguards load. The ratings of each emergency generator vary between 2,600 and 3,300 kW at 0.8 power factor, depending on the annual maintenance period and the load duration. Each emergency generator will feed one of the 4,160V engineered safeguards buses. Each generator is capable of feeding the safeguards loads of one 4,160V bus following required loss of coolant accident as well as selected nonemergency loads.

The analysis of the electric power system is described in detail in Section 2 of the Systems Analysis Report.

A.2 ENGINEERED SAFEGUARDS ACTUATION SYSTEMS

The engineered safeguards actuation systems monitors parameters to detect loss of integrity in the reactor coolant system pressure boundary and initiates operation of the high and low pressure injection systems, the reactor building isolation, the reactor building cooling, and the reactor building spray systems. In addition, the signal is used to start the emergency diesel generators and to control load sequencing.

The reactor coolant pressure and reactor building pressure have been selected as parameters to initiate engineered safeguards action. Pressure of 1,600 psig or 500 psig in the reactor coolant system and

4 psig or 30 psig in the reactor building are the levels at which injection and other engineered safety features are actuated. Each of these actuation parameters is measured by three sensors. The output signal of each sensor is monitored for each level by a bistable that has two output relays, one for each of two channels.

The analysis of the engineered safeguards actuation system is described in detail in Section 3 of the Systems Analysis Report.

A.3 NUCLEAR SERVICES RIVER AND CLOSED COOLING WATER SYSTEMS

The nuclear services closed cooling water system consists of four 33%-capacity nuclear services coolers and three 50%-capacity nuclear services closed cooling water pumps. This system, along with the intermediate cooling system, satisfies the cooling requirements of all nuclear-oriented services other than decay heat and reactor building emergency cooling. In the event of a LOCA, 100% redundancy of all nuclear services equipment is obtained by isolating nonessential items so that flow requirements are reduced to approximately half that of normal operation. An elevated surge tank of 1,470-gallon liquid capacity (1,600-gallon total capacity) provides storage of water for the nuclear services closed cooling system. Makeup is added from the demineralized water storage tank by remote manual action taken in the control room.

The nuclear services river water system, while having redundancy in itself, can also be supplemented by secondary services river water pumps, by valving if required. The nuclear services river water pumps are sized to cool the nuclear services coolers and also the intermediate service coolers. They are located in the intake screen and pump house. Each pump is equipped with a booster pump, which supplies pressurized filtered water to the pump shaft and the bearings.

River water is circulated through the tubes of the nuclear services coolers located in the cooler vault. Closed cooling water is circulated on the shell side. After passing through the coolers, the river water can be used for emergency deicing purposes or diverted to the cooling tower collecting sump or returned to the river. Radioactive fluid leakage will not be returned to the river from these systems unless a tube leak occurs simultaneously in a nuclear services cooler and in a cooler served by the closed system.

The analysis of the nuclear services river and closed cooling water systems are described in detail in Section 4 of the Systems Analysis Report.

A.4 DECAY HEAT RIVER AND CLOSED COOLING WATER SYSTEMS

Decay heat removal cooling water is provided by two separate 100%-capacity trains from the decay heat removal coolers back to the ultimate heat sink (Susquehanna River). Each of these trains consists of two separate loops, one closed and one river water. Each decay heat river water train consists of a 100%-capacity decay heat river water pump, which cools a 100%-capacity decay heat services cooler. Each closed cooling water train consists of a 100%-capacity decay heat closed cooling water pump, which circulates cooling water through a 100%-capacity decay heat removal cooler and through those pumps and motors associated with the decay heat removal system that require cooling. The 100% capacity referred to above is 100% of the cooling required during a 10CFR50 LOCA scenario. Either of the two decay heat trains will permit cooling down the plant under normal shutdown; operating both will provide a faster cooldown.

The analysis of the decay heat river and closed cooling water systems are described in detail in Section 5 of the Systems Analysis Report.

A.5 CONTROL BUILDING VENTILATION SYSTEM

The control building ventilation system is designed to continuously maintain the conditions in the control building within limits of temperature, humidity, and radiation so that engineered safety features will continue to function and to provide a ventilation rate sufficient for healthful human occupancy.

The basic function of this system is to maintain 75°F dry bulb/50% relative humidity inside when it is 95°F dry bulb/75% relative humidity outside and all the engineered safety features required for a LOCA are operating. The system is designed for automatic use of outside air for cooling whenever the outside air temperature is suitable for this purpose.

The control building ventilation system has also been designed to function after a significant radiation release to place selected areas in a recirculation mode and to place the chemical hood in the nuclear sample room and radiochemistry laboratory in a recirculating mode.

The control building ventilation system is a central system employing electric reheat for zone temperature regulation. The supply duct carries air from the conditioning equipment to the rooms on all four floors of the building.

The following major components are employed in the control building ventilation system:

- Two normal-duty supply fans, each sized to handle 100% of the required air supply.

- Two emergency-duty supply fans, each sized to handle 100% of the required air supply.

- Two cooling coil banks, each sized for 100% of the design load. Coils are of a standard finned-tube type. They are cooled by chilled water from mechanical water chillers. The coils are balanced to remove heat to keep the building temperature and relative humidity in the desired range.

- Two mechanical water chillers, each sized for 100% of the design load. Each chiller is a factory-assembled unit complete with all major components mounted on a base structure. Chiller compressors are of centrifugal design, and chiller condensers are of the water-cooled type. These are supplied with cooling water from the nuclear service closed water system.

- Two chilled-water pumps, each sized for 100% of the design water flow. These pumps are of the close-coupled, centrifugal type with mechanical seal.

The emergency recirculation system for Elevation 306' 0" is designed to recirculate, cool, and filter air through selected areas during emergencies that produce high radiation levels outside the control building. The system goes into its emergency mode on a signal from the engineered safeguard system of a design basis accident in the reactor building or on a signal from one or more of the monitoring devices protecting the system from the influx of contaminants carried by the outside and/or the return air.

The analysis of the control building ventilation system is described in detail in Section 6 of the Systems Analysis Report.

A.6 REACTOR PROTECTION SYSTEM

The reactor protection system monitors parameters related to safe operation and trips the reactor to protect the reactor core against fuel rod cladding damage. It also assists in protecting against reactor coolant system damage caused by high system pressure by limiting energy input to the system through reactor trip action.

The system consists of four identical protection channels, each terminating in a trip relay within a reactor trip (RT) module. In the normal untripped state, each protection channel functions as an AND gate, passing current to the terminating relay and holding it energized as long as all inputs are in the normal energized (untripped) state. Should any one or more inputs become deenergized (tripped), the terminating relay in that protective channel deenergizes (trips). Thus, for the trip signals, each protective channel becomes an OR gate.

Each of the four protection channels terminates in a channel trip relay within a reactor trip module. There are four such modules. Each protective channel trip relay has four logic-controlling contacts, each controlling a logic relay in one reactor trip module. Therefore, each reactor trip module has four logic relays controlled by the four protection channels. The four logic relays combine to form a two out of four coincidence network in each reactor trip module. The coincidence logics in all reactor trip modules trip whenever any two of the four protection channels trip.

The four RPS protective channels are identical in their functions. They are all combined in the system logic to trip the reactor automatically and protect the reactor core for the following conditions:

1. When the reactor power, as measured by neutron flux, exceeds a fixed maximum limit.

2. When the reactor power, as measured by neutron flux, exceeds the limit set by the reactor coolant flow and power imbalance.

3. When the reactor power exceeds the limit set by the number and combination of reactor coolant pumps in operation.

4. When the reactor outlet temperature exceeds a fixed maximum limit.

5. When a specified reactor pressure-outlet temperature relationship is ~xceeded.

6. When the reactor pressure falls below a fixed minimum limit or exceeds a fixed maximum limit.

7. When reactor building pressure exceeds a fixed maximum limit.

In addition to the above protective trips, an anticipatory trip has been added to the RPS to trip the reactor on loss of both main feedwater pumps or a main steam turbine trip.

The analysis of the reactor protection system is described in detail in Section 9 of the Systems Analysis Report.

A.7 TURBINE TRIP

The turbine receives steam from two steam generators (thermal energy) and converts the thermal energy to mechanical energy through rotation of the turbine shaf*. The turbine, in turn, is directly connected to an electric generator that produces electrical energy on rotation of an excited field.

Turbine trip is actuated by four main stop valves, which quickly shut off steam to the turbine under emergency conditions. These stop valves are located one each in the four main steam lines upstream from the control valves to which they are welded. One of the main stop valves is provided with an internal bypass valve capable of passing approximately twice the no-load flow for slow warming of the stop valves, control valves, high pressure shell, and for decreasing the pressure differential across the main stop valves until the hydraulic cylinder can open the valves. The remaining three stop valves have no bypass and are either fully open or fully closed.

The turbine has an electrohydraulic control system that controls acceleration, load, speed and overspeed by positioning of the steam valves (stop valves, control valves, and combined intermediate valves). Prior to turbine trip, the emergency trip system oil pressure is supplied to the disc dump valves of the hydraulic actuators on each steam valve. This oil pressure allows the steam valves to stay open. Under emergency conditions, sudden relieving of the oil pressure will result in rapid closure of all steam valves to prevent overspeed. If all four of either the stop or control valves are closed the turbine is said to be in a tripped condition.

The analysis of the turbine trip system is described in detail in Section 8 of the Systems Analysis Report.

A.8 MAIN STEAM SYSTEM

The main steam system delivers steam from the steam generators to the high-pressure turbine and the main feedwater pump turbines during startup, power operation, and when shutting down the unit. Under conditions in which both main feedwater pumps are unavailable, the steam generators deliver steam to the emergency feedwater pump turbine.

Also, after turbine trip, the main steam system dissipates all the energy produced in the reactor coolant system through the turbine bypass system to the condenser and to the atmosphere via the main steam safety valves. The 28.9% step load rejection capability of the turbine bypass valves and atmospheric dump valve requires that the main steam safety valves open on turbine trip.

The main steam system consists of two main steam lines from each OTSG to the high-pressure turbine for a total of four lines. The only cross-connection between the lines is in the turbine steam chest between the turbine stop valves and control valves. Each of the main steam lines is furnished with a main steam isolation stop check valve and branch lines that supply steam to the main feedwater pump turbines and to the emergency feedwater pump turbine.

The motor-operated main steam isolation stop check valves are located in the concrete portions of the intermediate building. They are remotely and manually operated from the control room to close in less than 2 minutes.

The main steam safety valves are located upstream of the main steam isolation stop check valves. The emergency feed pump turbine supply is upstream of the main steam isolation valves and also connects to the turbine bypass valves and the atmospheric dump valves. Downstream of the main steam isolation stop check valves are the main steam stop/control valve assemblies.

The analysis of the main steam system is described in detail in Section 9 of the Systems Analysis Report.

A.9 MAIN FEEDWATER AND INTEGRATED CONTROL SYSTEMS

The main feedwater system, in conjunction with the condensate and heater drains, is designed to supply water at a rate required by the steam generators during full power operation. The integrated control system provides the proper coordination of the reactor, steam generator feedwater, and turbine control under all operating conditions.

The main feedwater system maintains level in the OTSG throughout all modes of normal plant operation. It consists of two 60% capacity turbine-driven feedwater pumps that take suction from the low-pressure heater outlet header and discharge into a common header that supplies two trains of two high-pressure heaters each. Each pump is provided with a recirculation line to the main condenser. Feedwater from the high-pressure heater flows through a temperature mixing header and then enters the steam generator via separate feed lines each provided with main feedwater regulating valves.

The feedwater regulating valves are positioned by the integrated control system; differential pressure across the valve sets feed pump turbine governor speed. For startup or low-load operation, a smaller regulating valve is provided in parallel with the main regulating valve. Also, for startup and hot standby operations, a small bypass line and valve are installed around each of the main feedwater valves to supply a continuous low flow rate to the steam generator feedwater nozzles. The turbines driving the main feedwater pumps are supplied steam from the main steam system and discharge to the condenser. Without the circulating water system and condenser vacuum available, the main feedwater pumps will not operate.

The integrated control system properly coordinates the reactor, steam generator feedwater, and turbine control under all operating conditions. Proper coordination by the ICS consists of producing the best load response to the unit load demand, while recognizing the capabilities and limitations of the reactor, steam generator feedwater system, and turbine. When any single portion of the plant is at an operating limit or control section is on manual, the ICS design uses the limited or manual section as a load reference.

The ICS maintains constant average reactor coolant temperature between 15 and 100% rated power and constant steam pressure at all loads. Optimum unit performance is maintained by limiting steam pressure variations; by limiting the unbalance between the steam generator, turbine, and the reactor; and by limiting the total unit load demand on loss of capability of the steam generator feed system, the reactor, or the turbine generator. The ICS provides limiting actions to ensure proper relationships among the generated load, turbine valves, feedwater flow, and reactor power.

The ICS includes four independent subsystems including the unit load demand, the integrated master control, the steam generator control, and the reactor control. The system philosophy is that control of the plant is achieved through feed-forward control from the unit load demand. The ULD produces demands for parallel control of the turbine, reactor, and steam generator feedwater system through respective subsystems.

The steam generator control is capable of automatic or manual feedwater control from startup to full output. The integrated master control is capable of automatic or manual turbine valve control from minimum turbine load to full output and or manual control below minimum turbine load. The reactor control is designed for automatic or manual operation above about 15% output and for manual operation below 15%.

The analysis of the main feedwater and integrated control systems are described in detail in Section 10 of the Systems Analysis Report.

A.10 EMERGENCY FEEDWATER SYSTEM

The emergency feedwater system delivers water to the steam generators on low level in the steam generator for the purpose of removing decay heat.

The emergency feedwater system is divided into train A and train B, both of which are actuated simultaneously on loss of all four reactor coolant pumps, on loss of both main feedwater pumps, on low steam generator level, or on a 4-psig reactor building pressure signal.

The emergency feedwater system consists of two motor-driven pumps powered from redundant Class 1E 4,160V buses and one 100% capacity turbine-driven pump, which receives steam from the main steam lines. The motor-driven emergency feedwater pumps are automatically loaded on the diesel generator during loss of offsite power with or without simultaneous existence of an ESAS actuation. The three pumps are located in the intermediate building. The turbine-driven pump is physically separated from the motor-driven units.

The emergency feedwater pumps normally take suction through separate lines from the two condensate storage tanks. They may also be manually aligned to take suction from the condenser hot well or demineralized water storage tank. As a further backup source of last resort, river water can be used via the reactor building emergency cooling water pumps.

The three emergency feedwater pumps discharge into a common header from which separate 6-inch lines deliver water to each steam generator. Each of the 6-inch supply lines contains a flow-limiting venturi and two parallel air-operated control valves controlled by the heat sink protection system. The HSPS controls emergency feedwater flow after the emergency feedwater pumps have been activated.

The analysis of the emergency feedwater system is described in detail in Section 11 of the Systems Analysis Report.

A.11 PRESSURE CONTROL SYSTEM

Normal RCS pressure control is by the pressurizer steam cushion in conjunction with the pressurizer spray, pilot (electromagnetic) operated relief valve, and heaters. The system is protected against overpressure by reactor protective system circuits, such as the high-pressure trip, and by pressurizer relief and safety valves located on the top head of the pressurizer. Since all sources of heat in the system (i.e., core, reactor coolant pumps, and pressurizer heaters) are interconnected by the reactor coolant piping with no intervening isolation valves, all relief valves are located on the pressurizer.

The pressurizer spray line originates at the discharge of a reactor coolant pump in the same heat transport loop that contains the pressurizer. Pressurizer spray flow is controlled by an electric motor-operated valve using on-off control in response to the opening and closing pressure setpoints. An electric motor-operated valve in series with the spray valve provides a backup means of securing flow if the spray valve should stick open.

The PORV is mounted on the top head of the pressurizer. The main valve operation is controlled by the opening or closing of a pilot valve, which causes unbalanced forces to exist on the main valve disc. The pilot valve is opened or closed by a solenoid in response to the opening and closing signals from the pressurizer pressure instrumentation at pressure setpoints.

The pressurizer heaters replace heat lost during ncrmal steady state operation, raise the pressure to normal operation pressure during RCS heatup from a cooled down condition, and restore system pressure following transients. The heaters are arranged in 13 groups and are controlled by the pressure controller. The first six groups use modulating control and will normally operate at partial capacity to replace heat lost, thus maintaining pressure at setpoint within a reasonable margin of difference. A basic on or off control is used for the remaining seven groups. A low-level interlock prevents the heaters from being energized with the heaters uncovered.

The analysis of the pressure control system is described in detail in Section 12 of the Systems Analysis Report.

A.12 HIGH PRESSURE INJECTION/MAKEUP AND PURIFICATION SYSTEM

The makeup and purification system serves to control the reactor coolant inventory and the boric acid concentration in the reactor coolant system through the processes of letdown and makeup and to remove impurities in the water.

There are three pumps that serve both a makeup and purification function and a high pressure injection function. Normally, one is operating and two are in standby. The operating pump takes suction from the makeup tank and discharges to the normal makeup and the seal injection lines. Makeup flow to the reactor coolant system is regulated by the reactor coolant volume control valve, which operates on signals from the pressurizer level controller. If greater than normal makeup is required, a manual motor-operated valve allows the operator to provide increased makeup to the reactor coolant system without initiating HPI.

Upon engineered safeguards initiation, the pumps on engineered safeguards standby are activated. (The pumps on ESF standby may or may not include the already operating pumps.) Suction is taken from the borated water storage tank, discharging into each of the high pressure injection lines that discharge into the RCS downstream of the reactor coolant pumps.

The analysis of the high pressure injection/makeup and purification system is described in detail in Section 13 of the Systems Analysis Report.

A.13 LOW PRESSURE INJECTION/DECAY HEAT REMOVAL SYSTEM

The decay heat removal system removes decay heat from the core and sensible heat from the reactor coolant system in four distinct modes:

- Following certain LOCAs in the low pressure coolant injection mode.
- During the latter stages of cooldown in the closed loop recirculation mode.

- Following certain LOCAs in the low pressure, open loop recirculation mode.

- Following other smaller LOCAs in the high pressure or "piggy-back" recirculation mode, with the high pressure injection system.

The system also provides auxiliary spray to the pressurizer for complete depressurization, maintains the reactor coolant temperature during refueling, and provides a means for filling and draining the fuel transfer canal.

In the closed loop, decay heat removal mode, this system takes suction from an reactor coolant system hot leg outlet line and delivers the water back to the reactor through the core flooding nozzles after passing through the decay heat removal pumps and coolers. The decay heat removal system may be lined up in this mode when the reactor pressure is below the DHR system suction piping design pressure and temperature for cooldown of the system to refueling temperatures. The coolers remove the decay heat from the reactor coolant passing through them. With both coolers in operation, the decay heat removal system is designed to cool the reactor coolant system from 250°F to 140°F in 14 hours. Decay heat is transferred to the decay heat closed cooling water system through the decay heat removal cooler.

The major system components consist of two redundant trains, each consisting of a DHR pump and a cooler, as well as various pipes and valves, depending on the lineup. The decay heat removal pumps are arranged in parallel and are designed for continuous operation during the period required for removal of decay heat during a routine shutdown and refueling.

Each pump is provided with an integral motor lube oil system. Remotely operated vent valves provide for venting of air and noncondensibles from the pump casings under normal conditions and after the accident when decay heat removal vaults are not accessible.

The borated water storage tank is located outside the reactor building and the auxiliary building. It contains a minimum of 2,270-ppm boron in solution and is used for RCS inventory control. The borated water storage tank provides a suction source for the reactor building spray system, the decay heat removal system in the low pressure injection mode, and the makeup and purification system in the high pressure injection mode. Redundant high, low, and low-low level indication and alarms are provided on the main control console.

During a LOCA, the borated water storage tank water is delivered to the RCS via the emergency core cooling system injection pumps. When the BWST level drops to the low-low level alarm point of 3 feet, the operators switch the LPI pump suction to the reactor building sump by opening DH-V-6A and 6B, then shutting DH-V-5A and 5B. If the RCS pressure is greater than the shutoff head for the LPI pumps, the LPI system is aligned to inject water to the suction of the HPI pumps by opening DH-V-7A and 7B. After proper flow is verified, the operator then isolates the BWST from the injection pumps. This LPI to HPI injection lineup is referred to as the "piggyback" mode of operation and is also used in the HPI cooling mode upon low-low level in the BWST.

Whenever the LPI pumps are aligned to the reactor building sump as a suction source, the decay heat removal coolers are used to cool the sump water and reject the heat to the decay heat closed cooling water system.

The analysis of the low pressure injection/decay heat removal system is described in detail in Section 14 of the Systems Analysis Report.

A.14 REACTOR BUILDING ISOLATION SYSTEM

The reactor building isolation system closes containment penetrations not required for operation of the engineered safeguards to prevent leakage of radioactive materials to the environment from inside the reactor building or RCS. Leakage through penetrations is minimized by a double barrier so that no single, credible failure oı malfunction of an active or passive component can result in intolerable leakage. The installed double barriers take the form of closed piping systems, both inside and outside the reactor building, and various types of isolation valves.

Four types of isolation valve layouts exist, depending on what type of line is being isolated:

- Each line connecting directly to the reactor coolant system has two reactor building isolation valves. One valve is external and the other is internal to the reactor building. These valves may be either a check valve and a remotely operated valve or two remotely operated valves, depending on the direction of normal flow.

- Each line connecting directly to the reactor building atmosphere has two isolation valves. At least one valve is external and the other may be internal or external to the reactor building. These valves may be either a check valve and a remotely operated valve or two remotely operated valves, depending on the direction of normal flow.

- Each line not directly connected to the reactor coolant system or not open to the reactor building atmosphere has at least one valve either a check valve or a remotely operated valve. This valve is located externally to the reactor building.

- Lines that penetrate the reactor building and are connected to either the building or the reactor coolant system, but that are never opened during reactor operation, have two normally closed barriers; e.g., blind flange and closed valve.

All lines open to the containment atmosphere or connected directly to the RCS (either normally or intermittently that can result in transfer of radioactivity out of containment) that are neither part of the emergency core cooling systems nor support for RCP operation are isolated on reactor trip. Reactor building partial isolation occurs on a signal of approximately 4 psig in the reactor building. A 30-psig signal provides isolation for certain lines not isolated by the 4-psig signal. There are additional containment isolation signals, such as the reactor trip, high radiation, 1,600-psig RCS pressure, and pipeline break signals.

The analysis of the reactor building isolation system is described in detail in Section 15 of the Systems Analysis Report.

A.15 REACTOR BUILDING EMERGENCY COOLING SYSTEM

Reactor building emergency cooling is provided to remove heat from the containment atmosphere to limit stress on the reactor building structure.

Reactor building air recirculation and cooling units work in conjunction with the reactor building spray system during periods when decay heat is being deposited to the containment atmosphere. The systems are designed so that the heat removal capability required during the post-accident period can be attained by operating spray systems and cooling units in the emergency mode in various combinations. (See success criteria discussion in Plant Model Report, Section 4.1.4.)

Long-term reactor building heat removal depends on the operation of the reactor building emergency cooling units or the decay heat removal system since the reactor building spray system cannot remove heat from the reactor building.

Emergency and normal cooling is performed with the same basic units that are components of the reactor building ventilation system. Each unit contains an emergency cooling coil, a normal cooling coil, and a two-speed fan. For emergency cooling, the units will operate at a reduced speed under post-accident conditions, with the heat being rejected to river water. The back-pressure regulating valve on the emergency cooling coil discharge line maintains emergency system pressure above maximum containment design pressure and prevents leakage out of the containment through a damaged system.

Receipt of the reactor building isolation signal (4-psig reactor building pressure or a low reactor pressure of either less than 1,600 psig or less than 500-psig backup signal) automatically switches the reactor building emergency cooling system to the emergency mode. This includes:

1. Energizing the three recirculating air handling units.
2. Operating the three units at the lower speed.
3. Starting the reactor building emergency cooling pumps.
4. Opening the emergency cooling coil isolation valve on the outlet side of the coil. Inlet valves are normally open for leak monitoring purposes.
5. Closing the normal cooling coil isolation valve.

The analysis of the reactor building emergency cooling system is described in detail in Section 16 of the Systems Analysis Report.

A.16 REACTOR BUILDING SPRAY SYSTEM

The reactor building spray system is designed to furnish building atmosphere cooling in conjunction with decay heat removal system operating in the open loop recirculation mode to limit post-accident building pressure and to remove airborne fission products from the reactor building atmosphere, thus reducing the inventory of airborne fission products available for leakage to the environment if the containment should not be isolated or should fail due to overstress. The reactor building emergency cooling system described in Section A.15 above also has containment atmosphere heat removal capability. (See success criteria discussion in Section 4.1.4 of the Plant Model Report.)

The system consists of two pumps, two reactor building spray headers, and the necessary piping, valves, instrumentation, and controls. The pumps and remotely operated valves can be operated from the control room. The reactor building spray system is designed in two trains. Both trains operate independently. A crossover is provided between the two spray train suction lines and contains double manual valves, with a test line for recirculation of borated water from the building spray pumps. Each pump starts, initially taking suction from the borated water storage tank through the interface with the decay heat removal system. The spray is injected into the building atmosphere through a set of spray headers and nozzles for each train.

The analysis of the reactor building spray system is described in detail in Section 17 of the Systems Analysis Report.

A.17 INSTRUMENT AIR SYSTEM

The instrument air system supplies clean, dry, oil-free air at 100 psig throughout the plant for motive control of valves and instrumentation. The instrument air compressors, receivers, and dryer are located in the seismically hardened portion of the intermediate building. One instrument air compressor can supply all the air needed for normal plant operation.

The two instrument air compressors are supplied power from separate class 1E busses; however, the instrument air system is not safety related and, after a loss of offsite power, the compressors have to be manually restarted. When offsite power is available, two service air compressors also supply air to the instrument air system if air pressure drops to 80 psig.

A steam or feed line break in the intermediate building is assumed to cause failure of the instrument air system.

An automatic, heat reactivated air dryer in series with prefilters and afterfilters removes dirt particles and moisture from the air prior to distribution to system loads. If a failure were to occur in the air dryer (plugging or transfer failure), a complete loss of the instrument air system would result unless an operator locally bypasses the dryer using the manual bypass valve.

The 2-hour backup instrument air system has been analyzed separately and included in the analysis for the emergency feedwater system (Section 11 of the Systems Analysis Report); however, the backup instrument air supplied from compressors IA-P-2A and IA-P-2B was not included in the PRA due to the low capacity of these compressors.

The analysis of the instrument air system is described in detail in Section 18 of the Systems Analysis Report.

APPENDIX B

PRA METHODOLOGY

This appendix describes the concept of probability and the probability of frequency framework used throughout this study in Section B.1. Section B.2 introduces some basic concepts and definitions associated with probability distributions. The methods for propagation of the uncertainties represented by the probability distributions in the failure rate data and in the split fraction distributions are discussed in Section B.3.

The methodology details for each part of the PRA model construction process are contained in the corresponding sections of the full report; e.g. the methods followed for incorporating plant-specific data with generic failure rate distributions are described in the Data Analysis Report. Similarly, the methods and conventions followed to build the systems analysis models are described in Section 1 of the Systems Analysis Report, and so on for the other parts of the analysis. Section B.4 of this appendix describes the quantification process that links together the different parts of the PRA model to determine the accident sequences that contribute most to risk. Section B.5 discusses the importance measures used to evaluate the results.

B.1 PROBABILITY*

People have been arguing about the meaning of probability for at least 200 years, since the time of Laplace and Bayes. The major polarization of the argument is between the objectivist or frequentist schools that view probability as something external, the result of repetitive experiments, and the subjectivists who view probability as an expression of an internal state--a state of knowledge or a state of confidence.

In this study, we adopt the point of view that both schools are right; they are just talking about two different ideas. Unfortunately, they both use the same word--which seems to be the source of most of the confusion. We need, therefore, to give each idea the dignity of its own name. We do this by calling one idea frequency and the other probability. In the next section, we shall carefully explain the distinction we make in this study between these two words.

B.1.1 THE DEFINITION OF PROBABILITY AND THE DISTINCTION BETWEEN PROBABILITY AND FREQUENCY

What the objectivists are talking about we shall call frequency. What the subjectivists are talking about we shall call probability. Thus, "probability" as we shall use it is a numerical measure of state of knowledge, a degree of belief, a state of confidence. "Frequency," on the other hand, refers to the outcome of an experiment of some kind

*This section derives, in part, from Reference B-1.

involving repeated trials. Thus, frequency is a "hard" measurable number. This is so even if the experiment is only a thought experiment or an experiment to be done in the future. At least in concept, then, a frequency is a well-defined, objective, measurable number.

Probability, on the other hand, is a notion of a different kind. Defined as a number used to communicate a state of mind, it is thus inherently subjective and changeable as new information arrives. To make this notion useful, we must clearly define the correlation between the numbers and the state of mind.

This can be done in several ways. The most direct, however, is to use frequency in the following way. Suppose we have a lottery basket containing coupons numbered from 1 to 1,000. Suppose the basket is thoroughly mixed and that you are about to draw a coupon blindfolded.

We ask, "Will you draw a coupon numbered 632 or less?" With respect to this question you experience a certain state of confidence. Similarly, I experience a state of confidence with respect to this same question. Let us agree to call this state of confidence, "probability 0.632," equal to the frequency of such draws in an infinitely repeated experiment. Now, we both know exactly what we mean by p = 0.632.

Therefore, if you now say that the probability of your latest business venture succeeding is 0.632, I know exactly what your experiential state of confidence is. We have communicated!

In the same way, we define or "calibrate" the entire probability scale, from zero to one, using frequency as a standard of reference. Note that the process used here is entirely parallel to the way by which we define "red," "chair," "seventeen," and all other words or symbols.

This method of definition shows the intimate connection between probability and frequency. This connection needs to be recognized always and at the same time not allowed to obscure the fundamental difference. Frequency is used to calibrate the probability scale in a "bureau of standards" sense. Once the calibration is established, we then use probability to discuss our state of confidence in areas in which we are dealing with one-time events and have no frequency information at all.

In this way, we liberate ourselves from the restrictions of the relative frequency school of thought (e.g., that only mass repetitive phenomena can be analyzed probabilistically) and instead create for ourselves a systematic, disciplined theory and language for dealing with rare events, for quantifying risks, for making decisions in the face of the uncertainties that are inevitably present in decision situations, and for taking the consequent actions with the knowledge that these are the best decisions and actions possible in light of all the information available to us.

This then is the definition adopted in this report. For additional insight, we quote the following paragraph from unpublished notes by E. T. Jaynes:

> Probability theory is an extension of logic, which describes the inductive reasoning of an idealized being who represents degrees of plausibility by real numbers. The numerical value of any probability (A/B) will in general depend not only on A and B, but also on the entire background of other propositions that this being is taking into account. A probability assignment is "subjective" in the sense that it describes a state of knowledge rather than any property of the "real" world; but it is completely "objective" in the sense that it is independent of the personality of the user; two beings faced with the same total background of knowledge must assign the same probabilities.

As further elaboration, we cite the following paragraph by A. DeMorgan.*

> We have lower grades of knowledge, which we usually call degrees of belief, but they are really degrees of knowledge....
>
> It may seem a strange thing to treat knowledge as a magnitude, in the same manner as length, or weight, or surface. This is what all writers do who treat of probability, and what all their readers have done, long before they ever saw a book on the subject.... By degree of probability we really mean, or ought to mean, degree of belief.... Probability then, refers to and implies belief, more or less, and belief is but another name for imperfect knowledge, or it may be, expresses the mind in a state of imperfect knowledge.

B.1.2 THE DISTINCTION BETWEEN PROBABILITY AND STATISTICS

Corresponding to the above definitions of frequency and probability as numbers, we may say that statistics, as a subject, is the study of frequency-type information. That is, it is the science of handling experimental data. On the other hand, probability as a subject, we might say, is the science of handling the lack of experimental data. Probability is married to risk assessment in PRA, because, without uncertainty, there would be no risk.

Thus, one often hears it said that we cannot use probability because we have insufficient data. In light of our current definitions, we see that this is a misunderstanding. When one has insufficient data, there is nothing else one can do but use probability.

*Further discussion of the foundations of the subjectivistic theory can be found in References B-2 through B-6.

B.1.3 COMMENTARY ON THE DEFINITIONS OF FREQUENCY AND PROBABILITY - AN EXAMPLE

We shall give a simple, tutorial example to further clarify the concept of probability and to indicate how we make the distinction between probability and frequency.

If I tossed a coin and asked you for the probability of it coming up heads, you will of course say .5. If I tell you that I have just tossed the coin 10 times and the frequency of heads was .7 and now ask for the probability of a head on the next toss, you will still very likely say .5. If, however, I tell you that I have tossed it a hundred times and the frequency was .7, 70 heads, you will now begin to suspect that the coin is not equally balanced, and the probability you give for heads on the next toss may move up--say to .6.

If I tell you the frequency has been .7 in 10,000 trials, you will be convinced and will assign a probability of .7 to the next toss.

This example helps bring out the distinction between probability and frequency. The coin has not changed during this example, but your state of knowledge about the coin has--and this is reflected in your changing probabilities from .5 to .6 to .7. On the other hand, I knew the coin was unbalanced to begin with--and my probability was .7 all along.

Which of us was right? Both of us were right. Your probability reflected your state of knowledge and mine reflected mine. As such reflections, both were 100% accurate.

B.1.4 THE MEANING OF "THE" PROBABILITY - RELATION TO THE PHILOSOPHICAL BASIS OF RISK ASSESSMENT

However, what about "the" probability. Here our language plays tricks on us. There is no such thing as "the" probability--as if it were something external--there is only "your" probability, based on the evidence you have and "my" probability based on the evidence I have.

But, you say, suppose we toss the coin N times and plot the frequency of heads, $\phi(N)$, as a function of N. As N gets larger and larger, $\phi(N)$ will approach a limiting value. That value is "the" probability. Well, you could define it so. We find it more useful to call that limiting value "the" frequency--the frequency in an infinite experiment--and reserve the word probability to refer to the state of confidence at any moment. There is another sense, however, in which it can be said that there is a "the" probability. This is in the sense of the last sentence of Jaynes' definition. Any two idealized beings, "rational" beings, given the same total background of evidence and experience must assign the same numerical value of probability to a given proposition. That value could be said to be "the" probability. It is independent of the personality of the user; hence, "objective."

Thus, if you and I are both ideal beings, with the same knowledge, each of us is acting rationally, coherently or objectively (to the extent that our probability assignments follow the formalized rules of the theory of probability), then we will both assign the same probabilities. If we do not assign the same probabilities, then either one or both of us is not coherent, or we do not have the same total background of evidence and information.

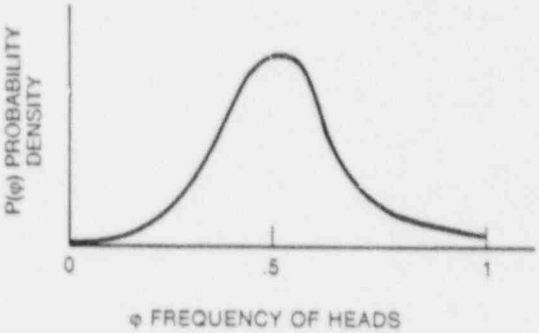
This idea of rationality or coherence is the philosophical cornerstone of our approach to risk assessment. For, if two rational beings, given the same body of information, will evaluate probabiiities the same way, then by our definition, they will also evaluate risk the same way. Thus, a given specific body of information will imply and require a specific quantitative value of risk, and this value is objective and independent of who evaluates it.

B.1.5 TWO METHODS FOR DISCUSSING UNCERTAINTY: THE "PROBABILITY OF FREQUENCY" FRAMEWORK

There are two basic methods for quantifying uncertainty, corresponding to two different questions. We illustrate these in the context of another coin flipping example. In "Method 1" we ask, "What is the probability of a head on the next toss, P(heads)?" Alternately, in "Method 2" we say, "I am going to toss the coin 10,000 times. What is the frequency (i.e., the percentage of heads, ϕ) going to be?"

In Method 1, we answer simply with a number, P(heads), our state of confidence on the prospect of a head on the next toss, as reflected for example in the odds we would take in a bet.

In Method 2, we are asked to predict the outcome, ϕ, of an experiment to be done in the future. Since we do not know this outcome, we express our prediction in the form of a probability curve against frequency; e.g.,



Thus, in the second method, we are led to the notion of a probability curve against frequency as a way of, or a framework for, expressing our state of knowledge about this as yet unperformed experiment.

This notion of probability of frequency and this distinction between Method 1 and Method 2 are central to the understanding of this study. Both methods will be used as appropriate. They are discussed further in later sections and will be of use to us in the next section in extending the definition of risk. We therefore expand our notation. The

Method 1 result can be derived from the Method 2 probability of frequency curve. The Method 2 probability of frequency curve $p(\phi)$ can be used to express our Method 1 probability of heads on the next try as

$$p(\text{head}) = \int_{0}^{1.0} \phi p(\phi) d\phi$$

We see thus that the second method includes or encompasses the first. The reverse cannot be said. Thus, Method 2 is a fuller, more complete way of talking about uncertainty.

Once a probability has been calculated, people inevitably ask, "How accurate is that probability?" "How confident are you in that number?" In response to such questions, authors of probabilistic risk assessments have been led to introduce such notions as confidence bounds on the probability and probability of probability, etc.

In the context of our definition, such phrases as "probability of probability" or confidence in confidence make no sense. In view of our usage of the term probability, the probability of frequency curves expresses our state of confidence. It thus appears as if the question is asking, "How confident are you in your state of confidence?" In this form, the question seems undefined and unanswerable. However, there is a valid thought behind it. What we need to do, therefore, is to expand our framework somehow in such a way that, within the enlarged framework, the question can be given a precise meaning and then be answered.

For this purpose, we make use of the probability of frequency idea in the following way. We imagine a thought experiment in which we undertake the proposed course of action, or inaction, many, many times. At the end of this experiment, we will be able to look back at the records and ask, "How frequently did scenario s_i occur?" This frequency will then be an experimentally measured number. Let us denote it by ϕ_i. Its units are occurrences per trial.

Imagine now, that the scenarios have been arranged in order of increasing severity of damage. That is to say, the damages X_i obey the ordering relationship

$$X_1 \; X_2 \; X_3 \; . \; . \; . \; X_N$$

If we now plot the points $<x_i,P_i>$, we obtain the staircase function shown as a dashed line, in Figure B-1.

If we draw in the smoothed curve, R(x), through the staircase, we can regard that curve as representing the actual risk. Hence we call it the risk curve.

Probably, the best known examples of such curves were published in the Reactor Safety Study, WASH-1400 (Reference B-2). Figure B-2 is an example taken from that study. Note in this example that the curves are plotted on log-log scale, which results in the characteristic concave downward shape. In this case, the asymptotes, as shown in Figure B-3, have the interpretation of maximum possible damage and probability of any damage at all.

We could then compute the cumulative frequency

$$\Phi = \sum_{x_j \geq x_i} \phi_i$$

(where the sum is over all scenarios having damage equal to or greater than x_i). We could now plot Φ versus x, obtaining Figure B-4, which we refer to as a risk curve in frequency format. This whole curve may be regarded as the outcome of our thought experiment.

The scenario frequencies and the damage associated with each scenario are constructed by combining probability of frequency distributions for each event in the scenario. The propagation of uncertainty process described in Section 4 of the this report (TSR) and Section B.3 result in $p(\phi_i)$ and $p(X_i)$ distributions for the frequency and consequences of each scenario i, respectively. Therefore, the cumulative frequency Φ_j of all scenarios having damage X_j or greater has associated with it a $p(\Phi_j)$ also. This means we are producing a family of curves $p(\Phi_j, x_i)$, represented pictorially by a "risk" curve in probability of frequency format. At each damage level on such a risk curve a vertical cut through the family looks like a probability of frequency curve.

Pictorially, this is represented by a diagram of the form of Figure B-5. This figure is what we call a risk curve in probability of frequency format. It consists of a family of curves, $\Phi_P(x)$, with the parameter being the cumulative probability. To use this diagram, we would, for example, enter with a specific x value and choose, say, the curve $P = 0.90$. The ordinate of this curve, $\Phi_{0.90}(x)$, is then the 90th percentile frequency of x. That is to say, we are 90% confident that the frequency with which damage level x or greater occurs is not larger than $\Phi_{0.90}(x)$.

B.1.6 THE DISTINCTION BETWEEN FREQUENCY DISTRIBUTIONS AND PROBABILITY DISTRIBUTIONS

We now use our definitions to distinguish two further situations that are often badly confused.

Let x denote the height of an individual person selected at random from a population. If we now measure the height of each person, we can draw a frequency distribution showing what fraction of the population falls in each height increment. If the population is large, we can, by a limiting process, express this distribution as a continuous curve, a frequency density distribution $\phi_x(x)$, as shown in Figure B-6.

The units of the $\phi_x(x)$ are thus frequency per unit x, or fraction of population per unit height. This curve is an experimental quantity. It portrays the variability of the population--a measurable quantity. The value of x therefore varies with the individual selected. It is a truly fluctuating or random variable.

Now, contrast the situation for which we pick a specific individual (say, Joe) in the population and ask what his height, x_{Joe}, is. Since we do not know his height for sure, we express our state of knowledge about it in the form of a probability density function, as in Figure B-7.

The units here are probability per unit height. In this case, x_{Joe} is not a random or fluctuating variable. x_{Joe} is a definite number. It is just that we do not know what it is. This is a very different situation from the situation shown on the population variability curve. Thus, ϕ_x is the frequency distribution of a random, or fluctuating, variable. $P(x_{JOE})$ is the probability distribution for a fixed, nonfluctuating, but unknown quantity.

This distinction between population variability curves and state-of-knowledge curves must be made when we analyze data on failure rates and initiating event frequencies from our specific plant and from other plants and other industries.

B.2 PROBABILITY DISTRIBUTIONS - BASIC CONCEPTS

Probability distributions are, of course, fundamental to any discussion of risk and are used extensively throughout this study. For convenience, therefore, this section collects and reviews some of the basic ideas and standard language relating to such distributions.

B.2.1 DISTRIBUTION FUNCTIONS

Given an uncertain variable X and a number x, the notation $X < x$ represents the hypothesis that X has a value less than or equal to x. The (cumulative) probability distribution function, $P(x)$, of the variable X is now defined as

$$P(x) \equiv \text{probability } (X < x) \tag{B.1}$$

This definition applies to both discrete variables (i.e., variables that take on a countable number of values) and continuous variables. Frequently, we wish to have more detailed information than that provided by Equation (B.1). In particular, for a discrete variable, we may wish to know the probability that $X = x$ and, for a continuous variable, the probability that X falls between x and $x + dx$. Thus, we define the probability function for a discrete variable,

$$p(x_j) = \text{probability } (X = x_j)$$

and the probability density function for a continuous variable

$$p(x) \equiv \frac{dP(x)}{dx}$$

The density function satisfies

$$\int_{-\infty}^{\infty} p(x)dx = P(\infty) - P(-\infty) = 1-0 = 1 \tag{B.2}$$

and the cumulative probability distribution function is calculated from

$$P(x) = \int_{-\infty}^{x} p(s)ds \qquad (B.3)$$

(The integrals in Equations (B.2) and (B.3) are replaced by sums when X is discrete.)

As an example of the above, let T be the time at which a particular piece of equipment first fails and let

$P(t)$ = probability that $T \leq t$

Then,

$$R(t) = 1-P(t)$$

known as the "reliability," is the probability that the equipment has not failed by time t.

The probability density function

$$p(t) = \frac{dP(t)}{dt} \qquad (B.4)$$

is the probability of failure, per unit time, at t. The "failure rate," or "hazard function," $\lambda(t)$ is defined as

$$\lambda(t) = \frac{p(t)}{R(t)} = \frac{1}{1-P(t)} \left[\frac{dP(t)}{dt}\right]$$

The interpretation of the failure rate is that $\lambda(t)dt$ is the conditional probability that the equipment will fail in dt about t, given that it has not failed up until time t.

We now examine briefly several widely used standard distributions of discrete and continuous types, which are frequently encountered in risk analysis work. First, however, we will define some characteristics that all distributions have.

B.2.2 MEASURES OF CENTRAL TENDENCY AND DISPERSION

We have suggested that a convenient way to express our state of knowledge about a random variable is to use a probability distribution. While a distribution gives in detail all that we know about the variable, it may be convenient to characterize the distribution by using one or more values that reflect its central tendency and its dispersion. Combining such values instead of the actual curve may also be useful as a first approximation method of combining distributions.

The most widely used measure of central tendency is the expected value (or mean), which is defined as

$$\alpha \equiv E[X] \equiv \begin{cases} \int_{-\infty}^{\infty} xp(x)dx \\ \text{or} \\ \sum_i x_i p_i \end{cases} \qquad (B.5)$$

according to whether x is continuous or discrete.

If the density function is interpreted as a mass distribution, then the expected value corresponds to the center of gravity. Besides the mean, there are two other measures of central tendency, the mode, and median.

The mode (or most likely value) is defined for a discrete variable as the value for which p_i is greatest and for a continuous variable as the value at which the density p(x) is maximum.

The median is defined as that point x_{50} for which

$$P(x_{50}) = 0.50 \qquad (B.6)$$

Thus,

$$\int_{-\infty}^{x_{50}} p(x)dx = 0.50 \qquad (B.7)$$

or for a discrete variable

$$\sum_{x_i \le x_{50}} p_i = 0.50 \qquad (B.8)$$

The percentile x_γ is defined as

$$P(x_\gamma) = \frac{\gamma}{100} \qquad (B.9)$$

From Equation (B.7), we see that the median is the 50th percentile. Two percentiles that are often used to indicate how broad the distribution is are the 5th and 95th percentiles, which are determined by Equation (B.8), with γ = 5 and 95, respectively.

A measure of dispersion is the variance (and its square root, the standard deviation). It is defined to be the second moment about the mean; that is,

$$\beta^2 \equiv E(X-\alpha)^2 \equiv \begin{cases} \int_{-\infty}^{\infty} (x-\alpha)^2 p(x)dx \\ \text{or} \\ \sum_i (x_i-\alpha)^2 p_i \end{cases} \tag{B.10}$$

The variance is related to the mean and the second moment about zero by

$$\beta^2 = E[X^2] - \alpha^2 \tag{B.11}$$

hence,

$$E[X^2] = \alpha^2 + \beta^2 \tag{B.12}$$

This equation states that the mean of the square of a random variable is equal to the square of the mean of the variable plus its variance. This observation will be useful later in the quantification of fault trees.

B.2.3 DISCRETE DISTRIBUTIONS

B.2.3.1 Binomial

The binomial distribution is applicable when an experiment can have only two outcomes; e.g., success or failure, such as in the case of a diesel generator either starting or not. Let us say the frequency of failure is f and of success, 1 - f, and that an experiment is repeated n times. The following function p(r), then, gives the probability of exactly r failures in n trials, i.e.,

$$p(r) = \frac{n!}{r!\,(n-r)!} f^r(1-f)^{n-r} = \binom{n}{r} f^r(1-f)^{n-r} \tag{B.13}$$

B.2.3.2 Poisson

Items of equipment that operate continuously, pumps for example, are usually modeled as having a failure rate, λ, that is constant in time. In this case, the probability of having exactly k failures in t operating hours is given by

$$p(k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t} \tag{B.14}$$

Viewed as a function of k, this expression is known as the Poisson distribution.

B.2.4 CONTINUOUS DISTRIBUTIONS

B.2.4.1 Normal (Gaussian)

The Gaussian distribution, or normal curve of error, is fundamental in probability work.

The density function of this distribution is

$$p(x) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right] , -\infty < x < \infty \qquad (B.15)$$

To get the standardized (tabulated) normal distribution, define the new variable

$$z \equiv \frac{x-\mu}{\sigma} \qquad (B.16)$$

in which case, Equation (B.7) becomes

$$p(z) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left[-\frac{z^2}{2}\right] \qquad (B.17)$$

Tables for the standardized distribution can be found in many textbooks (References B-7 and B-8).

B.2.4.2 Exponential

Referring back to the Poisson (or constant failure rate) process, set k = 0. Then, the probability of zero failures up to time t is

$$R(t) = e^{-\lambda t} \qquad (B.18)$$

The density function is

$$p(t) = \lambda R(t) = \lambda e^{-\lambda t} \qquad (B.19)$$

which, we notice, has units of probability per unit time.

The cumulative distribution is

$$P(t) = 1 - e^{-\lambda t} \approx \lambda t \qquad (B.20)$$

where the approximation holds for $\lambda t \leq 0.10$. The implications of this approximation when uncertainties are propagated will be discussed in later sections.

B.2.4.3 Lognormal

The lognormal distribution is used extensively in risk and reliability work and is relevant in more physical processes where the underlying variable is restricted to positive values; i.e., 0 to ∞. In the present study, as in past safety studies, the lognormal is used to represent our state of knowledge of component failure rates and also to represent the variability, or frequency distributions, of populations of components.

The density function for the lognormal is

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma x} \exp\left[- \frac{(\ell n\ x-\mu)^2}{2\sigma^2}\right] \ , \ 0 < x < \infty \tag{B.21}$$

Comparison of Equations (B.15) and (B.21) reveals that if x is lognormally distributed, then $\ell n\ x$ is normally distributed.

Very often in risk analysis, the primary variables are assumed to be lognormally distributed. It is of interest, then, to investigate some useful properties of that distribution in the present context.

The lognormal density was given in Equation (B.21). Note that this form contains two parameters, μ and σ. We sometimes write

$$x \simeq \Lambda(\mu,\sigma)$$

to mean that x is lognormally distributed with parameters μ and σ.

Several characteristic values of the distribution are as follows:

$$\text{Mean:} \qquad \alpha = \exp\left(\mu + \frac{\sigma^2}{2}\right) \tag{B.22}$$

$$\text{Variance:} \quad \phi^2 = e^{2\mu + \sigma^2}\left[e^{\sigma^2} - 1\right] = \alpha^2\left[e^{\sigma^2} - 1\right] \tag{B.23}$$

$$\text{Mode:} \qquad X_m = \exp\ (\mu-\sigma^2)$$

Inverting Equations (B.22) and (B.23), we get the parameters μ and σ as functions of the mean and variance; i.e.,

$$\sigma^2 = \ell n\left[\frac{\phi^2}{\alpha^2} + 1\right] \tag{B.24}$$

$$= \ell n\alpha - \frac{\sigma^2}{2} \tag{B.25}$$

Useful percentiles of the lognormal are:

$$\text{5th Percentile:} \quad x_{05} = \exp\ (\mu - 1.645\sigma) \tag{B.26}$$

$$\text{50th Percentile (median):} \quad x_{50} = e^{\mu} = \sqrt{x_{05}x_{95}} \tag{B.27}$$

95th Percentile: $x_{95} = \exp(\mu + 1.645\sigma)$ (B.28)

γ Percentile: $x_\gamma = \exp(\mu + k_\gamma\sigma)$ (B.29)

where k_γ is the appropriate coefficient found in tables of the standard normal distribution. The error factor (EF) is defined as

$$EF = \sqrt{\frac{x_{95}}{x_{05}}} = e^{1.645\sigma} \tag{B.30}$$

It follows immediately that

$$x_{95} = x_{50}EF \tag{B.31}$$

and

$$x_{05} = \frac{x_{50}}{EF} \tag{B.32}$$

Since $\ell n\ x$ is normally distributed, the most convenient way to look at a lognormal distribution is to write

$$x = me^{\sigma z} \tag{B.33}$$

When z in Equation (B.33) is a standard normal variate, then x is lognormally distributed; m is the median value of x and σ is called the lognormal standard deviation, or the "multiplicative" standard deviation. The reason for the latter term is seen in Equation (B.33) from the fact that if we increase z by the additive amount, 1.0, then x increases by the multiplicative factor e^σ. Thus, the multiplier e^σ plays the same role in a lognormal curve as the additive quantity σ plays in a normal curve. That is, when x changes by the factor e^σ, the cumulative probability changes by one standard deviation worth.

Two important properties of the lognormal distribution are (see Reference B-8):

- Property 1. If

  $$X = \Lambda(\mu_X, \sigma_X)$$

  and

  $$Y = C_1 X^{C_2}$$

  where C_1 and C_2 are constants, then

  $$Y = \Lambda(\mu_y, \sigma_y) \tag{B.34}$$

where

$$\mu_y = C_2\mu_x + \ell n\ C_1 \tag{B.35}$$

$$\sigma_y = C_2\sigma_x \tag{B.36}$$

This property simply states that if a lognormal variable is multiplied by a constant and raised to a power, the resulting variabl. will also be lognormal with parameters given by Equations (B.35) and (B.36).

We can easily prove this property by using Equation (B.33) to get

$$Y = C_1 m_x^{C_2}\ e^{C_2\sigma_x z} \tag{B.37}$$

Equation (B.37) states that Y is also lognormal with median

$$C_1 m_x^{C_2}$$

and lognormal standard deviation $C_2\sigma_x$. From Equation (B.27), we then get

$$C_1 m_x^{C_2} = e^{\mu_y} \tag{B.38}$$

and Equation (B.35) follows immediately.

- Property 2. If

$$X = \Lambda(\mu_x, \sigma_x)$$

and

$$Y = \Lambda(\mu_y, \sigma_y)$$

are independent, lognormally distributed variables, and

$$V = X \cdot Y \tag{B.39}$$

then,

$$V = \Lambda\left(\mu_x + \mu_y,\ \sqrt{\sigma_x^2 + \sigma_y^2}\right) \tag{B.40}$$

Using Equation (B.33), we get

$$V = m_x m_y \exp\ (\sigma_x z_x + \sigma_y z_y) \tag{B.41}$$

Since the sum of two normal curves is a normal curve, we have

$$\sigma_x z_x + \sigma_y z_y = \sigma_v z_v \tag{B.42}$$

where

$$\sigma_V = \sqrt{\sigma_x^2 + \sigma_y^2} \qquad (B.43)$$

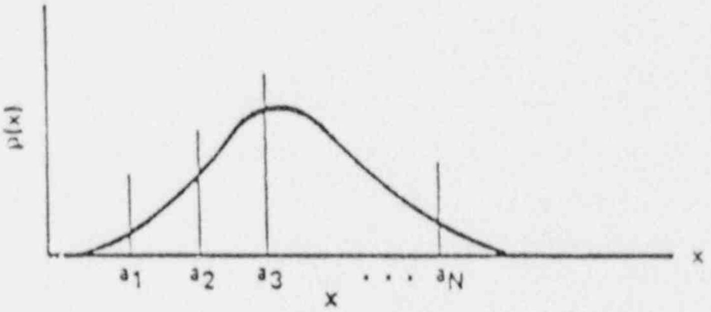
Thus, from Equation (B.41) we see that V is a lognormal variate with median $m_x m_y$ and lognormal standard deviation, Equation (B.43). Therefore, Equation (B.40) is proved.

These properties of the lognormal distribution will be used later in the quantification of system unavailabilities.

B.2.5 DISCRETE APPROXIMATIONS TO CONTINUOUS DISTRIBUTIONS

Continuous distributions are, of course, the tools that we use to express our state of knowledge about continuous variables. For purposes of numerical calculation, however, it is convenient to approximate these continuous models by discrete distributions. This discretization is, of course, similar to the procedures used in evaluating integrals by numerical quadrature.

Consider the following distribution, p(x), of the continuous variable x.



If we wish now to get a discrete approximation to p(x), we can do this simply by carving x up into intervals as shown in the figure. The idea is to assign the probability that x will fall in an interval (a_{i-1}, a_i) to a single point x_i inside that interval. This probability, say p_i, is simply

$$p_i = \int_{a_{i-1}}^{a_i} p_x(x)dx \qquad (B.44)$$

We can determine the points x_i in various ways. For example, x_i can be the mean value of the points in each interval. Thus, with the understanding

$$a_0 = -\infty, \qquad a_{N+1} = +\infty, \qquad (B.45)$$

we determine

$$x_i = \frac{1}{p_i} \int_{a_{i-1}}^{a_i} xp_x(x)dx. \qquad (B.46)$$

A second method is to simply take x_i as the midpoint of the interval, i.e.;

$$x_i = \frac{a_i + a_{i-1}}{2} \qquad (B.47)$$

or

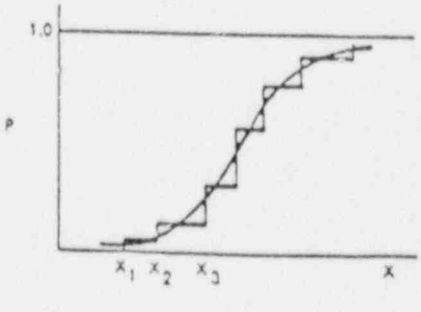
$$x_i = \sqrt{a_i a_{i-1}} \qquad (B.48)$$

In this case, we cannot use Equation (B.45). However, it will be satisfactory to choose a_0 and a_{N+1} appropriately so that the probability that x falls outside the interval (a_0, a_{N+1}) will be negligibly small. With these finite values of a_0 and a_{N+1}, Equation (B.47) or (B.48) can be applied to all intervals.

The points x_i may also be determined using any other reasonable method that facilitates the calculations (since this is the major reason for the discretization). For example, if the lognormal distribution, Equation (B.21), is to be discretized, it will be convenient to take advantage of its relation to the normal distribution and the fact that the normal is tabulated. Thus, we work with the logarithm of x, and we discretize the normal distribution and then switch back to the lognormal by taking exponentials.

The accuracy of the discretization increases as the number of intervals increases; i.e., for N large. The intervals do not have to be of equal length.

The above discussion has shown how to develop a discrete distribution from a continuous one. The reverse of this process, obtaining a continuous distribution from a discrete one, is simply a matter of "fitting" or "smoothing." A convenient way to do this is to plot the discrete distribution, in cumulative form, as a step function and then smooth in a sigmoid shape as shown below. This smoothed shape can then be differentiated graphically to obtain a density function.



B.3 PROPAGATION OF UNCERTAINTIES, THE METHOD OF MOMENTS, AND THE METHOD OF DISCRETE PROBABILITY DISTRIBUTIONS

The probability of frequency, $P(\phi_i)$, of each scenario, S_i, is calculated by combining probability of frequency distributions for each of the number of individual events (usually system failures) that define (make up) the scenario.

$$P(\phi_i) = f[P(\phi_{e_1}, P(\phi_{e_2}), \ldots P(\phi_{e_{N_i}})] \tag{B.49}$$

where N_i is the number of events in scenario i.

Having determined the function f (i.e., the events and the way they are combined) from the plant model, the next step is to combine the distributions, $P(\phi_k)$, to get the distribution $P(\phi_i)$. This step is known as the "propagation of uncertainties" for the frequency of scenario i.

For any arbitrary function f, a simple analytical form for the distribution $P(\phi_i)$, of course, does not exist. However, simplifying numerical methods do exist. Among these are the Monte Carlo method (Reference B-9), the method of moments (Reference B-10) and the method of discrete probability distributions (Reference B-11). The method most widely used in this study is the Monte Carlo method. As background for the discussion of this method, we first review the analytical expressions for combining two continuous and independent probabilistic variables and the method of discrete probability distributions.

Propagation of uncertainties using discrete probability distribution arithmetic becomes cumbersome when the number of equations and variables is large. This complexity stems from two sources. The first source of complication is that probabilistic operations are nondistributive for the multiplication operation over addition. This means that the order in which multiplication and addition are performed can affect the final results. A second source of complexity is the manner in which the resultant discrete distribution tends to have many more points than either of the two distributions involved in the operation. This complication can be resolved by condensation of the resultant distribution into a smaller number of discrete points although this condensation process can introduce some additional approximations. It is the first source of complexity, the requirement for correctly sequencing the arithemetic operations, that is the greatest limitation.

B.3.1 COMBINING PROBABILITY DISTRIBUTIONS, ANALYTIC, OR CONTINUOUS VARIABLE CASE

Let x and y be independent variables having the probability density functions $p_x(x)$, $p_y(y)$. If $z = x + y$, then the density function for z is expressed by the convolution integral

$$p_z(z) = \int_{-\infty}^{\infty} p_x(x) p_y(z-x) dx \tag{B.50}$$

Similarly, if

$$z = x\,y \tag{B.51}$$

then

$$p_z(z) = \int_{-\infty}^{\infty} p_x(x) p_y(\tfrac{z}{x})\,\frac{1}{x}\,dx \tag{B.52}$$

(with any ambiguity at x = 0 handled by limit operations from both sides in the obvious way).

More generally, let

$$z = f(x,\ y) \tag{B.53}$$

where, for any specific values of z and x, y has a specific value denoted by

$$y = f^{-1}(z,\ x); \tag{B.54}$$

that is

$$z \equiv f[(x,\ f^{-1}(z,\ x)] \tag{B.55}$$

Then

$$p_z(z) = \int_{-\infty}^{\infty} p_x(x) p_y[f^{-1}(z,x)]\,\frac{\partial}{\partial z}\,f^{-1}(z,\ x)dx \tag{B.56}$$

which may be thought of as a more general form of convolution. Again, there are obvious further generalizations possible, but this is sufficient for our purposes.

In real-life applied work, we rarely have the luxury of dealing with analytic forms and even in those rare cases may be unable to perform the integrations [Equation (B.56)] analytically. We are therefore led to seek approximate procedures.

B.3.2 THE METHOD OF DISCRETE PROBABILITY DISTRIBUTIONS

The method of discrete probability distributions is used extensively in this study. We therefore give a fairly complete exposition as follows.

B.3.2.1 Discrete Probability Distributions

Let x be an ordinary scalar variable and let x_1, x_2, ..., x_n denote particular discrete values of x. Let p_1, p_2, ..., p_n be associated probability values so that

$$\sum_{i=1}^{n} p_i = 1 \tag{B.57}$$

Then, the set of doublets,

$$<p_1, x_1>, <p_2, x_2>, \dots <p_n, x_n> = \{<p_i, x_i>\} \qquad (B.58)$$

may be called a DPD and may be thought of as a discrete approximation to a continuous probability density function $p(x)$.

More fundamentally, we need not introduce $p(x)$ and may instead regard the DPD directly as an expression of our state of knowledge with respect to variable x. This is the point of view we shall take from here on.

We shall sometimes also refer to a set of doublets, Equation (B.58), as a probability "histogram." This usage, however, is explicitly not intended to suggest that the x_i should be regularly spaced. On the contrary, coming from the point of view of the previous paragraph, we allow ourselves total freedom to select the x_i and p_i any way at all, save only that the set $\{<p_i, x_i>\}$ adequately represents our state of knowledge and that it is suited to the numerical procedures we have in mind.

Thus, for example, suppose we were particularly interested in low values of x; i.e., in the low-side tail of the distribution. We would then place several of the x_i within this low-side tail, even though the corresponding p_i was small. In this way, we would ensure that the low values of x would be appropriately represented in our subsequent calculations.

B.3.2.2 Probabilistic Addition

Suppose the variables x, y, z are related by

$$z = x + y \qquad (B.59)$$

and suppose our state of knowledge with respect to x and y is expressed by the DPDs

$$x = \{<p_i, x_i>\}, \; y = \{<q_j, y_j>\} \qquad (B.60)$$

Moreover, suppose these states of knowledge are independent in the sense that, if we found out the true value of y, this would not affect our DPD for x, and vice versa.

For this situation, we may now define the operation of addition of two DPDs as follows

$$\{<p_i, x_i>\} + \{<q_j, y_j>\} = \{<p_i q_j, x_i + y_j>\} \qquad (B.61)$$

We now regard the set of doublets on the right as a DPD representing our state of knowledge of the variable z.

$$z = \{<r_{ij}, z_{ij}>\}$$

where

$$r_{ij} = p_iq_j, \; z_{ij} = x_i + y_j$$

Equation (B.61) then is our algorithm for probabilistic addition. It may be regarded as a discrete analog to the convolution operation, Equation (B.50). As an example of this algorithm, if

$$x = \{<.1, -1> <.5, 1> <.4, 2>\}$$

$$y = \{<.2, 5> <.8, 10>\}$$

the'

$$z = \{<.02, 4> <.1, 6> <.08, 7> <.08, 9> <.4, 11> <.32, 12>\}$$

B.3.2.3 Probabilistic Multiplication

Similarly, we define multiplication of DPDs as

$$\{<p_i, x_i>\} \{<q_j, y_j>\} = \{<p_iq_j, x_iy_j>\} \tag{B.62}$$

Thus, if

$$z = xy$$

then,

$$z = \{<r_{ij}, z_{ij}>\} \tag{B.63}$$

with

$$r_{ij} = p_iq_j, \; z_{ij} = x_iy_j \tag{B.64}$$

As an example, let us take the x and y of the previous paragraph. Then, z is the set of doublets,

$$z = \{<.02, -5> <.1, 5> <.08, 10> <.08, -10> <.4, 10> <.32, 20>\}$$

Equation (B.64) is the discrete analog of Equation (B.52). In a similar way, we can write the discrete version of Equation (B.56). We summarize all this in the following section.

B.3.2.4 General Rule of Probability Arithmetic for Binary Operations

If

$$z = f(x, y) \tag{B.65}$$

where x, y are the independent DPDs,

$$x = \{<p_i, x_i>\}, \; y = \{<q_j, y_j>\} \tag{B.66}$$

then z is the DPD,

$$z = \{<r_{ij}, z_{ij}>\} \qquad (B.67)$$

where

$$r_{ij} = p_i q_j, \; z_{ij} = f(x_i, y_j) \qquad (B.68)$$

We note in passing that

$$\sum_{ij} r_{ij} = 1.0$$

so that Equation (B.67) is a bona fide DPD. We also note that obtaining the DPD for z is a simple matter of two nested "do loops" on a computing machine. We finally note the straightforward generalization to the case of more than two arguments in f. That is, if

$$z = f(x^1, x^2, \ldots x^M) \qquad (B.69)$$

where each x^m is a DPD

$$x^m = \{<p^m_{i_m}, x^m_{i_m}>\}, \qquad (B.70)$$

then z is the DPD

$$z = \{<r_{i_1 \ldots i_M}, z_{i_1} \ldots z_{i_M}>\} \qquad (B.71)$$

where

$$r_{i_1 \ldots i_M} = \prod_{m=1}^{M} p^m_{i_m} \qquad (B.72)$$

$$z_{i_1 \ldots i_M} = f \; x^1_{i_1}, x^2_{i_2}, \ldots x^M_{i_M} \qquad (B.73)$$

If the number of variables here, M, is large, and f is complicated, then the DPD approach, Equation (B.73), becomes computationally burdensome. At this point, the Monte Carlo approach becomes more feasible.

B.3.3 MONTE CARLO ERROR PROPAGATION

Monte Carlo error propagation is used in this study to quantify all system and plant model equations. Monte Carlo error propagation does not require that the arithmetic operations be carefully sequenced to avoid introducing dependencies between distributions, and the number of variables, which can be easily combined, is very large.

The Monte Carlo technique of simulating probability distributions is based on mapping uniform, random deviates through a continuous cumulative distribution function [CDF(x)], normalized to 1.0, as illustrated in Figure B-8. For every random value of y on the interval [0, 1], there corresponds a value of x on the interval [a, b]. Assuming a uniform density of random deviates on the ly-axis, n, the total number of random deviates on any interval dy, is simply ndy. The corresponding interval on the x-axis then has density ndy/dx. Since the probability density function of a random variable is proportional to the derivative of the corresponding CDF, this method of mapping uniform deviates through the CDF in effect simulates the PDF of the random variable.

After obtaining a random sample for each input variable according to its pecified PDF, these samples can then be combined according to the equations that describe the output function to obtain a random sample from the output distribution. This process is then repeated many times as part of the Monte Carlo sampling process. These samples can then be sorted and evaluated statistically to determine the parameters of the resultant distribution and its CDF. The PDF of the resultant distribution is also provided, usually in histogram form.

The Monte Carlo sampling process does introduce slight errors in the computation of the output distribution. With a suitable number of samples, however, this error can be limited to very manageable levels. Estimates of the error in the sample output distribution percentiles and in the first and second moments can be evaluated statistically to ensure that the error is not significant.

For this study, the continuous input variable distributions are first approximated by discrete probability distributions tjat preserve the means of the original, continuous distributions. Consequently, all failure rate data are approximated by discrete distributions when propagating the uncertainties in the system models for each of the split fractions. The split fraction probability of frequency distributions are then also approximated by discrete distributions when computing the probability of frequency distributions for each plant damage state and for the total core melt frequency.

B.4 QUANTIFICATION OF THE PRA MODELS

The results from the quantification of the TMI-1 PRA models are the core damage frequency, the plant damage state probability of frequency curves and the dominant contributors to the magnitude of the core damage frequency. The magnitude of the risk is determined by several analyses that are combined using a variety of special purpose computer programs.

Figures B-9 through B-12 show the different computer programs and how they interact to complete the quantification process. The number in the upper left corner of each box in the figures will be referenced in the following text to orient the reader to the overall process. The quantification process is divided into five analysis areas: system analysis, support system event sequence analysis, frontline system event sequence analysis, seismic analysis, and the analysis of fires, floods and external events. This breakdown of the analysis activities is not a distinct separation of effort and work functions, but rather is a general division of activities in which there is some degree of interaction in working toward a common goal. This breakdown of the total analysis effort is consistent with the work breakdown structure followed in the creation of the PRA models.

B.4.1 SYSTEM ANALYSIS QUANTIFICATION

The many system analysis models are documented in the System Analysis Report. Results from the quantification of these models are also provided in that report. These results were generated using the RISKMAN3 computer program; i.e., Reference B-12. Once the system algebraic equations (data base S2) and component failure rates data base (i.e., block S1 in Figure B-9) have been prepared for the RISKMAN3 program, the system analysis models can be easily quantified.

- Data Base S1. The failure rate data base, S1, consists of the distributions associated with maintenance frequencies and durations, human error rates, and all initiating event frequencies that are derived directly from experience data and common cause failure model parameters.

- Computer Code S3. The RISKMAN3 program can compute the split fractions for the systems analyses models. Both a point estimate and a Monte Carlo quantification option are provided. The point estimate quantification uses the mean values from the data base variable distributions. The resulting split fraction values are approximations to the mean value of the split fraction distributions. The accuracy of the point estimate approximation to the mean is dependent on the form of the split fraction equations. The point estimate quantification is a fairly close approximation of the mean, provided the equations do not contain variable squared or cubed terms. The Monte Carlo calculation also updates the CSF.RM3 file, which contains the distributions for each split fraction.

  Since the system equations generally do contain such terms, the final mean values of the split fraction distributions are computed using the RM3 Monte Carlo quantification option. The point estimate quantification is used only for debugging the split fraction equations. The results presented in the Systems Analysis Report for each system are the mean values computed using the Monte Carlo option of RISKMAN3.

- Data Base S4. The mean values for each split fraction are stored in a file known as the master frequency file (MFF.RM3). The master frequency file is used when quantifying the accident sequence frequencies, which are discussed in the next section.

- Data Base S5. When the Monte Carlo option of RM3 is used, the complete distribution for the split fractions is also computed in addition to the mean value. The complete probability of frequency distributions for these split fractions are also stored in a file (CSF.RM3) for subsequent propagation of uncertainties through the most dominant scenarios (100 for TMI-1 PRA) of data base E14, using RM5.

B.4.2 SUPPORT SYSTEM EVENT SEQUENCE ANALYSIS

This section and the following ones discuss how the system split fractions described in the previous section are used as input in the quantification of the plant model event trees and in the propagation of uncertainties for the key accident sequences. The first stage of the plant model, the support model event tree, is discussed here and displayed in Figure B-10.

- Data Base P1. The construction of the support system model begins with the preparation of intersystem dependency tables. Both the support-to-support system dependency table and the support-to-frontline system dependency table are used as input. These tables are provided in Section 3 of the Plant Model Report.

- Computer Code P2. The support model event tree structure is prepared, based on the input from P1 and other knowledge of the operation of the support systems. The ETC9 program (See Reference B-13) can be used in the event tree drawing mode to help in this process. The event tree structure input consists of top event definitions, the top event number at each branch, the end state for each branch, and the branches involved in each instance of repeated tree structure logic; i.e., transfers. The support tree structure is then printed out for analyst review. The analyst reviews the tree structure and modifies it if necessary. After the tree structure is finalized, the appropriate split fractions are assigned to each branch point in the tree for the case in which the initiating event does not disable a support system for the turbine trip initiating event.

- Data Base P3. A support system ETC9 input file is prepared for the turbine trip initiating event. The tree structure and assignment of split fractions from the master frequency file (data base S4) is prepared. The analyst is also required to prepare a table that defines the impacts on frontline systems of different support system top event failures using data base P1.

- Computer Code P4. The ETC9 program is next used to help the analyst determine the end states for the support tree using the turbine trip input file (P3). This is an important part of the overall accident sequence model construction because the number of final support states for which all of the frontline event trees are quantified, with the number of initiating events analyzed, determines the size and computational complexity of the overall model. The ETC9 code identifies the impacts of each sequence through the support tree, groups sequences with the same impacts into impact vectors, and then collects all impact vectors with very low frequency into a common state to reduce the total number of unique end states with appreciable frequency. This determination of significant and unique impact vectors is repeated for each quantification of the support tree. Separate quantifications of the support tree are only required for those initiating event groups that differ in their impacts on the support system top events. Although the unique impact vectors computed for the support tree structure are the same for all initiating events (i.e., they are not dependent on the quantification), those impact vectors that are grouped together by frequency binning do differ from one quantification run to the next. The union of all the significant impact vectors for all support tree quantifications are candidates for support tree end states. For the TMI-1 PRA, this list of candidate support states was reviewed manually and selected states were judgmentally combined to limit the total number.

- Data Base P5. The final list of support system states and the definitions of these states in terms of their impacts on the frontline systems are saved for the generation of data base P8.

- Data Base P6. The end states of the support system event tree are assigned to specific support system states. A second version of the turbine trip ETC9 input file is then produced using these designations. Then, appropriate split fractions are made to produce a stacked ETC9 input file with one run per initiator group. The dependency table is removed.

- Computer Code P7. ETC9 is run to requantify the support tree for each of the initiating event groups of interest using data base P6.

- Data Base P8. One output from ETC9 is a description of the support tree scenario fragments and a sequence of successes and failures of top events and split fractions through the support tree for each quantification. This list of split fractions for each scenario fragment is ordered by their end state and frequency. This file will be input to the MAXIMA program (E12) (commonly referred to as the ".MAX" file).

- Data Base P9. Another output file produced by ETC9 contains an ordered list of the dominant scenario fragments with the failed and successful split fractions by name for each one. This file is to be used by MAXNAIL to produce the RM5 equation file.

- Data Base P10. The list of support states and their definitions (i.e., data base P5) is used along with the master frequency file (i.e., S4) to prepare a split fraction translation table. This table was prepared manually. The table describes how the assignment of split fractions to the frontline trees is to be changed as a function of the support state. The analyst first prepares a set of rules that document how the split fraction assignment is to be changed as a function of the related frontline impacts. The frontline impacts of each support state are then compared with these rules to identify the split fraction assignment changes. The results are then summarized in table form for subsequent use in the quantification of the frontline event trees.

B.4.3 FRONTLINE SYSTEM EVENT SEQUENCE ANALYSIS

T[illegible]r sequence analysis provides scenario frequency results from all [illegible] calculations to produce curves for core damage and plant damage state frequencies. The dominant contributors to each category are also tabulated and ranked.

The analysis is performed in two stages. First, the event sequence quantification is performed using the mean values from the initiating event frequencies and from the split fraction results; i.e., using the master frequency file. The results from this full quantification of the plant model event trees identifies the most important scenarios. The frequencies for these important scenarios are then reevaluated to quantify the uncertainty by propagating probability of frequency distributions for the split fractions and initiating events through the scenario equations to produce such distributions for the plant damage states and the total core melt frequency. Further explanation of this process is provided in the form of a description of the corresponding blocks in Figure B-11.

- Data Base E1. The data necessary for the event sequence analysis is provided by the results from each of the previously described analysis areas. The initiating events to be evaluated must be provided, along with a description of the potential frontline system plant response to each of these initiators in the form of an event sequence diagram. From this information, plant event tree models must be created.

- Computer Code E2. Event tree structures are prepared, based on the event sequence diagrams provided as input. The ETC9 program can be used in the event tree drawing mode to help in this process. The event tree structure input consists of top event definitions, the top event number at each branch, the end state for each branch, and the branches involved in each instance of repeated tree structure logic; i.e., transfers. These tree structures were then printed out for analyst review. After the tree structures were finalized, the appropriate split fractions were assigned to each branch point in the tree for the case in which all support systems are assumed available. The analyst also specifies the end states for the main line trees or for the subtrees if they are used. If one or more subtrees are required, the analyst must also specify the end states of the main line tree, which then determine which of the subtrees are transferred to from the main line tree. This step then provides all of the input necessary to evaluate the frontline event trees, assuming the boundary condition all of the support systems are available.

- Data Base E3. The input file for the case in which all support systems are assumed available is provided for all the frontline event trees. Such a frontline event tree input file is produced for each initiating event. Separate main line and subtree input files may be produced for each initiating event, depending on the number of top events required to model the plant response.

- Computer Code E4. The all support available ETC9 input files are then used as one of the input files to the ETCIN program. The ETCIN program takes the split fraction translation file as input from the support system analysis and the event tree code input files for the all support available boundary condition to produce a boundary condition table for each frontline event tree.

- Data Base E5. The boundary condition table produced by ETCIN indicates how to change the ETC9 input files from the all support available boundary condition to produce stacked input for to all other support system states. Run numbers and the unique runs for each event tree are also identified.

- Computer Code E6. The user then examines the boundary condition tables to determine if modifications need to be made. Run numbers may also be modified if necessary. The TABLE computer program then uses these final boundary condition tables with the ETC9 input files for all support available run to prepare the ETC9 input files for all support system states other than the all support available case. These other support system state quantification runs are then stacked behind the all support available case in a single input file for each event tree.

- Data Base E7. The full ETC9 data file contains a set of stacked runs for each event tree. The first run is the all support available case and subsequent runs consist of default and conditional split fractions that are specific to each support system state. The event tree end states and structures do not change with support state and therefore only appear once in the data file with the first run.

- Computer Code E8. ETC9 is used to quantify the frequency of scenarios through the frontline event trees, based on the assignment of split fractions documented in the E7 data base. The full ETC9 input files are quantified, including those from the fire and seismic analysis. The numerical values for each split fraction in the data files are extracted from the master frequency file that is produced by the systems analysis; i.e., S4. Each such stacked run of ETC9 produces an input file for MAXIMA (data base E9) and one for MAXNAIL (data base E10).

- Data Base E9. One output from the ETC9 runs is a file containing information about each event tree branch or scenario fragment in the frontline event trees. This information includes the conditional frequency of the sequence fragment, the failed split fraction names, and the end state to which the sequence fragment is assigned. The total frequency of each end state of the tree is also provided. This information is produced for each quantification of the frontline event trees; i.e., one such listing for each support state quantified. Only the scenarios above a user-specified cutoff appear in this data base.

- Data Base E10. A second output from ETC9 is a description of the scenario fragments, a sequence of successes and failures of top events and split fractions through the tree in question. This list of split fractions for each scenario fragment is ordered by their end state and frequency.

- Data Base E11. A third output file is provided by ETC9. The combination of all such files produced by ETC9 contains information about all the end states, support system states, frontline main trees, subtree names, and run numbers of each event tree used in quantifying the plant model.

- Computer Code E12. The MAXIMA7 (Reference B-14) code makes use of two of the output files from ETC9 to link together the scenario fragments and determine the dominant scenarios to each plant damage state and to the total core damage frequency. MAXIMA uses the direction data file (E11) and the scenario frequency data set (E9). It also uses a list of the EO file names (data base E21).

- Data Base E13. One output of MAXIMA7 is a file containing a complete list of all scenarios going to core damage and to each plant damage state. These scenarios are ordered by frequency. The scenario frequency, the run number for the scenario fragment used in each segment, and the name of the end states in each segment through which the scenario passes are all provided. This file then becomes input to the MAXNAIL code.

- Data Base E14. MAXIMA7 also produces a file containing the initiating event frequencies and the matrix of total conditional frequencies of going from each initiating event to each plant damage state. These conditional frequencies are the sum of the frequencies of all scenarios going from the initiating event to one plant damage state divided by the initiating event frequency. This matrix of conditional frequencies is referred to as the M-matrix. If a level 2 or 3 PRA is performed, the plant M-matrix will be subsequently processed by the CRUSS (Reference B-15) program to combine it with the containment and the site matrices. Up to this point, the sequence frequency quantification is based on point values. Uncertainty propagation is accomplished on just the important sequences, as described in the following steps.

- Computer Code E15. The computer code MAXNAIL uses the scenario fragment descriptions contained in data base E10 and the scenario list data base E13 to produce end-to-end scenario algebraic equations in terms of the success and failures of system split fractions for input into RM5 (computer code E17).

- Data Base E16. The MAXNAIL code produces a file that contains one equation each for the total core damage frequency and for all important plant damage states. Each equation consists of an algebraic sum of the frequencies for each scenario that contributes to the total. Each scenario frequency is expressed as the product of the success or failures of the split fraction applicable for that scenario.

- Computer Code E17. RISKMAN5 is used to propagate all of the initiating event and split fraction distributions thru the scenario equations provided in data bases S1 and S3. RISKMAN5 reads the scenario equations (i.e., E16 and Q12) and the associated quantification data (i.e., S1, S3, and Q4) for the split fractions and the initiating event frequencies. It produces the probability of frequency distributions for total core damage and for inidividual plant damage states in data base E18.

- Data Base E18. The data base file produced by RISKMAN5 contains the probability of frequency distribution for total core damage frequency and for the frequency of each plant damage state. These distributions are stored in cumulative form.

- Computer Code E19. Program DPLOT reads the core damage and plant damage state frequency distributions from the E18 data base and plots either the cumulative or probability distribution functions for each.

- Output E20. The plots of the cumulative distribution functions and the probability distribution functions represent summary level results of the quantification process. The list of dominant sequences determined by MAXIMA7 (i.e., E13) and the point estimate contributions of each initiating event (i.e., E14) provide just a few of the many ways that the results can be further evaluated for risk management purposes.

B.4.4 SEISMIC ANALYSIS

The methods used for the assessment of seismic events are documented in Section 2 of the External Events and Environmental Hazards Report. The quantification of the seismic scenario frequencies requires input from other tasks, as indicated in Figure B-9.

- Data Base Q1. This data base contains the frequencies of ground motions of various sizes at the plant. This provides the initiating event frequencies for the seismic events. The continuous range of seismic event magnitudes is discretized into four levels for purposes of the quantification.

- Data Base Q2. A second data base provides the structural analysts' estimates of the seismically initiated ground accelerations at which plant structures and components are predicted to fail; i.e., the fragility curves. These estimates are provided in the form of parameters of lognormal distributions. Then, for each of the four seismic intervals, a probability of frequency distribution can be constructed for the seismic failure frequency of each structure and component. The mean values of these distributions are stored in a failure rate data base file for seismic events. The fragility analysis also identifies the failure modes for the equipment or structures on which the fragility curves are based.

- Computer Code Q3. The RISKMAN3 computer code is used to quantify the systems models, accounting for both the seismic and nonseismic failure causes. The systems analysts use the failure modes determined by the fragility analysts to decide how the seismic impacts are to be incorporated into the models. Once the system equations are modified accordingly, RISKMAN3 is used to quantify the system models. A separate quantification is required for each seismic level.

- Data Base Q4. The seismic system quantification results are stored in four different master frequency files; i.e., one for each seismic level. The point estimate results, which approximate the mean values for these system results, are then ready for quantification of the seismic event trees. The split fraction distributions are generated only for those split fractions in scenarios found to be important to risk.

- Data Base Q5. The seismic support model and frontline event trees are the same as those used for the turbine trip initiating event. However, the assignment of split fractions to these trees is somewhat modified to account for the additional dependencies introduced by the seismic initiator. The names of all the system split fractions are kept the same as in the quantification for the turbine trip initiator. However, the numerical values change as a function of seismic level, as documented in data base Q4.

- Computer Code Q6. ETC9 is used to quantify the frequency of scenarios thru the seismic support and frontline event trees, based on the assignment of split fractions documented in the Q5 data base. The full ETC9 input files are quantified, including those for all four seismic levels. The numerical values for each split fraction in the data files are extracted from the master frequency files, which are produced by the systems analysis; i.e., Q3. Each such stacked run of ETC9 produces an input file for MAXIMA.

- Data Base Q7. One output from the ETC9 runs is a file containing information about each event tree branch or scenario fragment in the frontline event trees. This information includes the conditional frequency of the sequence fragment, the failed split fraction names, and the end state to which the sequence fragment is assigned. The total frequency of each end state of the tree is also provided. This information is produced for each quantification of the seismic event trees. Only the scenarios above a user-specified cutoff appear in the data base.

- Data Base Q8. A second output from ETC9 is a description of the scenario fragments; i.e., a sequence of successes and failures of top events and split fractions through the tree in question. This list of split fractions for each scenario fragment is ordered by their end state and frequency.

- Computer Code Q9. The MAXIMA7 (Reference B-14) code makes use of two of the output files from ETC9 to link together the scenario fragments and determine the dominant scenarios to each plant damage state and to the total core damage frequency. MAXIMA7, as applied to seismic events, uses the same direction data file (E11) as the nonseismic MAXIMA7 run; i.e., as E12. The scenario fragment frequency data base for the seismic events (i.e., data base Q7) is also used by MAXIMA7.

- Data Base Q10. One output of MAXIMA7 is a file containing a complete list of all the seismic scenarios going to core damage and to each plant damage state. These scenarios are ordered by frequency. The scenario frequency, the run number for the scenario fragment used in each segment, and the name of the end states in each segment through which the scenario passes are all provided.

- Data Base Q11. MAXIMA7 also produces a file containing the initiating event frequencies and the matrix of total conditional frequencies of going from each seismic initiating event to each plant damage state. These conditional frequencies are the sum of the frequencies of all scenarios going from the initiating event to one plant damage state divided by the initiating event frequency. This matrix of conditional frequencies is referred to as the M-matrix. If a level 2 or 3 PRA is performed, the plant M-matrix will be subsequently processed by the CROSS (Reference B-15) program to combine it with the containment and the site matrices.

- Data Base Q12. Up to this point, the sequence frequency quantification for seismic events is based on point values. Uncertainty propagation is accomplished on just the important sequences. Review of the completed seismic M-matrix quickly reveals that the contribution frum seismic events is very small relative to all other events. Consequently, the steps in the nonseismic quantification process to identify the key scenarios for uncertainty analysis, which are very few, and to write them in equation form for uncertainty propagation were easily accomplished manually. These equations were transferred over to the RISKMAN5 set of equations for all other initiating events (i.e., see the description for E17) for propagation of uncertainties.

B.4.5 FIRE, FLOOD, AND EXTERNAL EVENTS ANALYSIS

The assessment of fires, floods, and external events is event specific. Generally, the quantification of such events is done without the aid of the computer. The number of sequences is generally very few, and use can often be made of previous, detailed calculations done for other plants, but for which the overall conclusions are generically applicable to simplify the analysis. This was found to be the case in the TMI-1 PRA.

For the TMI-1 PRA, the important sequences for such events were identified using hand calculations. When additional failures, independent of the initiator, were found to be important, use is made of the results from the systems analysis models (i.e., the master frequency file, S4) to quantify these additional failures. The key scenarios based on the point estimate results are then loaded into RISKMAN6 for uncertainty propagation. In Figure B-9 this data base file is referred to as F1.

B.5 CALCULATION OF SYSTEM IMPORTANCE

The contribution to risk of each scenario and system was reported in Section 5 of this report. These contributions were calculated using the point estimate plant model (M) matrix for this level 1 PRA, computed by combining the mean values of the split fraction distributions and combining them with the mean value initiating event frequency vector, O. This section describes how this "disassembly" process can be generalized to identify risk contributions from a level 2 or 3 PRA that generates the containment (C) and site (S) matrices as well; i.e., presents the results in terms of release category frequencies and frequencies of exceeding specified damage indices (e.g., number of early fatalities) in addition to the frequencies of each plant damage state, as computed in the current study. It runs this assembly process backward to disassemble or "decompose" the risk into its important pinch point contributors, then to "unsum" at each pinch point to get individual contributors. Diagonal matrices can be developed from the M, C, and S-matrices to quantify the contribution of each state at each pinch point to the other states at other pinch points, including to risk. For instance, the plant damage state diagonal matrix,

$$\phi_D^y$$

can be combined with the site and containment matrices to determine the importance of each plant damage state to each type of offsite health effect. The diagonal matrix

$$\phi_D^y$$

for the plant damage states consists of the vector ϕ^I M (ϕ^I = initiating events vector; M = plant model matrix) arranged diagonally into a square matrix in which both dimensions are the number of plant damage states. To further decompose the results requires going to the event trees and system models to identify specific event sequences and systems contributing to each plant damage state. From there, it is possible to dig still deeper by consulting the appropriate cause tables for the system alignments and individual components contributing to each system.

For instance, to find the important plant damage states with respect to risk, the example plant damage state vector

$$\phi_D^y$$

shown in Table B-1 is made into a square matrix

$$\phi_D^y = \begin{bmatrix} \phi_1^y & 0 & \ldots & 0 \\ 0 & \phi_2^y & & 0 \\ 0 & 0 & \ldots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \ldots & \phi_N^y \end{bmatrix}$$

with N diagonal entries, one for each PDS, which, if multiplied by the product of containment matrix C and site matrix S, yields the matrix,

$$\phi_D^y CS$$

An example consisting of one row of this matrix for one damage index is shown in Table B-2. This matrix is the frequency of exceedance for early fatalities calculated for each PDS. One row on this table shows one contribution of the plant damagc state to early fatalities. One major contributor, PDS VE, is indicated by the line surrounding the points on its column. This table entry is the risk curve labeled "VE" shown graphically with the total risk curve from all PDSs for early fatalities in Figure B-13.

After the plant damage states that are the major contributors to risk have been identified, the microscope can be turned up to find the scenarios that contribute most of the frequency of each plant damage state. The plant damage state frequencies presented in Section 5 were calculated by summing the frequency of all scenarios leading to it. Similarly, the early fatalities that are caused (for example, plant damage state VE) are caused mostly by the specific scenario that leads to most of the frequency of PDS VE. This is true because each scenario goes to only one PDS. Thus, the risk that is attributable to each scenario can be calculated by taking a ratio of frequencies. Since

$$\phi^{Y}_{VE} = \sum_{i=1}^{\substack{\text{all scenarios}\\ \text{to PDS VE}}} \phi_{i,VE} = \text{the total frequency of plant damage state VE}$$

and

$$\phi^{t}_{xVE} = \phi^{Y}_{VE} CS$$

where

$$\phi^{t}_{x\ VE}$$

is the frequency of exceeding level 1 of damage indice x due to scenarios in plant damage state VE, then by substitution

$$\left[\phi^{t}_{x}\right]_{VE} = \sum_{i=1}^{\substack{\text{all VE}\\ \text{scenarios}}} \phi_{i,VE}\ CS$$

The risk associated with each scenario can be calculated from the PDS risk using the scenario frequency $\phi_{i,VE}$

$$\left[\phi^{t}_{x}\right]_{i,VE} = \left[\phi^{t}_{x}\right]_{VE} \cdot \left[\frac{\phi_{i,VE}}{\phi^{y}_{VE}}\right]$$

where the term in braces is the fraction of the total PDS VE frequency from each scenario. This equation means that any number in Table B-2 can be multiplied by the frequency fraction for each scenario to get a scenario-specific risk curve, which would be similar to that for the total damage state risk curve.

Knowing the risk attributable to each scenario is interesting but not as interesting as knowing the risk associated with each system. The microscope can be turned up even further to find the contribution of each system to risk. This is done by using the risk for each scenario to find the risk for each system (event tree top event). Each scenario consists of an initiating event and the failure of one or more responding systems.

The frequency of a scenario is calculated by multiplying the initiating event frequency by the conditional split fraction of each (failure) event in the scenario. Most scenarios that lead to core damage consist of at least one top event failure. (An exception to this are V-sequences in which core damage is a direct result of the initiating event.) The risk associated with each system that fails in a scenario is all of the risk associated with that scenario. This concept can be appreciated by considering what it would mean to make a system perfect. If a system were made perfect, its failure frequency (conditional split fraction) becomes zero. If any top event in a scenario has a frequency of zero, the scenario has a frequency of zero. For a scenario to have a frequency of zero means the scenario cannot happen. If it cannot happen, it does not exist. Therefore, making any top event in a scenario perfect makes the scenario and its contribution to risk disappear; hence, one less way of getting severe core damage and, thus, of getting risk to the public.

To find the risk associated with each system, the total risk associated with all scenarios containing the failure of a particular system, j, can be summed:

$$\left[\phi^{t}_{x}\right]_{j} = \sum_{\ell=1}^{\substack{\text{all PDSs contributing}\\ \text{to damage type, t}\\ \text{at level x}}} \; \sum_{i=1}^{\substack{\text{all scenarios}\\ \text{to PDS } \ell \text{ with system j}}} \left[\phi^{t}_{x}\right]_{i} \qquad \text{(B.5.1)}$$

The sum is over all scenarios in each PDS containing the failure of system j and contributing to the damage type, early fatalities. Then, the contributions from all PDSs are also summed. Unlike a scenario, a system failure may occur in many scenarios in many different plant damage states.

System contributions to risk calculated in this way mean that if the system were fixed so that its failure could not appear in any scenario (i.e., if it were made perfect), the total frequency of exceedance of early fatalities would be reduced by the amount $[\phi^{t}_{x}]_{j}$. They would no longer contribute to risk.

Some scenarios may contain more than one system (top event) failure. If one system in a scenario is fixed, then the scenario will disappear. Therefore, the risk associated with other systems appearing in the scenario will also be reduced. $[\phi^{t}_{x}]_{j}$ for other systems will have to be recalculated after each system is fixed. Said another way, $[\phi^{t}_{x}]_{j}$ represents the reduction in risk attributable to each system only if they are fixed one at a time.

If only one system failed in each scenario, the percentage contribution, of, say, HPI would remain constant after EFW was fixed. If all scenarios contained both AFW and HPI failures, fixing either system would eliminate the risk entirely.

The next step in unraveling the risk is to turn up the microscope still further and find the important system failure causes that contribute to risk. To do this, we must go to the cause table for each system and find the fraction of the system split fraction associated with each cause, k, of system failure:

$$\left[\phi_x^t\right]_j^k = \left[\frac{f_{k,j}}{\sum\limits_{k=1}^{\substack{\text{all causes}\\ \text{in system j}}} f_{k,j}}\right] \cdot \left[\phi_x^t\right]_j = f_{k,j}\left[\phi_x^t\right]_j$$

The denominator in this equation is just the total split fraction for system, j, which, if the $f_{k,j}$ terms are percentages, is just 100%.

Further, if the contribution to risk of all operator errors, for instance, is sought, then

$$[\phi_x^t]_j^k$$

must be summed over all systems with operator errors as a cause:

$$\phi_x^{t\ \substack{\text{operator}\\ \text{errors}}} = \sum_{j=1}^{\substack{\text{all operators with}\\ \text{operator errors}}} f_{j,\ \text{operator error}} \cdot \phi_{x\ j}^t$$

Results of the TMI-1 PRA are presented in Section 5 of this report in terms of the percentage contribution of a particular system to risk. This percentage is the measure of "importance" used. Each of the frequencies discussed above can be converted to importance by dividing

$$\phi_x^t$$

Important systems are those that appear in scenarios, the sum of whose frequency dominates the plant damage states important to risk. The process described above was run through for all PDSs in the computer code MAXIMA.

The ways to reduce the frequency of severe core damage can also be calculated using this same logical procedure. The importance of a scenario, i, with respect to core damage frequency is just

$$\frac{\phi_{i,PDS}}{\phi_{total}}$$

where the denominator is the total core damage frequency. The importance of a system, i, is to reducing core damage frequency is like Equation (B.74).

$$\frac{1}{\phi_{total}}\left\{\sum_{P=1}^{\substack{\text{all}\\ \text{PDSs}}}\left[\sum_{i=1}^{\substack{\text{all scenarios}\\ \text{in PDS P with}\\ \text{system j}}}\phi_{i,P}\right]\right\}$$

In a similar fashion, the importance of a system failure cause, k, is just

$$\frac{1}{\phi_{total}}\left\{\sum_{j=1}^{\substack{\text{all systems}\\ \text{with failure}\\ \text{cause k}}} f_{j,k}\left[\sum_{P=1}^{\substack{\text{all}\\ \text{PDSs}}}\left(\sum_{i=1}^{\substack{\text{all scenarios}\\ \text{in PDS P with}\\ \text{system j}}}\phi_{i,P}\right)\right]\right\}$$

where $f_{j,k}$ is the importance of cause k to the failure system j.

B.6 REFERENCES

B-1. Kaplan, S., and B. J. Carrick, "On the Quantitative Definition of Risk," Risk Analysis, Vol. 1, No. 1, March 1981.

B-2. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

B-3. de Finetti, B., Theory of Probability, Vols. 1 and 2, John Wiley & Sons, New York, 1974.

B-4. Savage, L. J., The Foundation of Statistics, 2nd Ed., Dover Publications, New York, 1972.

B-5. Lindley, D. V., Introduction to Probability and Statistics from a Bayesian Viewpoint, Cambridge University Press, 1970.

B-6. Apostolakis, G., "Probability and Risk Assessment: The Subjectivistic Viewpoint and Some Suggestions," Nuclear Safety, Vol. 19, No. 3, pp. 305-315, May-June 1978.

B-7. Green, A. E., and A. J. Bourne, Reliability Technology Wiley Interscience, New York, 1972.

B-8. Aitchison, J., and J. A. C. Brown, The Lognormal Distribution, Cambridge University Press, 1963.

B-9. Hammersley and Handscomb, Monte Carlo Methods, Methuen, London, 1964.

B-10. Apostolakis, G., and Y. T. Lee, "Methods for the Estimation of Confidence Bounds for the Top-Event Unavailability of Fault Trees," Nuclear Engineering and Design, Vol. 41, pp. 411-419, 1977.

B-11. Kaplan, S., "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations--Application to Seismic Risk Assessment," Risk Analysis, Vol. 1, No. 3, September 1981.

B-12. Simpson, D. B., et al., "RISKMAN3 User Manual," PLG-0455, May 1986.

B-13. Buttemer, D. R., et al., "ETC9 (Event Tree Code 9), Computer Code User Manual," PLG-0466, April 1986.

B-14. Mikschl, T. J., et al., "MAXIMA7 Computer Program User Manaul," PLG-0514, October 1986.

B-15. Wheeler, D. M., and D. C. Bley, "CROSS Computer Code," PLG-0219, February 1982.

TABLE B-1. VALUES AT SECOND PINCH POINT - PLANT DAMAGE STATE FREQUENCIES ($\phi^I M$)

Plant Damage State	Frequency
SEFC	7.41-6
SEF	1.28-9
SEC	1.76-8
SE	6.53-10
SLFC	1.91-5
SLF	4.76-9
SLC	1.93-6
SL	1.25-8
TEFC	8.43-7
TEF	1.61-9
TEC	9.32-7
TE	2.27-7
AEFC	1.75-6
AEF	1.87-10
AEC	8.23-9
AE	1.05-11
ALFC	9.76-6
ALF	7.27-10
ALC	3.98-10
AL	2.52-13
V	1.05-7
Total (Core Melt)	4.21-5

NOTE: Exponential notation is indicated in abbreviated form; i.e., 7.41-6 = 7.41 x 10^{-6}.

TABLE B-2. UNCONDITIONAL FREQUENCY OF EXCEEDANCE OF EARLY FATALITIES BY PLANT DAMAGE STATE

PLANT DAMAGE STATES

NUMBER OF EARLY FATALITIES

EFFECT IS EARLY FATALITIES

NUMBER	TEC	TE	AEFC	AEF	AEC	AE	ALFC	ALF	ALC	AL	VE	TOTAL RISK
1.000E+00	3.040E-11	2.612E-08	4.413E-11	8.000E-15	2.372E-13	3.194E-12	2.463E-10	2.693E-14	1.003E-14	7.616E-14	2.625E-08	5.520E-08
2.000E+00	3.009E-11	2.612E-08	4.413E-11	8.000E-15	2.372E-13	3.184E-12	2.463E-10	2.693E-14	1.003E-14	7.616E-14	2.625E-08	5.519E-08
3.000E+00	3.009E-11	2.612E-08	4.413E-11	8.000E-15	2.072E-13	3.184E-12	2.453E-10	2.693E-14	1.003E-14	7.616E-14	2.625E-08	5.519E-08
5.000E+00	2.976E-11	2.612E-08	4.352E-11	7.934E-15	2.043E-13	3.184E-12	2.428E-10	2.667E-14	9.891E-15	7.616E-14	2.598E-08	5.481E-08
7.000E+00	2.976E-11	2.532E-08	4.352E-11	7.835E-15	2.043E-13	3 184E-12	2.428E-10	2.642E-14	9.891E-15	7.616E-14	2.598E-08	5.396E-08
1.000E+01	2.912E-11	2.532E-08	4.231E-11	7.703E-15	1.986E-13	3.075E-12	2.351E-10	2.590E-14	9.617E-15	7.354E-14	2.516E-08	5.321E-08
2.000E+01	2.874E-11	2.532E-08	4.170E-11	7.637E-15	1.458E-13	3.075E-12	2.327E-10	2.565E-14	9.477E-15	7.354E-14	2.479E-08	5.283E-08
3.000E+01	2.718E-11	2.532E-08	4.044E-11	7.504E-15	1.896E-13	2.965E-12	2.256E-10	2.513E-14	9.190E-15	7.092E-14	2.437E-08	5.204E-08
5.000E+01	2.394E-11	2.532E-08	3.495E-11	6.915E-15	1.641E-13	2.854E-12	1.950E-10	2.284E-14	7.944E-15	6.827E-14	2.378E-08	4.861E-08
7.000E+01	2.264E-11	2.375E-08	3.248E-11	6.463E-15	1.525E-13	2.854E-12	1.812E-10	2.133E-14	7.383E-15	6.827E-14	1.932E-08	4.543E-08
1.000E+02	2.200E-11	2.375E-08	3.127E-11	6.334E-15	1.468E-13	2.854E-12	1.745E-10	2.082E-14	7.108E-15	6.827E-14	1.860E-08	4.467E-08
2.000E 02	1.908E-11	2.375E-08	2.754E-11	5.934E-15	1.293E-13	2.635E-12	1.537E-10	1.928E-14	6.253E-15	6.303E-14	1.640E-08	4.236E-08
3.000E+02	1.844E-11	2.375E-08	2.695E-11	5.866E-15	1.265E-13	2.525E-12	1.504E-10	1.902E-14	5.124E-15	6.040E-14	1.504E-08	4.198E-08
5.000E+02	1.618E-11	2.295E-08	2.383E-11	5.435E-15	1.119E-13	2.306E-12	1.330E-10	1.747E-14	5.416E-15	5.516E-14	1.422E-08	3.921E-08
7.000E+02	1.552E-11	1.741E-08	2.321E-11	4.577E-15	1.090E-13	1.976E-12	1.295E-10	1.540E-14	5.276E-15	4.727E-14	1.355E-08	3.295E-08
1.000E+03	1.424E-11	1.424E-08	2.262E-11	4.217E-15	1.052E-13	1.757E-12	1.262E-10	1.412E-14	5.141E-15	4.203E-14	1.349E-08	2.920E-08
2.000E+03	1.132E-11	1.029E-08	1.833E-11	3.273E-15	8.603E-14	1.547E-12	1.023E-10	1.107E-14	4.165E-15	3.940E-14	1.094E-08	2.233E-08
3.000E+03	9.383E-12	7.913E-09	1.585E-11	2.715E 15	7.443E-14	1.537E-12	8.846E-11	9.293E-15	3.603E-15	3.676E-14	9.479E-09	1.827E-08
5.000E+03	6.147E-12	7.122E-09	1.095E-11	2.087E-15	5.141E-14	1.208E-12	6.110E-11	6.975E-15	2.493E-15	2.889E-14	6.553E-09	1.438E-08
7.000E+03	4.529E-12	4.747E-09	7.909E-12	1.467E-15	3.713E-14	1.099E-12	4.413E-11	4.943E-15	1.797E-15	2.627E-14	4.740E-09	9.968E-09
1.000E+04	4.529E-12	3.956E-09	7.909E-12	1.365E-15	3.713E-14	9.881E-13	4.413E-11	4.576E-15	1.797E-15	2.363E-14	4.740E-09	9.130E-09
2.000E+04	1.618E-12	7.917E-10	2.434E-12	3.754E-16	1.142E-14	5.489E-13	1.358E-11	1.336E-15	5.531E-16	1.313E-14	1.458E-09	2.365E-09
3.000E+04	3.235E-13	7.910E-10	6.083E-13	1.815E-16	2.856E-15	5.489E-13	3.394E-12	5.794E-16	1.383E-16	1.313E-14	3.646E-10	1.218E-09
5.000E+04	3.235E-13	7.910E-10	6.083E-13	1.623E-16	2.856E-15	0.	3.394E-12	5.046E-16	1.383E-16	0.	3.646E-10	1.217E-09
7.000E+04	3.235E-13	1.582E-13	6.083E-13	6.493E-17	2.856E-15	0.	3.394E-12	2.523E-16	1.383E-16	0.	3.646E-10	3.792E-10
1.000E+05	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
2.000E+05	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
3.000E+05	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
5.000E+05	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
7.000E+05	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
1.000E+06	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
2.000E+06	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
3.000E+06	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
5.000E+06	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
7.000E+06	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
1.000E+07	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
2.000E+07	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
3.000E+07	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
5.000E+07	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
7.000E+07	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
1.000E+08	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
2.000E+08	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
3.000E+08	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
5.000E+08	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
7.000E+08	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
1.000E+09	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
2.000E+09	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
3.000E+09	0.	0	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
5.000E+09	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
7.000E+09	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.

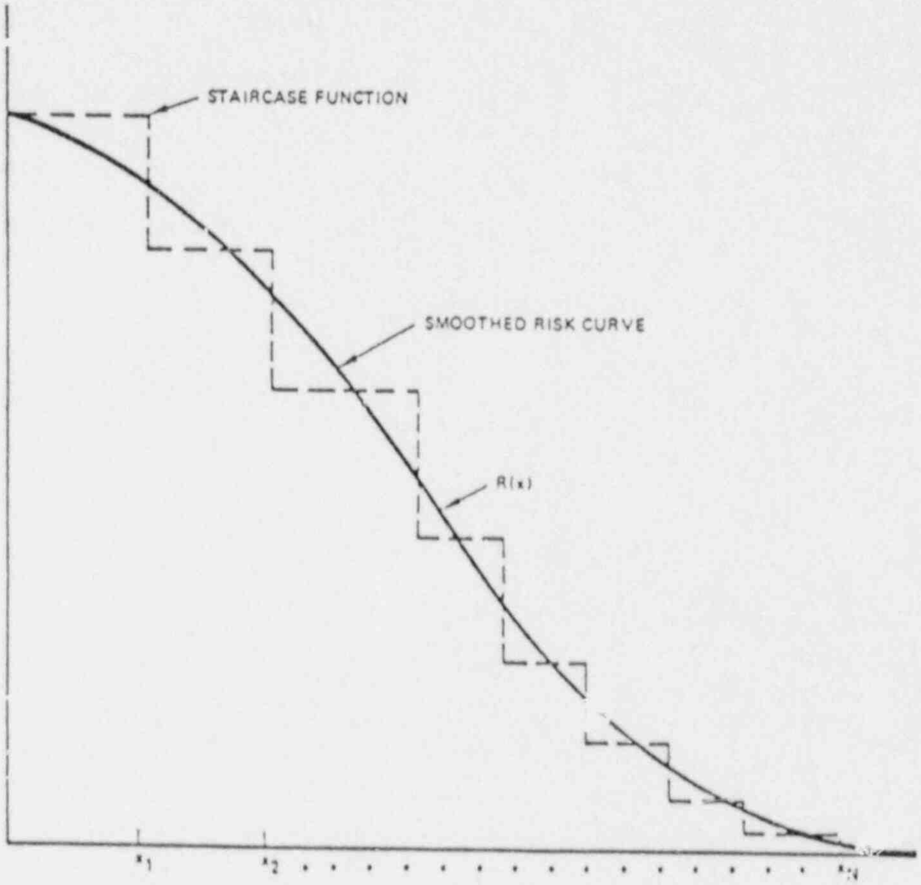


FIGURE B-1. RISK CURVE

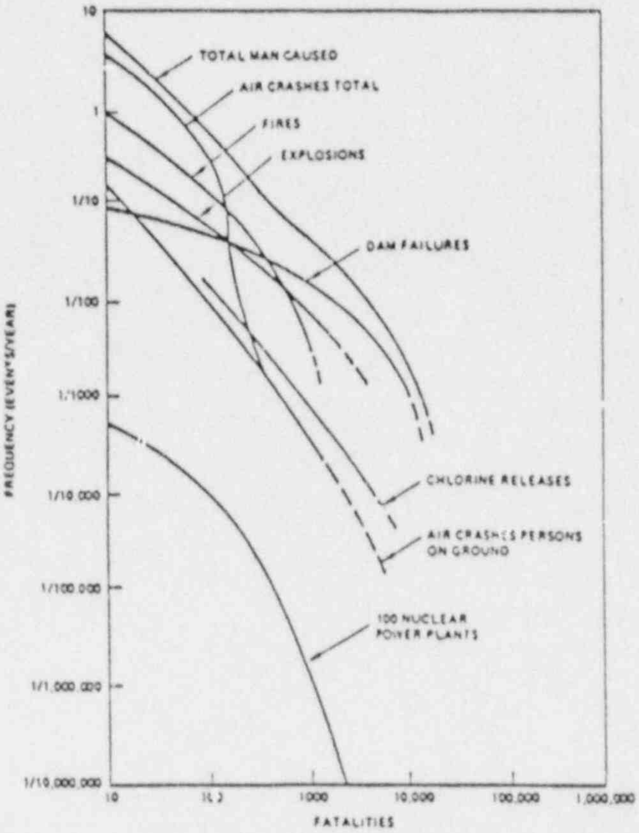


FIGURE B-2. FREQUENCY OF FATALITIES DUE TO MAN-CAUSED L,ENTS

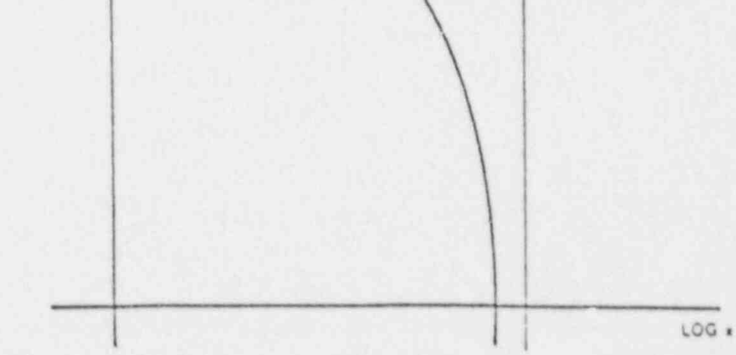


FIGURE B-3. RISK CURVE ON A LOG-LOG SCALE

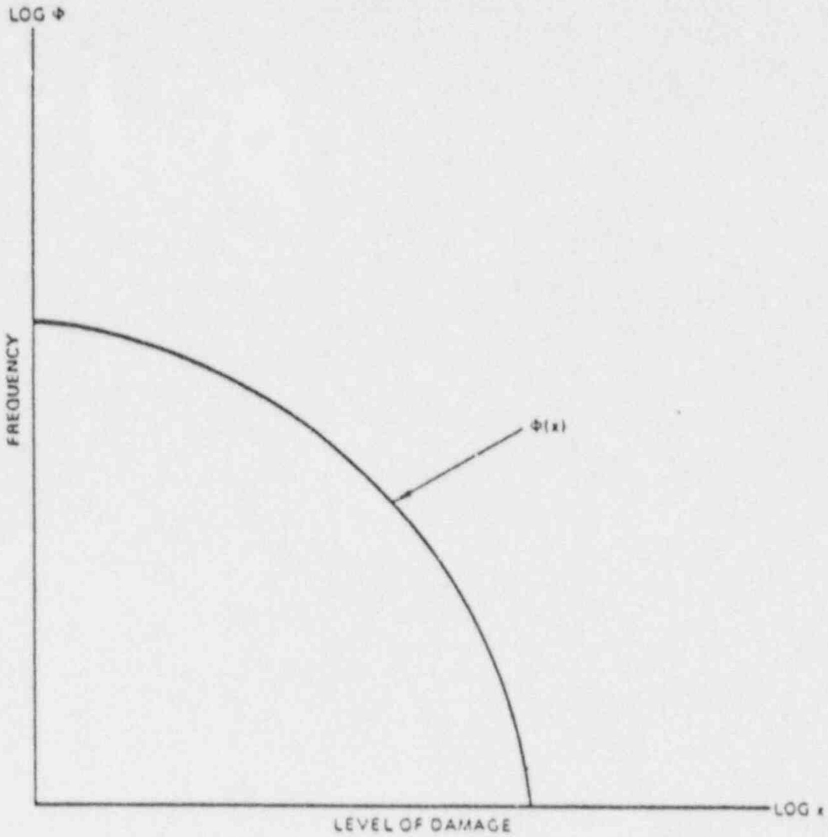


FIGURE B-4. RISK CURVE IN FREQUENCY FORMAT

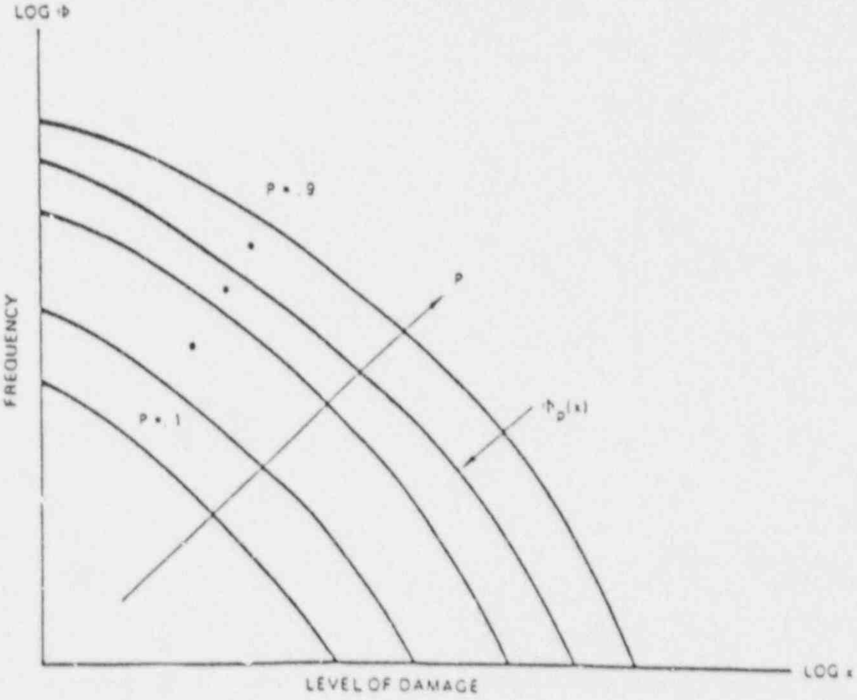


FIGURE B-5. RISK CURVE IN PROBABILITY OF FREQUENCY FORMAT

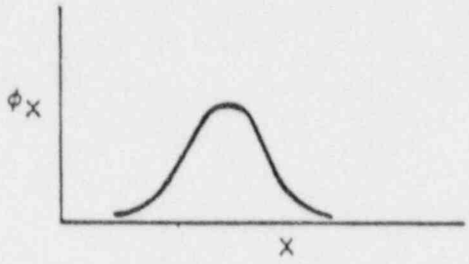


FIGURE B-6. POPULATION VARIABILITY CURVE

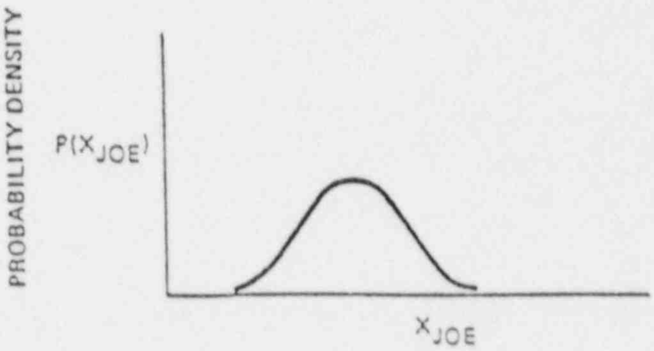


FIGURE B-7. STATE-OF-KNOWLEDGE CURVE

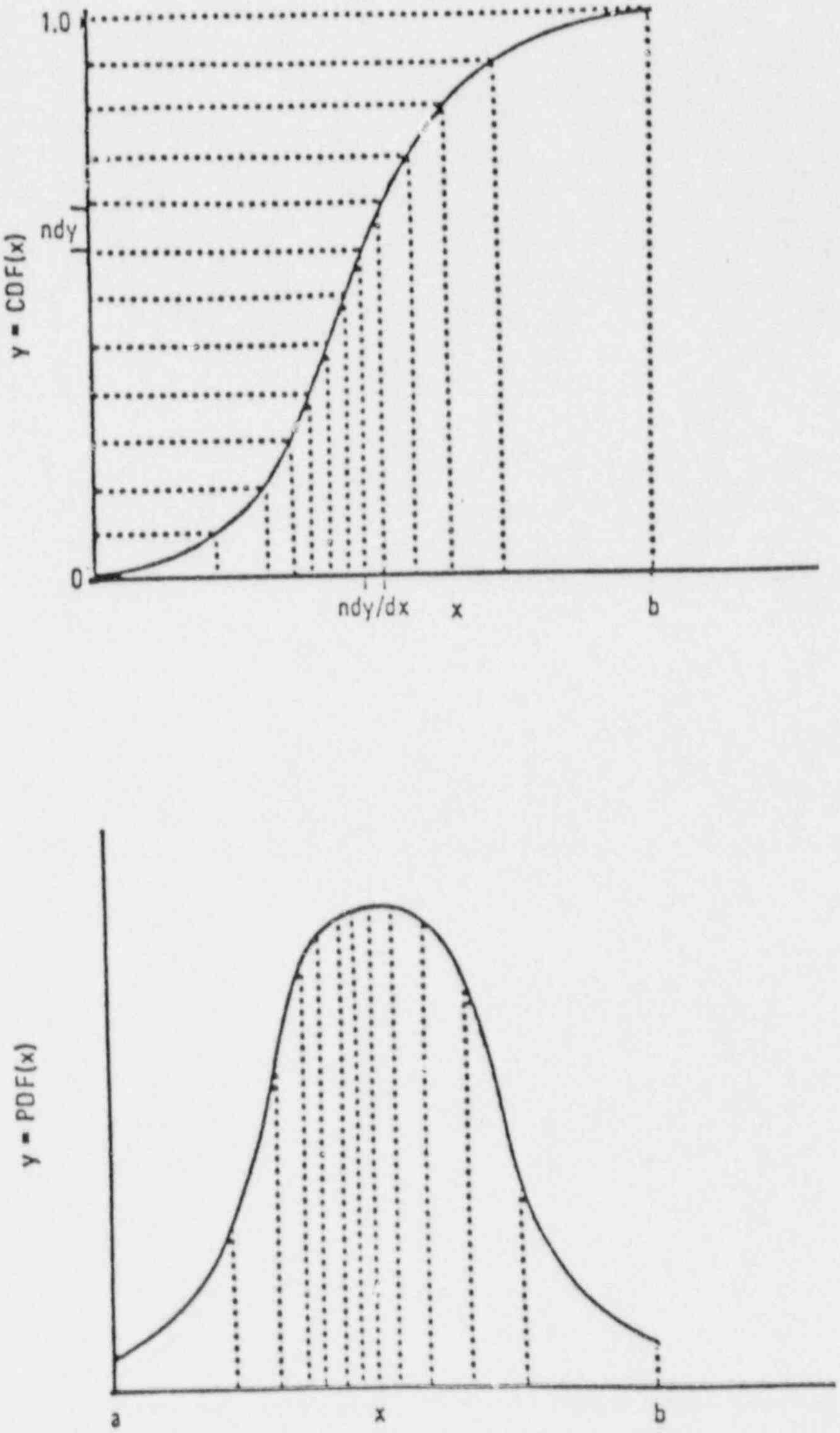


FIGURE B-8. MONTE CARLO SIMULATION TECHNIQUE

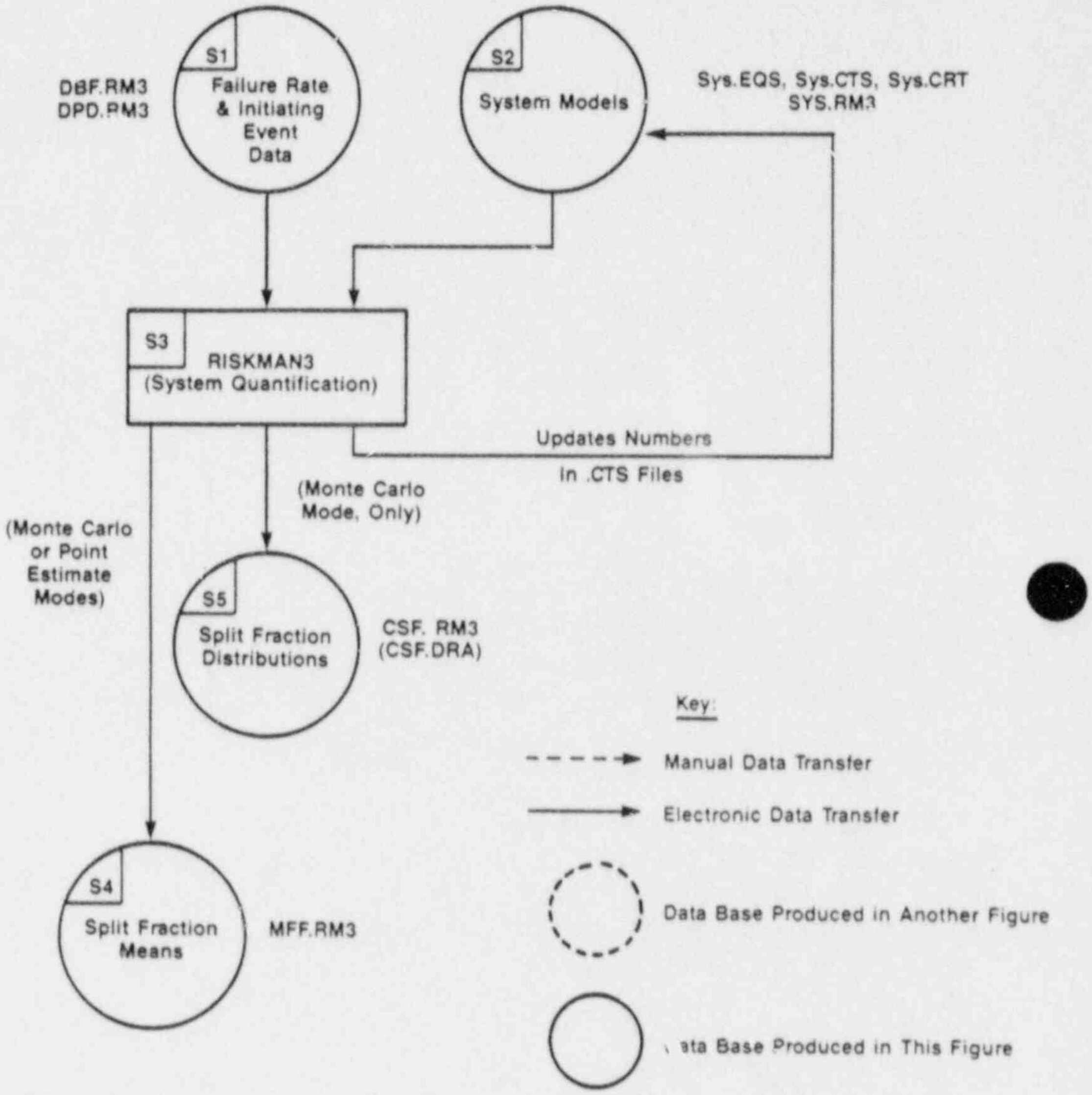

S1
Failure Rate & Initiating Event Data
DBF.RM3
DPD.PM3
S2
System Models
Sys.EQS, Sys.CTS, Sys.CRT
SYS.RM3
S3
RISKMAN3 (System Quantification)
Updates Numbers
in .CTS Files
(Monte Carlo Mode, Only)
(Monte Carlo or Point Estimate Modes)
S5
Split Fraction Distributions
CSF. RM3
(CSF.DRA)
S4
Split Fraction Means
MFF.RM3
Key:
Manual Data Transfer
Electronic Data Transfer
Data Base Produced in Another Figure
\ ata Base Produced in This Figure

FIGURE B-9. QUANTIFICATION PROCESS FLOW CHART--SYSTEMS ANALYSIS

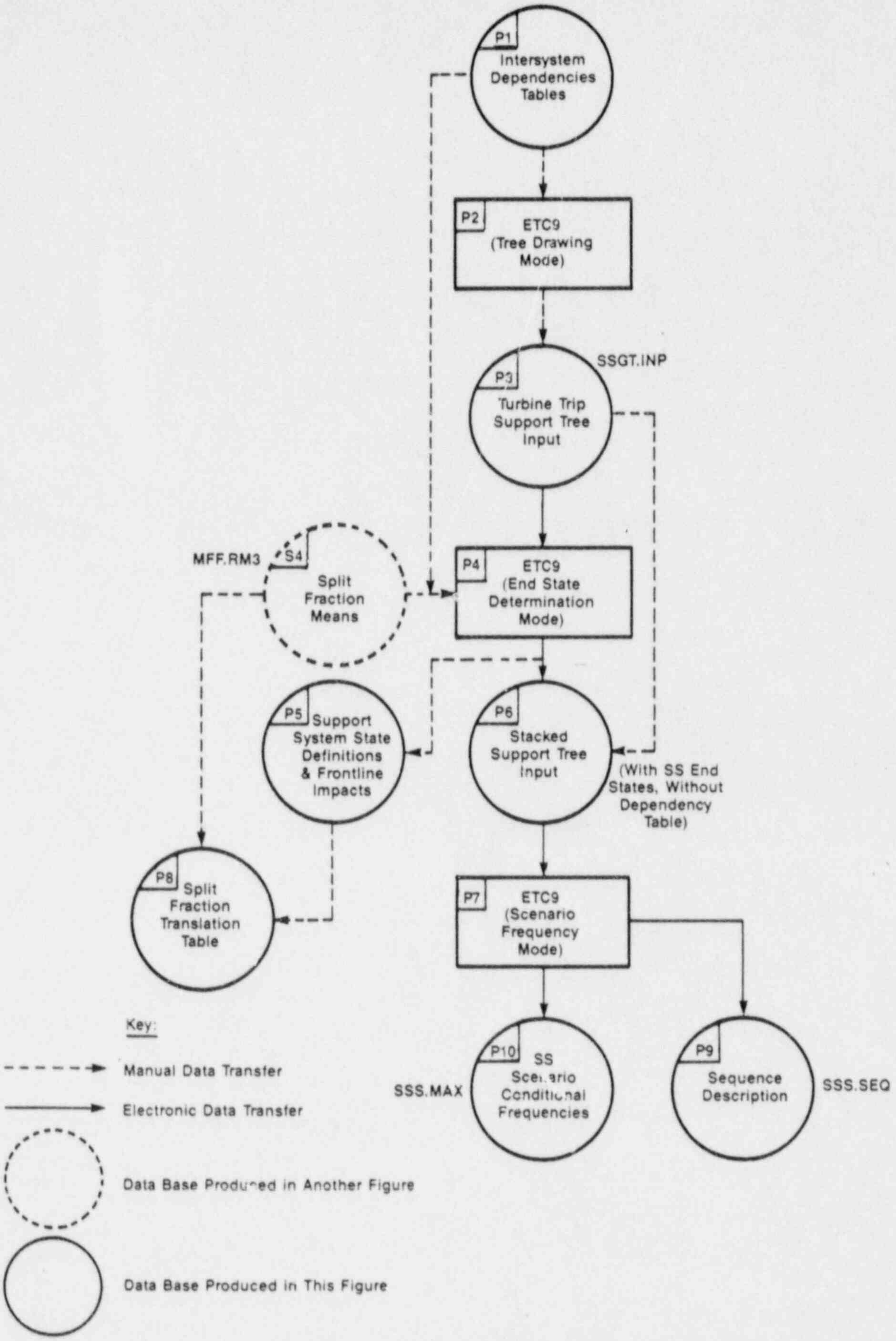

P1
Intersystem Dependencies Tables
P2
ETC9 (Tree Drawing Mode)
SSGT.INP
P3
Turbine Trip Support Tree Input
MFF.RM3
S4
Split Fraction Means
P4
ETC9 (End State Determination Mode)
P5
Support System State Definitions & Frontline Impacts
P6
Stacked Support Tree Input
(With SS End States, Without Dependency Table)
P8
Split Fraction Translation Table
P7
ETC9 (Scenario Frequency Mode)
Key:
Manual Data Transfer
Electronic Data Transfer
Data Base Produced in Another Figure
Data Base Produced in This Figure
SSS.MAX
P10
SS Scenario Conditional Frequencies
P9
Sequence Description
SSS.SEQ

FIGURE B-10. SUPPORT SYSTEM ANALYSIS

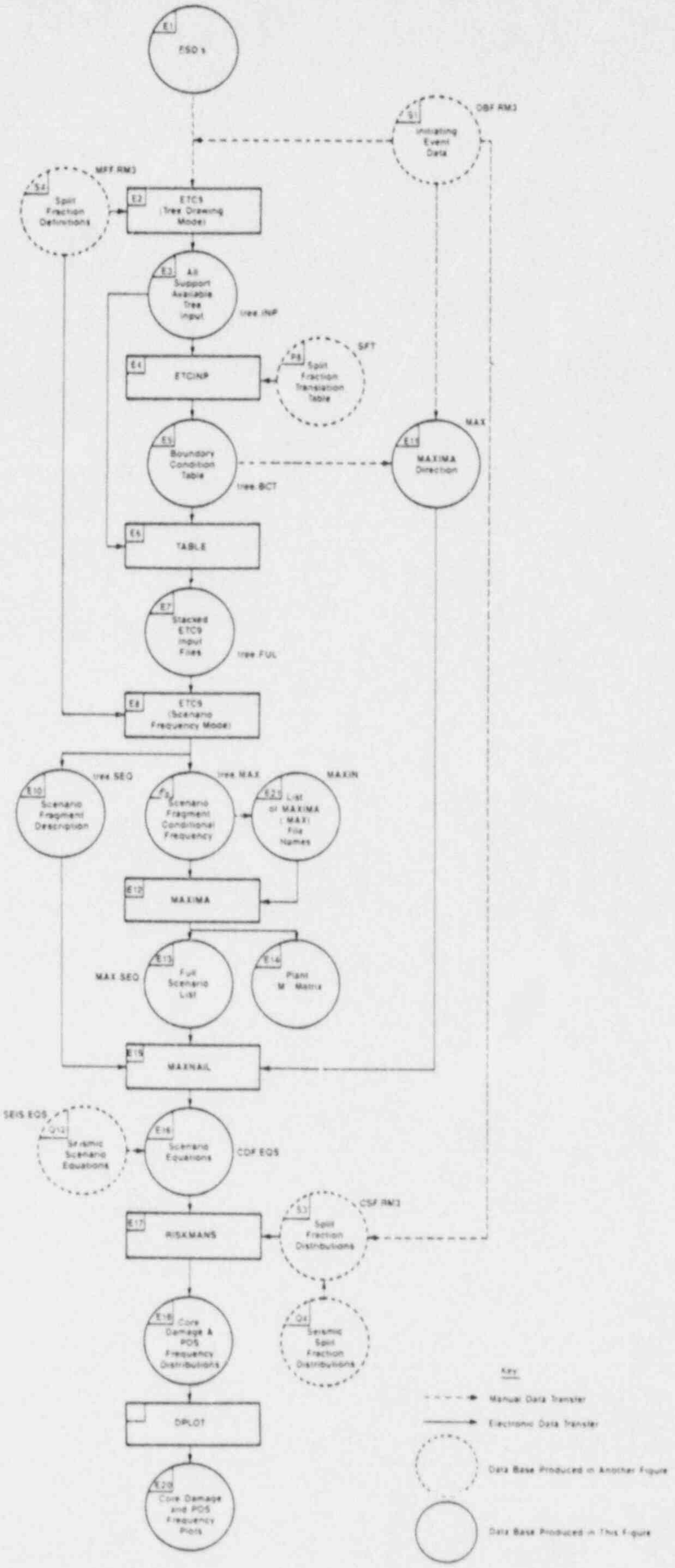

E1
ESD's
S1
Initiating Event Data
DBF.RM3
S4
Split Fraction Definitions
MFF.RM3
E2
ETC9 (Tree Drawing Mode)
E3
All Support Available Tree Input
tree.INP
E4
ETCINP
P8
Split Fraction Translation Table
SFT
E5
Boundary Condition Table
tree.BCT
E11
MAXIMA Direction
MAX
E6
TABLE
E7
Stacked ETC9 Input Files
tree.FUL
E8
ETC9 (Scenario Frequency Mode)
E10
Scenario Fragment Description
tree.SEQ
F9
Scenario Fragment Conditional Frequency
tree.MAX
E21
List of MAXIMA (MAX) File Names
MAXIN
E12
MAXIMA
E13
Full Scenario List
MAX.SEQ
E14
Plant M Matrix
E19
MAXNAIL
SEIS.EQS
Q12
Seismic Scenario Equations
E16
Scenario Equations
CDF.EQS
E17
RISKMANS
S3
Split Fraction Distributions
CSF.RM3
E18
Core Damage & PDS Frequency Distributions
Q4
Seismic Split Fraction Distributions
DPLOT
E20
Core Damage and PDS Frequency Plots
Key
Manual Data Transfer
Electronic Data Transfer
Data Base Produced in Another Figure
Data Base Produced in This Figure

FIGURE B-11. EVENT SEQUENCE ANALYSIS

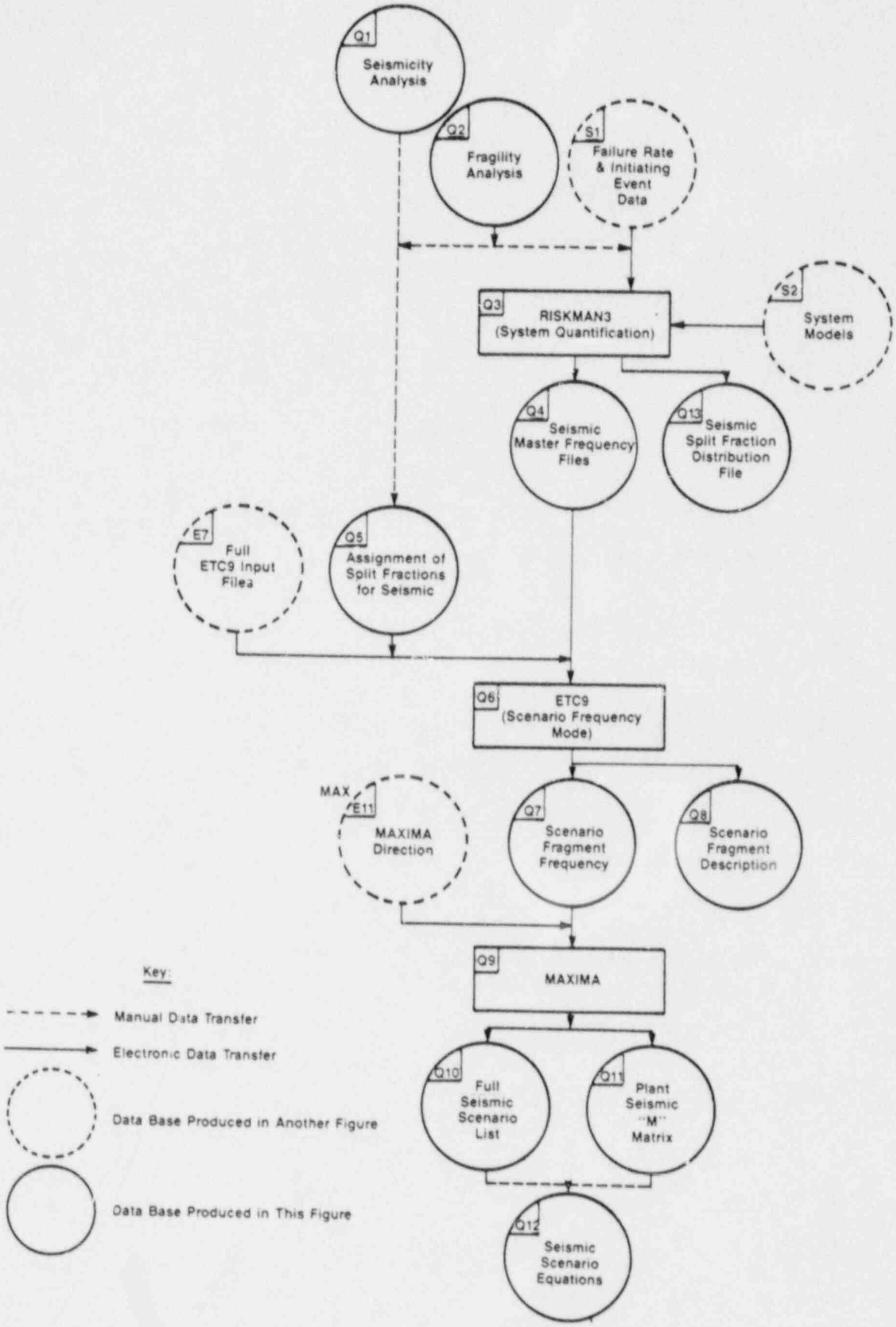

Q1
Seismicity Analysis
Q2
Fragility Analysis
S1
Failure Rate & Initiating Event Data
Q3
RISKMAN3 (System Quantification)
S2
System Models
Q4
Seismic Master Frequency Files
Q13
Seismic Split Fraction Distribution File
E7
Full ETC9 Input Filea
Q5
Assignment of Split Fractions for Seismic
Q6
ETC9 (Scenario Frequency Mode)
MAX
E11
MAXIMA Direction
Q7
Scenario Fragment Frequency
Q8
Scenario Fragment Description
Q9
MAXIMA
Q10
Full Seismic Scenario List
Q11
Plant Seismic "M" Matrix
Q12
Seismic Scenario Equations
Key:
Manual Data Transfer
Electronic Data Transfer
Data Base Produced in Another Figure
Data Base Produced in This Figure

FIGURE B-12. SEISMIC ANALYSIS

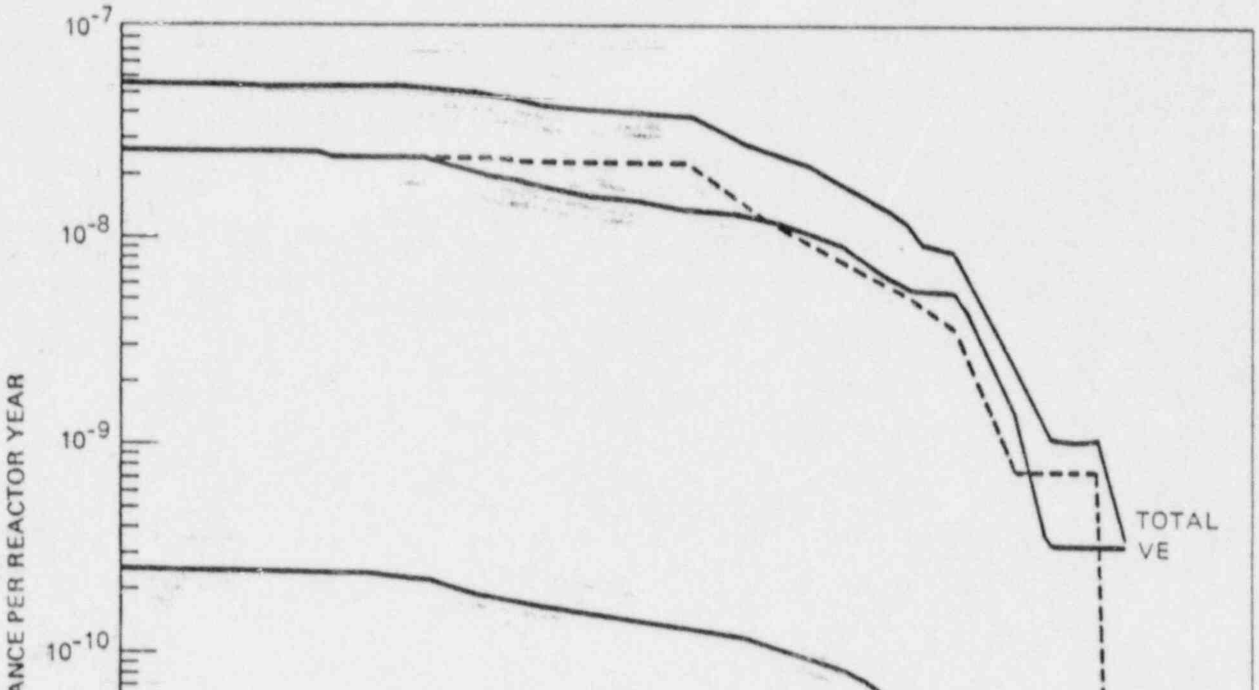


FIGURE B-13. UNCONDITIONAL FREQUENCY OF EXCEEDANCE OF EARLY FATALITIES BY PLANT DAMAGE STATE