Copy_____
PLG-0525
Volume 1

Three Mile Island Unit 1 Probabilistic Risk Assessment

EXECUTIVE 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

SUMMARY OF CONTENTS

ACKNOWLEDGMENT

In an undertaking of this size, there are many more people who contribute to the end product along the way than are identified in the title page. Key members of the TMI-1 PRA study team who participated in every major area of this assessment throughout the life of the project are members of the GPUN Risk Analysis Section. They are as follows: Ken Goddard, Section Manager, Chuck Adams, Hassan Elrada, Ed Rodrick, and (in the early stages of the project) R. Locke. Under Ken Goddard's guidance and continuous efforts, the personnel in this section contributed greatly to the ultimate content of this study. In addition to their efforts, other members of the GPU organization who made special technical contributions include: Chuck Husted, Brent Mays, Lou Lanese, and Howard Crawford.

An essential part of this analysis has been technical review. Members of the technical review board who provided expert advice and direction were as follows:

- C. D. Adams, GPU Nuclear Corporation, Safety Review Staff
- P. P. Bieniarz, Risk Management Associates
- R. W. Griebe, Aisling, Inc.
- J. M. Hudson, ACTA, Inc.
- J. E. Lynch, Babcock & Wilcox Company
- W. R. Sugnet, Electric Power Research Institute/Nuclear Safety Analysis Center
- N. G. Trikouros, GPU Nuclear Corporation, Manager of Safety Analysis and Plant Control
- G. B. Varnado, International Energy Associates, Ltd.
- J. P. Gaertner, Electric Power Research Institute
- R. W. Whitesel, GPU Nuclear Corporation, Nuclear Safety Analysis Department, Director

Special acknowledgment is made to the principal investigator, Frank Hubbard, for his untiring effort in both the technical and editorial aspects in bringing this project to a timely completion.

Other PLG staff members both in Washington, D.C., and in the Newport Beach, California, offices who participated in this project are also appreciated. Others at PLG not included on the cover page who made notable contributions are Kathleen Ramp and Tom Mikschl.

FOREWORD

This Executive Summary Report provides a concise discussion of the major results, conclusions, and recommendations of the Three Mile Island, Unit 1 (TMI-1) probabilistic risk assessment (PRA) performed by Pickard, Lowe and Garrick, Inc. (PLG), and GPU Nuclear Corporation (GPUN). It also presents an overview of the historical perspective of PRA methodology and a comparison of the results with those of some other PRAs.

In addition to this Executive Summary, this PRA is documented in a set of reports that discuss each part of the analysis as shown in Figure 1. Each report in the set is described briefly:

- Technical Summary Report. The purpose of this report is to provide an overview of the TMI-1 PRA methodology and results in more detail than is done in the Executive Summary. This report contains material necessary for understanding the following reports and should be read first.

- Plant Model Report. The Plant Model Report contains a description of all of 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 interactions between support systems and frontline systems, the plant damage states, the quantification of the plant model, and the detailed results.

- Systems Analysis Report. The Systems Analysis Report presents all of the system performance models used to calculate the numbers used for evaluating the event trees, thereby producing scenario frequencies.

- Data Analysis Report. This report presents the basic component data base (e.g., equipment failure rate and length of time to repair) developed for use in the TMI-1 PRA systems and initiating event frequency analysis. A discussion of some of the techniques used and steps taken in developing the data base is also presented.

- Human Actions Analysis Report. The Human Actions Analysis Report provides the plant event sequence models with frequencies for both favorable and unfavorable operator actions. This report quantifies the frequency of failure of the identified human actions. These frequencies are included in the plant model to delineate the human contribution to the core damage frequency.

- Environmental and External Hazards Report. The Environmental and External Hazards Report (EEHR) characterizes the impact of environmental and external hazards on TMI-1. Environmental hazards cause equipment failure from sources within the plant boundaries; e.g., fire, internal flood, steam, etc. Such environmental hazards may simultaneously affect several plant components. External hazards, on the other hand, are causes of equipment failure that originate outside the plant boundaries; e.g., earthquakes, external floods, aircraft crashes, etc. The EEHR sorts through all such hazards to determine which ones contribute significantly to core damage frequency.

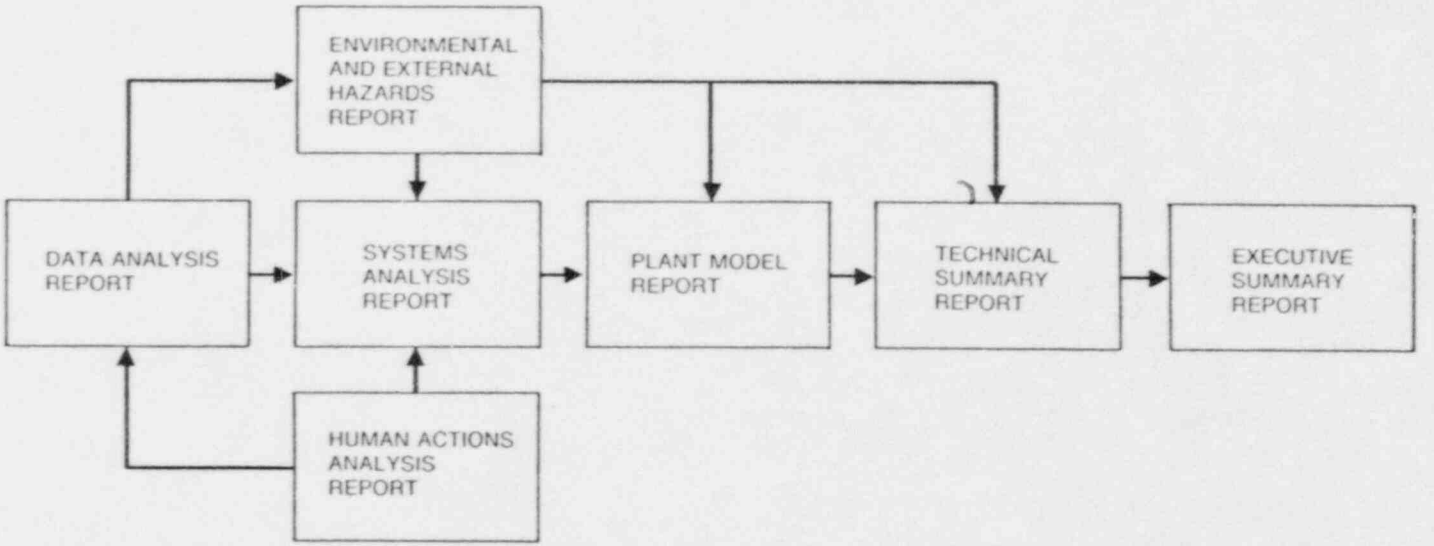


FIGURE 1. INTERACTION BETWEEN REPORTS IN THE TMI-1 PRA

CONTENTS

LIST OF TABLES AND FIGURES

1. INTRODUCTION

1.1 BACKGROUND

The TMI-1 PRA was initiated by GPUN in the fall of 1983. The consulting firm of PLG was retained as the primary contractor for the conduct of the study. It is a Level 1 PRA, as defined by the PRA Procedures Guide (Reference 1), including a treatment of external events. GPUN undertook such a study to develop a management decision-making tool that would help address various important issues, 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 the public and its employees.

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

- Provide a quantitative assessment of the range of the frequency of core damage, 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 range of the risk from operating TMI-1 in terms of the likelihood of core damage and its associated uncertainty.

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

- Rank plant systems and components quantitatively in terms of their contribution to the frequency of core damage.

- Develop a plant risk model and the tools for its use 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.

1.3 SCOPE OF THE PRA

The TMI-1 probabilistic risk assessment is a plant-specific assessment of core damage frequency, including such accident initiators as pipe breaks and the effect of floods, earthquakes, fires, and other more complex events. It includes consideration of all alleviating systems* and all systems whose failure to perform might increase the consequences produced by an initiating event. Both safety and nonsafety systems were considered for any favorable or unfavorable contribution that they might make to influence the frequency of core damage scenarios. Containment safety features were included for possible use at some later date for extending the analysis to incorporate containment response and offsite consequences.

In a truly plant-specific risk assessment like this, each plant seems to reveal its own set of dominant risk contributors. To allow early use of the PRA as a risk management tool, a "first pass," Phase I model was developed in the first 8 months of the project. Phase I was an abbreviated though a comprehensive scoping analysis intended to facilitate a more detailed and lengthy second phase. Phase I produced an approximate or focusing PRA to identify early those systems and assumptions that require more information or a more detailed analysis prior to their incorporation in the final risk model. In TMI's case, for instance, the control building ventilation system was found to be one whose failure could lead to core damage, but little was known about the course of events following its failure, including such facts as: given system failure, 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 before finalization of the control building ventilation system failure model and its incorporation into the detailed Phase II PRA model.

In Phase II, key systems and scenarios for plant safety were analyzed very closely, with the objective of identifying potential changes in design and operation. The Phase II risk model evolved over 2 years and included 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. An important result of this refinement was the treatment of human actions. These actions, while not unique to the TMI-1 PRA, were used much more extensively than in previous PRAs. They include such actions as possible miscalibration of sensors, manual actuation of systems whose automatic actuation had failed, and operator recovery of systems postulated to fail.

---

*The term "alleviating" is used throughout the TMI-1 PRA reports in the sense of 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."

In addition to producing the risk model, the scope of the PRA involved the transfer of PRA technology to GPUN staff and computer facilities. The codes involved were developed specifically to simplify the quantification of the TMI PRA model, including special input preparation codes to streamline processing.

The most important result of the TMI-1 PRA has been to identify opportunities to reduce the core damage frequency. To facilitate the continued quantitative management of the TMI-1 risk, the following additional products have been developed:

1. A final report, including this summary report and a technical summary report.

2. The PRA model, consisting of system and scenario models and data bases.

1.4 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 "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 that can actually reduce safety. With the growth of experience with operating nuclear power plants, the upper bound calculations have been replaced with an analytical approach that assesses nuclear power plant safety more realistically by putting such upper bound results into context. Probabilistic risk assessment 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). 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 3). 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 were 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 (Reference 4) 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 4, 5, and 6) and 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 4. (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 (RSS) under the direction of Professor N. C. Rasmussen of MIT (Reference 7). 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 operated at base power. The report showed the way to derive and present risk results meaningfully to technical specialists and policymakers 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 more probable transients and the small loss of coolant accidents (LOCA) that often make up most of the contribution to risk.

The accident that occurred at TMI-2 in March 1979 (Reference 8) 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 a failure of high pressure injection was included as one of the Reactor Safety Study (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 model was the likelihood that operator interruption would be the cause of the failure of high pressure injection flow. It also did not model the operator's subsequent action to restart high pressure injection (HPI) flow which prevented loss of reactor vessel integrity.

The initial reaction to the TMI accident was negative with respect to the value and role of probabilistic risk assessment; on reflection, the attitude 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 9) and the so-called Rogovin Report (Reference 10). Following the lead of these commissions' reports, several post-TMI NRC reports also noted the value of quantitative risk analysis (References 11 through 14).

A draft report of the "OPSA, Oyster Creek Probabilistic Safety Analysis," was completed in 1979 (Reference 15). It was begun before the TMI-2 event, but coincidently already included many of the features suggested by the TMI-2 post-mortem. The Zion (Reference 16) and Indian Point PRAs (Reference 17) and others performed by PLG for various utilities built on the Oyster Creek PRA methods and also 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. One impact of the above advances has been a more accurate specification of the contributors to risk. The methodology now allows identification of the contributors to risk and the ability to observe, in increasing detail, what is driving the risk. 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 contributors to risk 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 1). Developed by experienced practitioners in private industry, in the NRC, 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.

The important risk scenarios from other PRAs cannot be directly applied to TMI-1. Recent experience indicates that the scenarios important to risk are even more plant specific than realized after the early PRAs. A striking example is the difference in dominant risk contributors between the Indian Point Units 2 and 3, which are similar units located on the same site (Reference 17).

The ultimate reason for doing a risk assessment is to assist utility management in making safety-related decisions. The risk assessment provides vital input to the decision-making process. A PRA can assist in making decisions about whether to modify a plant or its procedures for operation and maintenance by comparing the calculated risk to the risk at other plants and to the Nuclear Regulatory Commission's (NRC) proposed safety goals. After the final results have been assembled, the methodology permits a clear examination of risk contributors from several different perspectives and at successive levels of detail. Risk quantified before and after any proposed change allows prediction of the effectiveness of the change. With this detail, options can be identified that can be the most effective in reducing risk.

Reduction in the frequency of core damage may result from changes in specific plant components, personnel training, or procedures. The plant-specific risk model developed in this project is designed to assist in this level of decision making.

It is also important to note that as a "model" the PRA provides an estimate of the actual but not exactly known core damage frequency. Changes to this estimate can also result from incorporation of new information, changes in study assumptions and/or better analysis methods, which do not affect the actual core damage.

2. RESULTS

This section summarizes the results of the PRA. The quantification of the frequency of core damage is presented in Section 2.1. The frequency of core damage is calculated from the sum of the frequencies of a multitude of postulated accident sequences. Each such accident sequence, or scenario, consists of an initiating event and the failure of one or more systems designed to alleviate the consequences of the initiating event. These results are presented in Section 2.2. Section 2.3 puts these results into perspective relative to regulatory guidelines and to other PRAs. Finally, Section 2.4 identifies new information that will, when incorporated into the PRA, reduce the total frequency of core damage. All of the results presented here are discussed in somewhat greater detail in the Technical Summary Report and in great detail in Section 6 of the Plant Model Report.

2.1 CORE DAMAGE FREQUENCY

The curves in Figures 2-1 and 2-2 are key results of the PRA. Both figures are presented because two formats have become widely used in PRAs to present core damage frequency and its associated uncertainty. Figure 2-1 is a probability density curve,* and Figure 2-2 is a cumulative probability curve. These curves represent our complete state of knowledge about the TMI-1 core damage frequency, including uncertainty.

Uncertainity about the frequency of core damage stems from many factors, including variation in data, modeling approximations, and incomplete information. Such uncertainty has been accounted for, to the extent possible, in all elements of the study. As shown, Figure 2-2 indicates a mean frequency of 5.5×10^{-4} per year and a median (our "best estimate") of 1.5×10^{-4}. It also communicates that the TMI-1 PRA team is 90% confident that the core damage frequency is between 2.6×10^{-4} and 9.4×10^{-4} per year.

The frequency of core damage is calculated from the sum of the frequencies of accident sequences. It is important to note that although the risk of operating TMI-1 is characterized, in part, by the core damage frequency, the actual health risk to the public can only be measured by performing containment and offsite consequence analyses. Such analyses take into account the effectiveness of containment safety systems in containing radiation leakage and the effect on public exposure of weather population distribution and evacuation during any leakage.

---

*The area under the probability density curve between any two frequency values gives the probability that the core damage frequency will be greater than or equal to the lower frequency and less than or equal to the upper frequency. The total area under the curve is equal to 1 and represents our certainty that the core damage frequency must be bounded by the frequencies under the curve. Any point on the cumulative distribution curve indicates the probability (y-axis) that core damage frequency will be less than or equal to its x-axis value.

2.2 DOMINANT CONTRIBUTORS TO CORE DAMAGE FREQUENCY

The accident sequences that contribute the most to the frequency of core damage are ranked in Table 2-1. It is interesting to note that 33% of the core damage frequency is attributable to one scenario: the loss of control building ventilation and the subsequent failure to recover it prior to core damage. (Other scenarios initiated by a loss of CBV contribute an additional 3%.) The control building ventilation (CBV) system is designed to maintain the control building rooms at normal conditions; that is, within desired limits of temperature and humidity. Failure of the ventilation system causes the internal room temperatures to increase and, within a period of hours, to exceed the design temperatures of the electronic and electrical equipment in the rooms. At some elevated temperature (which is not well known), equipment will fail, and the plant will automatically trip or be tripped by the operator. This calls on the systems to remove decay heat to operate, but, in this dominant accident sequence, these systems also eventually fail due to loss of motive and/or control power, as more electrical equipment in the control building fails. (Refer to Section 2.4 for recent information that impacts these results; also refer to Section 3.2, Technical Insights, for further discussion of loss of the control building ventilation (CBV). Core damage will result from the failure to remove decay heat. This scenario also includes the likelihood of the operator trying, but failing, to recover control building ventilation and trying, but failing, to provide alternative ventilation.

The next three highest frequency scenarios at 6%, 4%, and 4%, respectively, are fires in three different areas of the plant. The first is in the motor control center area of the auxiliary building, and the other two are in the 1S switchgear room and the engineered safeguards analysis system (ESAS) cabinet areas of the control building. These fires are assumed to interrupt either power or control to both trains of the systems required to maintain reactor coolant pump (RCP) seal integrity and provide injection flow to the reactor coolant system (RCS) following RCP seal failure. (Refer to Section 2.4 for recent information that impacts the results; also see Section 3.2, Technical Insights, for a discussion of the limitations and uncertainty in the fire analysis.)

The fifth highest frequency scenario is characterized by the occurrence of a medium LOCA and the failure to manually initiate recirculation from the reactor building sump. More specifically, this sequence requires a manual switchover of the low pressure injection pump suction from the empty borated water storage tank to the reactor building sump. Failure of the manual switchover may occur for several reasons, including failure on the part of the operator to recognize the event, failure of the low level alarm of the borated water storage tank to notify the operator of a near-empty condition, or equipment failure in the lines that take suction from the sump. This scenario contributes about 3% to the overall core damage frequency. Similar scenarios initiated by large and very small LOCAs together contribute an additional 2%.

The sixth most significant accident sequence involves three independent failures: an excessive amount of main feedwater being fed to the steam generators initiates the event, failure to provide high-pressure injection pump minimum-flow recirculation fails the reactor coolant pump

seal injection, and reactor coolant pump seal cooling also fails. In this scenario, the excessive main feedwater causes the reactor coolant system to cool down and depressurize enough to generate a 1,600-psi engineered safeguards actuation signal. This signal starts high pressure injection and closes the HPI minimum-flow recirculation line to the makeup tank among other actions. The operator then fails to reopen this recirculation line when he throttles HPI flow, causing the HPI pumps to fail. (Continued seal injection flow of 32 gpm is inadequate for minimum flow requirements of three high pressure injection pumps.) This disables both reactor coolant makeup and seal injection. The reactor coolant pump seal cooling (from ICCW) has failed due to independent causes. The pump seals, deprived of both injection and cooling, degrade and leak, causing a loss of RCS inventory. Since makeup is not available due to the failed makeup pumps, core uncovery and damage eventually occur. The scenario is commonly referred to as an "RCP seal LOCA." Refer to Section 4 for a discussion of recent information that may impact these results.

As a further means of identifying the major risk contributors in the plant, we can focus on the events that initiate scenarios. The loss of control building ventilation initiates the most important scenario of Table 2-1. The importance of events that initiate many scenarios of small individual contributions to core damage frequency is not so obvious. Their importance then can only be known by tallying their total contribution to core damage frequency, as shown in Table 2-2.

The scenarios can be examined at yet a greater level of detail; namely, at the systems level. That is, the large number of scenarios considered in the TMI-1 PRA were further analyzed to find the system failures that dominate the frequency of severe core damage. These results are presented in Table 2-3. The importance of these systems was calculated by adding the frequency of all scenarios in which the failure of a particular system occurs. Therefore, the total percentage of all contributing systems may exceed 100% because more than one system failure may occur in each core damage scenario.*

2.3 RESULTS IN CONTEXT

The TMI-1 PRA represents an extensive application of state-of-the-art risk assessment methodology. This section briefly examines the differences between the methods used and the results calculated for TMI-1 and those assessed in risk studies for other nuclear power plants, as

---

*The importance percentage calculated in this way usually indicates the percentage reduction in core damage frequency, which 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%. One exception to this rule is for cases when a containment safety feature has failed but the system does not contribute to core damage. Fixing the containment safety feature in this case will not reduce core damage frequency. Another exception is when there are two systems failed in the scenario, either one of which would, by itself, lead to core damage. Fixing one such system would not reduce the total core damage frequency.

shown in Table 2-4. These comparisons consider differences in PRA methodology, plant design, and statistical representation of the results. The differences identified in the comparison illustrate the need for extreme caution in making such comparisons. Comparisons are meaningful only when there is commonality of such items as initiating events, basic event data, scope, and methods of calculating uncertainty.

As indicated in Table 2-4, the TMI-1 PRA core damage frequency is relatively high in comparison to the results from other PRAs. A major reason for this is the nature of the major contributors to core damage frequency and the assumptions used in the quantification of their frequency. Two major contributors (responsible for approximately half of the TMI-1 total) are loss of control building ventilation and fires in electrical equipment rooms. Section 2.4 describes the potential impact of new information on reducing the core damage frequency from these contributors.

These scenarios were not treated in detail in most of the other studies referenced in Table 2-4. Other studies might also be at a more refined point in terms of incorporating modifications to reduce the frequency of such scenarios. In addition to these major items, the comparison to the results of other PRAs may be affected by differences in PRA methodology and assumptions. Some examples of such differences are:

- Treatment of Potential Common Cause Failures. Potential common cause failures of identical redundant equipment have not been treated the same in all PRAs. Later PRAs, especially PLG's, have used advanced methodology. For instance, in the case of the TMI-1 PRA, the analysis used generic and all available TMI-1 specific data. These data were used consistently for analyzing the failure rate of identical components (e.g., valves and pumps) within and across redundant trains of all systems. The results of other PRAs, those using the Interim Reliability Evaluation Program (IREP) methodology, for example, do not include the impact of this state-of-the-art treatment of common cause failures.

- Accounting for the Impact of Potential Human Actions. Human actions were considered extensively in the TMI-1 PRA. Approximately one-half of all the human actions analyzed were those taken to recover failed systems. A very consistent, uniform method was used to document the basis for the human action numbers used in the TMI-1 PRA; therefore, the TMI-1 PRA team did not hesitate to incorporate such actions where appropriate. The operator was never automatically assumed to be successful. On a case-by-case basis his actions were carefully characterized and the likelihood of success was quantified. Wherever such analysis was not performed the operator was assumed to have been unsuccessful.

Systems analysis in all the PRAs generally use the techniques developed for reliability analysis. System logic models are developed as a framework for analyzing accident sequences that may lead to core melt. These models are used to analyze the top events (headings) of event trees and the systems that support the top events. Generally, the systems analysis of the Limerick and Big Rock Point PRAs was similar to the Reactor Safety Study. The Reactor Safety Study methodology application

(RSSMAP) of Oconee, Sequoyah, and Grand Gulf drew directly from RSS experience. Midland, Oconee, Susquehanna, Seabrook, Bellefonte, Browns Ferry, South Texas, Pilgrim, Salem, Hatch, Nine Mile Point, Indian Point and Zion PRAs have taken advantage of more recent advances in systems analysis methods; e.g., the treatment of dependent failures. While the RSS employed conservative success criteria for system operability, later PRAs, including RSSMAP studies, used new information (for example from the Three Mile Island Unit 2 studies), resulting, in some cases, in less conservative (more realistic) criteria.

More recent studies, including the TMI-PRA, are considering a more complete set of initiating events. For instance, steam generator tube ruptures and fires were measurable contributors in the TMI-PRA but were judged to be unimportant and therefore not studied explicitly in the Reactor Safety Study and other risk assessments.

For external events, such as fire, earthquake, tornado, hurricane, and flood, the RSS performed a scoping overview analysis and concluded that the risk due to these events is less than the risk resulting from other causes. External event analysis was not within the scope of the Limerick and RSSMAP PRAs. Big Rock Point analyzed fires and earthquakes and found fires, in particular, to be important to the overall risk. For Zion and Indian Point, earthquakes were found to be important, especially for latent health effects. This was because an earthquake could result in both core damage and containment failure. Otherwise, the joint frequency of core damage from an internal initiating event and the independent, subsequent failure of Zion's very high capacity containment is much lower.

The TMI-PRA modeled more scenarios than generally considered in other PRAs. This was done because the effects of interdependencies among systems were found to be very important at TMI-1. This includes support systems (e.g. electric power or cooling water), which have been found to be as important as at most other plants examined to date. As a result, dependency between systems were necessarily treated in more detail in the TMI-PRA.

The RSS compiled component failure data from a variety of sources, establishing a benchmark data base. Some updates based on recent industry and plant-specific experience were made for the TMI-1, Midland, Oconee, Limerick, Big Rock Point, Zion, and Indian Point PRAs. TMI-1 adopted and, in some cases, extended the data techniques used in previous PLG PRAs.

Human interaction and reliability analyses were performed at the system and sequence level in the RSS analysis. These interactions were quantified by new techniques that have subsequently been incorporated in to the Swain and Guttmann handbook (NUREG/CR-1278) (Reference 18). Subsequent PRAs have employed this handbook extensively. The Zion and Indian Point studies first introduced some specific operator actions into their event trees. The TMI-1 PRA considerably extends consideration of operator actions. Operator actions to recover failed systems were found to be important to reducing risk at Midland and even more important at TMI-1.

Common cause failure of identical components was included in the system models. Advances in the methodology of treatment of common cause failure since the Reactor Safety Study have resulted in the use of the beta factor or "multiple Greek letter" method in the TMI-1 PRA. This method distinguishes between multiple failures of two or three components. Details of this methodology can be found in Section 2.2, (Common Cause Failure Parameters) of the Data Analysis Report.

Uncertainty analysis and the inclusion of uncertainty in representing the results is an essential part of any PRA. Not all Interim Reliability Evaluation Program and RSSMAP PRAs represented their uncertainties quantitatively. The TMI-1 PRA made a special effort to quantify the uncertainty in the results. The use of frequency distributions rather than point estimates for core damage frequency is seen as an important improvement toward increasing the confidence, rigor, and credibility of the risk assessments.

Some PRAs, such as Limerick's, refer to point estimates of risk without associating with these numbers any statistical parameter, such as mean, median, or mode. The RSS "best estimate" values were represented as medians, and judgmental "uncertainty factors" were estimated for the final frequency and consequence values. The risk estimates were assumed to be lognormally distributed. The RSS median core melt frequency is 6×10^{-5} for pressurized water reactors (PWR), with an approximate uncertainty factor of 5. Based on the lognormal distribution, one obtains a mean value of 1.3×10^{-4} for the RSS.

Point estimates reported in all studies, except those for Oyster Creek, Zion, Big Rock Point (BRP), and Indian Point, were medians; that is, "best estimates" or 50th percentile results. In this type of work, mean values will almost always be higher than the medians; therefore, comparisons among results of various PRAs should be made by using equivalent statistical parameters; i.e., means should be compared to means and medians to medians, but not means to medians. In addition, since the TMI-1 PRA includes the impact of external events, its results should only be compared to those of other PRAs that also included external events.

2.4 IMPACT OF RECENT INFORMATION

Any PRA is a model and a living document. As such, it provides an estimate of the actual but unknown core damage frequency and is subject to change as a result of new information and changes to study assumptions. Since the results presented in this report were calculated, additional information has been received, which indicates that the contribution from some events has been overestimated. This information will reduce the uncertainty associated with and the mean frequency of a number of major contributors to the core damage frequency. This will also decrease the mean frequency of core damage. New information has been received about the effects of the loss of control building ventilation and the consequences of fires in the control building. Also, recent tests of the effect on reactor coolant pump seals of losing both cooling and injection indicate that more time may be available before leakage becomes large. All of this information, if it eliminated the

contributions of loss of CBV and of the most important fires, could reduce core damage frequency by up to approximately 50%.

2.4.1 LOSS OF CONTROL BUILDING VENTILATION

Included in the frequency of loss of control building ventilation scenarios that go to core damage is the likelihood that the operator recovers cooling to the equipment in the control building before the room temperatures reach 104°F. At 104°F, equipment required to maintain reactor coolant pump seal injection or cooling and mitigate the failure of the seals is assumed to be lost. Tests in September of 1987 have indicated that more time is available for operator action prior to the hottest rooms reaching 104°F. It may, in fact, take as long as 24 hours for these rooms to reach 104°F. This longer time is due to initial overestimations of the heat generation rates in these rooms. In addition, the outside air temperatures for which temporary ventilation would be effective can therefore be higher. More time available for recovery will result in a higher likelihood that the operator will succeed in establishing alternative ventilation. This higher likelihood will reduce the frequency of loss of control building ventilation scenarios that go to core damage, thus reducing the total core damage frequency. If the heatup is slow enough so the operator has more than enough time to perform the action successfully, then the frequency of the scenario will become insignificant. Because the total contribution of these scenarios is currently so great, any change in their contribution would significantly reduce the total core damage frequency. The results of these recent tests will be reviewed and their impact on the estimated core damage frequency will be incorporated into the next revision of the PRA.

2.4.2 FIRE HAZARD SCENARIOS

Two areas of recent changes relative to the PRA fire scenario frequencies are:

1. Additional Appendix R modifications made after completion of the PRA analysis. For instance, power is now removed from some valves during normal operation, which precludes their actuation by hot shorts during a fire that is currently considered in the PRA.

2. New procedures have been put into place to provide more guidance on equipment operation and recovery for specific fires. Among the fires to which these procedures apply are those of the most importance in the PRA. These procedures provide guidance for the operator, from the control room or from the remote shutdown panel, to operate equipment more effectively, which will prevent or mitigate RCP seal failures.

2.4.3 REACTOR COOLANT PUMP SEALS

Tests performed by the Westinghouse Electric Company on RCP seals (Reference 19) under loss of all AC power conditions have shown that reactor coolant pump seals leaked no more than 16 gpm during the 20-hour

test. It is believed that these tests may be representative of the seals for the reactor coolant pumps at TMI-1.

Except for station blackout and loss of river water scenarios, no credit was taken in the PRA for recovery of seal cooling and/or seal injection in scenarios after both were lost. Seal LOCAs occur, as noted previously in the loss of control building ventilation scenarios, in all the fire scenarios that were explicitly modeled, and in other scenarios in which multiple independent failures occur.

Incorporation of these actions and additional recovery time, which the Westinghouse tests indicate are available, will significantly increase the likelihood of successful accomplishment of these and such actions that already exist in the PRA. Increasing the application of recovery and the likelihood of successful recovery will reduce the frequency of core damage scenarios that contain the failure of seal injection and cooling, thus reducing the total core damage frequency.

TABLE 2-1. SCENARIOS CONTRIBUTING SIGNIFICANTLY TO CORE DAMAGE FREQUENCY*

Order Number	Description	RCP Seal Failure	Contribution to Severe Core Damage Frequency (percent)	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}

*If all scenarios were listed, the total contribution to the core damage frequency would equal 100%.
**Long-term decay heat removal is also unavailable.
†Seal cooling and injection are both failed.

TABLE 2-1 (continued)

Sheet 2 of 2

Order Number	Description	RCP Seal Failure	Contribution to Severe Core Damage Frequency (percent)	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}
		Subtotal	56.5	3.10×10^{-4}
		All Other Scenarios	43.5	2.4×10^{-4}
		Total	100	5.5×10^{-4}

*Seal cooling and injection are both failed.

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

Description	Percent Contribution to Core Damage Frequency	Mean Frequency per Reactor Year
INTERNAL	80.6	4.43×10^{-4}
Loss of Support Systems:	52.8	
Loss of CBV	36.4	2.00×10^{-4}
Others	8.2	4.53×10^{-5}
Loss of Offsite Power*	5.	2.90×10^{-5}
Loss of River Water to Pumphouse	2.	1.58×10^{-5}
All Other Transients	11.1	6.09×10^{-5}
Very Small LOCAs (including steam generator tube rupture)	10.1	5.58×10^{-5}
All Larger LOCAs	6.5	3.58×10^{-5}
LOCA outside Containment	< 0.1	1.00×10^{-7}
EXTERNAL	19.4	1.07×10^{-4}
Fires Explicitly Modeled**	15.7	8.64×10^{-5}
All Other Fires and All Internal Floods	< 2	$< 1.00 \times 10^{-5}$
Earthquakes	0.5	2.70×10^{-6}
External Flood	1.4	7.5×10^{-6}
Tornado	<< 0.1	1.2×10^{-8}
Turbine Missile	< 0.1	2.3×10^{-7}
Aircraft Crash	< 0.1	1.0×10^{-7}
Toxic Chemical	< 0.1	2.6×10^{-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 2-3. SYSTEMS CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE FROM INTERNAL EVENTS

System	System Total Contribution to Core Damage Frequency From Internal Events
Control Building Ventilation	43%
Decay Heat Removal	37%
High Pressure Injection	37%
Electric Power	24%
Main Steam and Feedwater	23%
RCS Pressure Control	22%
Decay Heat Cooling Water	21%
Intermediate Closed Cooling Water	9%
Emergency Feedwater	6%
Instrument Air	4%
Nuclear Services Cooling Water	4%
Engineered Safeguards Actuation	2%
Reactor Protection	1%

NOTE: A system's contribution is calculated by adding the frequency of all sequences in which the failure of the system occurs and core damage results. This sum is then divided by the total core damage frequency from internal events only to calculate the percentage contribution from each system. Since more than one system failure may occur in each core damage sequence, the total percentage due to all system contributions exceeds 100%. These precentages are higher than would be obtained by basing them on the total core damage frequency.

TABLE 2-4. CORE MELT FREQUENCY COMPARISON
(Occurrences per Reactor Year)

PRA Study	Median	Mean	Scope and Date Published	Plant Vendor	Assessment Team	Sponsor
PWRs						
TMI-1 - Internal Internal and External	3.5×10^{-4} 4.5×10^{-4}	4.4×10^{-4} 5.5×10^{-4}	Level 1 01/87	Babcock & Wilcox	PLG/GPUN	General Public Utilities Nuclear
Midland Internal and External	2.1×10^{-4}	3.1×10^{-4}	Level 2 05/84	Babcock & Wilcox	PLG	Consumers Power Company
Indian Point 2 - Internal Internal and External	5.0×10^{-5} 1.0×10^{-4}	7.9×10^{-5} 1.4×10^{-4}	* 04/82	Westinghouse	PLG	Consolidated Edison Company
Indian Point 3 - Internal Internal and External	3.0×10^{-5} 5.0×10^{-5}	1.3×10^{-4} 1.4×10^{-4}	* 04/82	Westinghouse	PLG	Consolidated Edison Company
RSS-Surry-Internal	6.0×10^{-5}	1.2×10^{-4}*	Level 3 10/75	Westinghouse	WASH-1400	AEC NRC
Zion - Internal Internal and External	5.0×10^{-5} 5.2×10^{-5}	5.7×10^{-5} 6.7×10^{-5}	Level 3 09/81	Westinghouse	PLG	Commonwealth Edison
DRS Internal	4.0×10^{-5}	9.6×10^{-5}	Level 3			
Oconee-Internal	2.0×10^{-4}	4.0×10^{-4}*	Level 2 05/81	Babcock & Wilcox	RSSMAP	NRC
Sequoyah	6.0×10^{-5}	1.2×10^{-4}*	Level 2 02/81	Westinghouse	RSSMAP	NRC
Arkansas Nuclear One - Internal	5×10^{-5}		Level 2 06/82	Babcock & Wilcox	IREP	NRC
Calvert Cliffs - Internal	2×10^{-3}		Level 2 05/82	Combustion Engineering	IREP	NRC
Crystal River	4×10^{-4}		Level 2 12/81	Babcock & Wilcox	SAI	NRC/IREP
Bellefonte Unit 1 - Internal and External	Between 10^{-4} and 10^{-3}		Level 1 10/85	Babcock & Wilcox	PLG	Tennessee Valley Authority
Seabrook - Internal and External	1.9×10^{-4}	2.3×10^{-4}	Level 3 12/83	Westinghouse	PLG	Public Service Company of New Hampshire
Oconee Unit 3 - Internal and External	1.8×10^{-4}	2.5×10^{-4}	Level 3 06/84	Babcock & Wilcox	Duke Power Company/NSAC	Electric Power Research Institute
BWRs						
Grand Gulf - Internal	3.0×10^{-5}	6.0×10^{-5}*	Level 2 10/81	General Electric	RSSMAP	NRC
RSS-Peach Bottom Internal	3.0×10^{-5}	6.0×10^{-5}	Level 3 10/75	General Electric	WASH-1400	AEC/NRC
Limerick - Internal	1.5×10^{-5}	2.8×10^{-5}	Level 3 09/82	General Electric	SAI	Philadelphia Electric Company
Browns Ferry Unit 1 - Internal	2×10^{-4}		Level 2 07/82	General Electric	IREP	NRC

*Calculated from the median; assumes lognormal distribution; uncertainty factor of 5.

TABLE 2-4 (continued)

PRA Study	Median	Mean	Scope and Date Published	Plant Vendor	Assessment Team	Sponsor
Millstone - Internal and External	3×10^{-4}		Level 2 01/82	General Electric	Westinghouse	Northeast Utilities Service Company
Pilgrim - Internal and External	7.6×10^{-5}	9.0×10^{-5}	Level 1 Phase I 11/86	General Electric	PLG	Boston Edison Company
Hatch - Internal	4.6×10^{-4}	1.0×10^{-3}	Level 1 Phase I 04/86	General Electric	PLG	Georgia Power Company

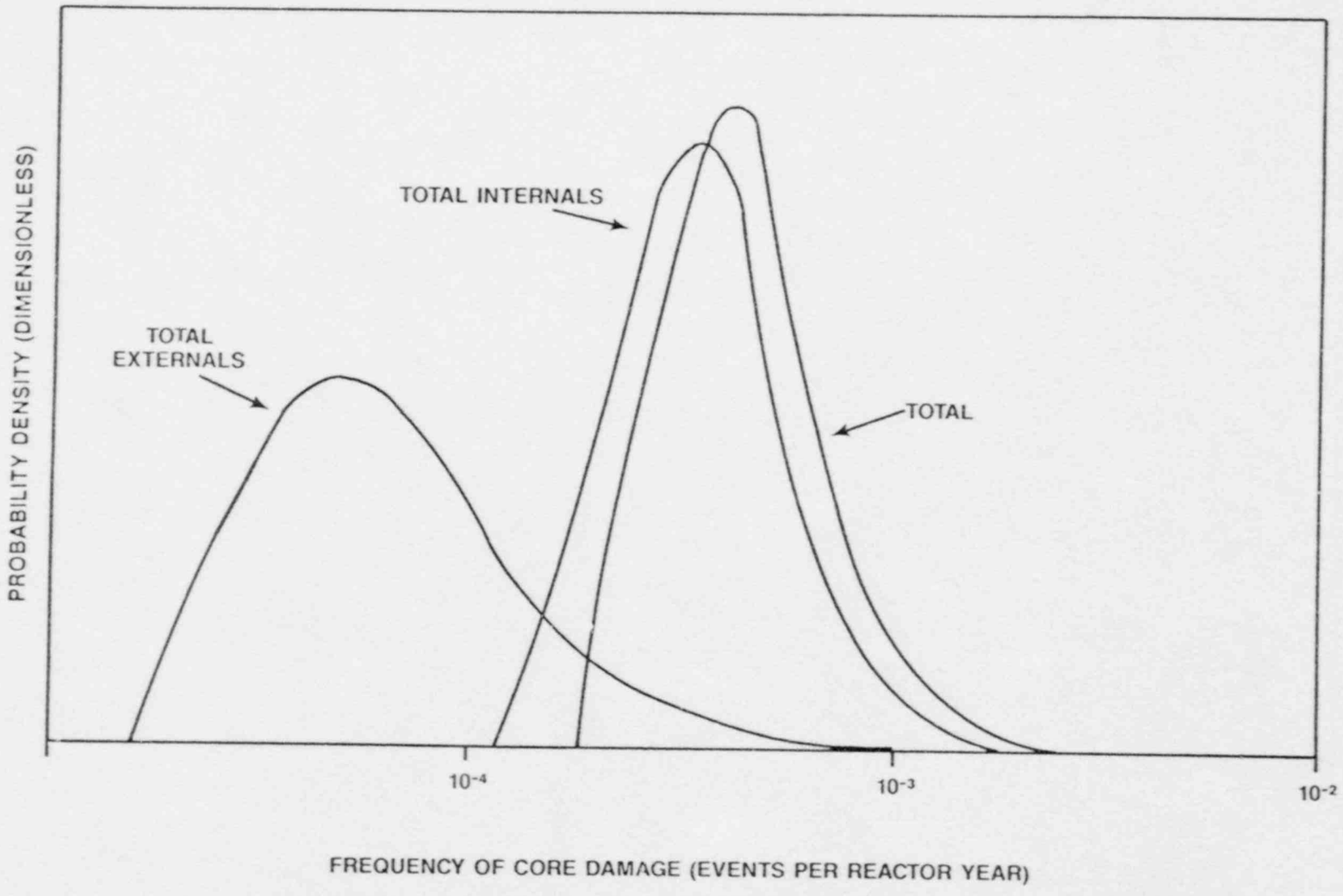
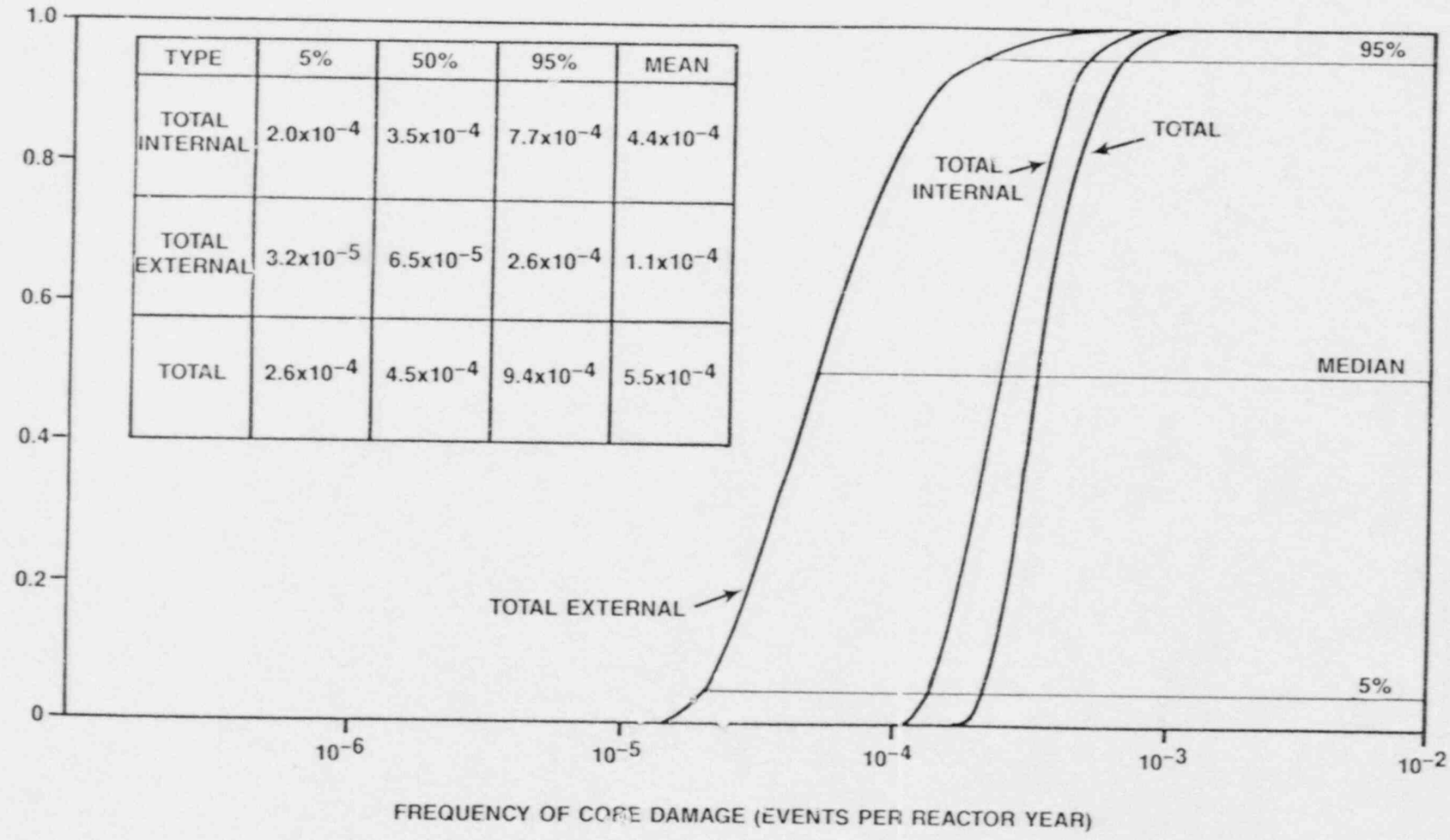


FIGURE 2-1. TMI-1 PRA PROBABILITY OF CORE DAMAGE FREQUENCY DISTRIBUTIONS (PROBABILITY DENSITY FORMAT)



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 2-2. TMI-1 PRA PROBABILITY OF CORE DAMAGE FREQUENCY DISTRIBUTIONS (CUMULATIVE PROBABILITY FORMAT)

3. INSIGHTS AND RECOMMENDATIONS

The TMI-1 PRA has produced a number of operational modifications and several technical insights into the operation of the plant. Based on the results* of this PRA, it has been possible to identify the most meaningful actions to be taken to better understand the contributors to, and to reduce the frequency of, core damage. These are presented in Section 3.3.

As a result of the TMI-1 PRA, a number of technical insights into the operation of the plant were gained. These insights and the resulting recommendations (some of which were incorporated early enough to be used within the analysis) are presented in Sections 3.1 and 3.2.

3.1 OPERATIONAL CHANGES RESULTING FROM AND INCORPORATED INTO THE PRA

These changes were:

- The system analyses for the reactor building emergency cooling water system identifed that it was possible for the system discharge valve to fail to open, when required, and possibly go undetected due to lack of definitive instrumentation and procedures. As a result, changes were made to the system surveillance procedures, alarm response procedures, and operator training material. These changes provided an effective increase in the opportunity for operator action, which was credited in the analysis.

- Early and current results of the TMI-1 PRA show failures in the control building ventilation system (CBVS) to be large contributors to core damage frequency. Recommendations were made that will result in changes to the CBVS emergency procedures. These changes incorporate the use of emergency fans to cool the engineered safeguards electrical equipment if normal ventilation is lost. Credit was taken for these changes in the analysis. (Note: All equipment necessary for operators to use these revised procedures has been procured; however, the connections required to attach them to existing plant duct work are not complete as of October 1987.)

- The makeup and purification system operating procedure and the engineered safeguard system status checklist were revised to ensure that when makeup pump B is selected for engineered safeguards actuation, its corresponding lube oil pumps are powered from the same electrical power train as the B makeup pump. This prevents a mismatch from taking place.

*Recent information based on tests of TMI control building ventilation system and a review of assumptions used in determining the effects of important fire scenarios are discussed in Section 2.4.

3.2 TECHNICAL INSIGHTS

Foremost among the insights gained by the PRA is the recognition of factors underlying the greatest portion of risk at TMI-1. These factors and their relative contribution to risk are described below.

- Failures of Support Systems, Including Control Building Ventilation. As shown in Table 2-3, failures of support systems contribute to a major part of the calculated core damage frequency at TMI-1. The predominant support system failure is that of the control building ventilation system (43%), which, in turn, fails the safety-related AC and DC power to plant systems and leads to a failure to remove decay heat.

  Other support system failures contributing significantly to core damage frequency are electric power (24%), the decay heat river water and closed cooling water systems (21%), intermediate closed cooling water for reactor coolant pump seal cooling (9%), instrument air (4%), and nuclear services cooling water (4%).

- Reactor Coolant Pump Seals. Failure of RCP seal cooling and seal injection is believed to lead to degradation, leakage, and eventual failure of the seals, even with the pumps not running, as long as the RCS is hot and pressurized. Such failures, called "seal LOCAs," that are accompanied by loss of HPI flow occur in scenarios that account for a majority of the core damage frequency in this study. Changing knowledge about seal LOCAs would not necessarily eliminate their contributing the same portion of the calculated core damage frequency, however, since many of the seal LOCA scenarios (such as loss of CBVS described above) would eventually lead to core damage anyway because of the failure to remove decay heat. In many such scenarios, however, seal LOCAs will dictate the time available to recover systems and prevent core damage.

- Operator Actions. Many operator actions are modeled in the PRA, and their inclusion is an important factor in preventing core damage in many sequences. (These actions and their importance are summarized in Table 3-1.) Such sequences include many in which the operators successfully restore failed systems (control building ventilation, decay heat closed cooling water or decay heat river water, and offsite or onsite power) or initiate a system when automatic initiation has failed (reactor protection; engineered safety features actuation). However, many core damage sequences include failures by the operators to take a procedural action; e.g., switchover from injection to recirculate following a LOCA, providing HPI pump minimum flow recirculation when throttling HPI, and initiating HPI cooling.

- Fires. This study included many of the fire protection modifications made at TMI-1 to comply with 10CFR50 Appendix R. However, the PRA fire analysis included the likelihood (albeit small) of fires more intense than those considered in Appendix R. These low frequency fires would be intense enough to compromise the fire barriers provided in accordance with Appendix R to protect equipment in the area of the fire. The possibility of such fires is substantiated by

the industry data (see Section 3 of the Environmental and External Hazards Report), including the Licensee Event Reports that identify the occurrence of degradation of fire barriers and of failures of administrative controls. These low frequency fires contribute approximately 15% to the frequency of core damage. All such scenarios involve seal LOCAs with failure of makeup to the RCS.

The models and data for fire frequency, severity, propagation, and suppression are not as well refined as those used for other parts of the PRA. Therefore, the uncertainty associated with the results of the fire analysis is higher. Among the major assumptions made in performing the fire analysis that contributed to this increased uncertainty by requiring more analyst judgment, were:

- Probability and Location of Critical Fires
- Fire Growth and Propagation
- Fire Suppression
- Hot Shorts

(See Section 3, Spatial Interactions of the Environmental and External Hazards Report for a detailed discussion of the assumptions involved in, and the limitations of, this analysis.)

- Train Dependency in Decay Heat Removal. At TMI-1, the decay heat river water, closed cooling water, and decay heat removal systems are composed of two separate trains without cross-connection capability from the control room. The decay heat removal (DHR) system is the only system with cross-connection valves between the trains and these are manual valves. As a result, a large number of combinations of unavailabilities or failures of two components, one in each train, can lead to failure of the DHR function. Also, failure of one DHR train with failure of the opposite train of AC or DC power is important. Although operator actions will mitigate many of these occurrences, train dependency still leads to a high core damage contribution.

- Distribution of Core Damage Frequency. Although the major part of core damage frequency is attributable to sequences discussed above, a significant portion of the frequency is accounted for by a large number of low frequency sequences. This makes it difficult to discuss these sequences or to develop meaningful insights from them except by looking at system actions that occur in many scenarios.

3.3 RECOMMENDATIONS

The following recommendations were based on the insights described in Section 3.2 and on other findings during the PRA. These recommendations are the product of the thinking of many people at GPUN, PLG, and attendees of the Technical Review Board meetings. The recommendations have not been subject to "cost-benefit" analysis, and before significant expenditures are made, such analysis will be required. As a follow-on activity to the PRA, the benefit in terms of core damage frequency reduction and the various costs associated with acting on each of these recommendations should be quantified and compared to other options for controlling and reducing risk.

- Control Building Ventilation System. Since failures of the control building ventilation system contribute to 43% of the total core damage frequency from internal events, several actions are recommended to better understand this problem, improve the reliability of the system, and improve the operator's ability to cope with system failures.

  - The temperatures at which equipment in the control building would fail is an important assumption in the analysis. More accurate estimates of these temperatures should be pursued. If the failure temperatures are higher, more time will be available for system recovery, and some equipment may not fail at all.

  - A procedure to provide temporary emergency ventilation to critical areas of the control building by using portable fans should be instituted. Development of this procedure started as a result of the PRA, and the PRA CBVS analysis takes credit for the existence of this procedure. (Note: The viability of any such procedure is still limited by the outside air temperature.)

  - As an alternative or as a supplement to the above procedure, a procedure for reducing the loading on buses in the control building (and thus reducing the heat generation rates) could be instituted. If sufficient time is available, reducing loads is less desirable than using temporary emergency ventilation because reducing load minimizes the equipment available for use during the shutdown.

  - Certain minor modifications to the CBVS could reduce or eliminate some system failure modes.

    - Currently, all of the second-floor area isolation dampers are supplied from one power supply, and all of the third-floor area isolation dampers are fed from another power supply. A rearrangement of these power supplies could reduce the vulnerability of room cooling to failure of a single DC power supply.

    - Indication in the control room of the CBVS inlet, outlet, and recirculation dampers does not show actual damper position. Providing indication to the operators from limit switches would make timely response to a damper failure more likely.

    - The CBVS control air supply is vulnerable to flooding or fires in the area of the compressors. A backup air supply from the plant instrument air system would reduce this vulnerability.

  - Investigate improvements in maintenance, spare parts inventories, and job [illegible] that would reduce the time needed to restore the system to [illegible]on after a failure and therefore would reduce the unavai[illegible]ities of CBVS equipment.

- Reactor Coolant Pump Seals. Because RCP seal leakage and failure following loss of seal injection and seal cooling are important in many core damage scenarios, a better understanding of this issue is important and improvements to these important support systems should be sought.

  - GPUN should follow industry activities on the subject of RCP seal integrity and factor what is learned into design, maintenance, and operations, as well as into the PRA.

  - The intermediate closed cooling water pump discharge check valves have a history of failure that impacts the reliability of that system for providing RCP seal cooling. Improvements in design or maintenance should be investigated.

  - Loss of instrument air causes loss of both seal cooling and seal injection. Improvements to air system reliability are thus valuable. The new air dryers should improve system reliability although the dryer transfer mechanism is still a vulnerability that requires prompt operator action in case of failure (to avert a plant trip and loss of RCP seal cooling).

  - Procedures and training should emphasize the importance of seal cooling, seal injection, and the actions necessary to prevent seal damage.

- Fires. The fire hazard scenarios, which were signficant contributors to the core damage frequency in the TMI-1 PRA, should be examined more carefully to confirm the validity of the assumptions about which cables and other equipment are damaged. All Appendix R modifications that have been completed to date and recovery actions currently in procedures should be included in the PRA model. If they continue to be important scenarios, the values used for frequency of occurrence, severity and nonsuppression factors should be further analyzed to reduce the uncertainty associated with them.

- Onsite Electric Power. Failures in the onsite electric power system are significant contributors to core damage frequency. Several vulnerabilities and potential improvements have been identified.

  - TMI-1 diesel generators have starting failure rates comparable to the industry average, but higher than average maintenance unavailabilities primarily caused by preventive maintenance. Unavailability due to preventive maintenance stems from scheduling maintenance during periods of plant operation. The maintenance program and scheduling should be evaluated with the aim of achieving the lowest possible total unavailability for the diesel generators.

  - During automatic start attempts of the emergency diesel generators caused by an engineered safeguards actuation signal, the diesel shutdown relays are blocked, which allows starting air to continue flowing to the engines until the air supply is exhausted. For nonengineered safeguards starts if the engines are not running within 7 seconds (as evidenced by oil pressure

and RPM), the air supply valves close. Closing the valves conserves air and allows the operator to correct the cause of the start failure and make another start attempt without having to recharge the air supply tanks. A modification to the starting circuit is recommended to allow multiple start attempts even during engineered safeguards automatic starts.

- In scenarios in which AC power sources are lost, the time for which DC power will continue to be available for instrumentation and control is an important factor. Battery capacity, loads, and procedures for conserving DC power should be reviewed with the aim of maximizing the time available before DC power would be lost.

- Offsite Electric Power. The ability to restore offsite power after an extended loss could be jeopardized by the design of the switchyard in which power for air compressors and breaker heaters comes from the switchyard itself. In cold weather, a station blackout could result in the breakers becoming inoperable after some period of time, as the SF_6 gas cools down. Two additional 100-kW diesel generators, separate from the plant emergency diesel generators, are presently being procured to mitigate this situation.

- Decay Heat Removal, Closed Cooling Water, and River Water. Combinations of unavailability or failure of components in these systems (or associated power supplies) contribute significantly to core damage frequency. This is due largely to the strict separation of the trains, which produces many pairs of train A and B failures. Two areas of improvement seem worthwhile. First, the unavailability of decay heat removal trains could be reduced. This requires an examination of maintenance policies and practices. Second, the ability to cross-connect trains mechanically and/or electrically should be examined. This will require some modifications. The ability to back up decay heat river water with another river water source (as can be done with nuclear services and secondary services river water) should be considered.

- High Pressure Injection. The HPI system and several operator actions associated with it appear as important contributors to core damage frequency. Recommendations relating exclusively to operator actions are described later in this section. Certain aspects of the HPI system design should be considered for possible improvement.

  - Failure of the operator to open MU-V-36 and MU-V-37 to provide a recirculation flow path for the HPI pumps when throttling HPI or makeup could be avoided by leaving those valves open at all times or by providing an automatic opening signal on low flow. The former is preferable for both reliability and simplicity and should be pursued.

- BWST suction valves (MU-V-14A and MU-V-14B) failure leads to almost immediate HPI pump failure. Operating with the suction crossties open would provide increased reliability, but would introduce a possible single failure (pipe break) for the HPI system. This change is being investigated.

- The "B" HPI pump oil pumps are powered from bus 1C, which may be fed from a different AC power train than HPI pump B itself, although procedures have been modified to reduce the time in this configuration. The automatic transfer of bus 1C is blocked by an engineered safeguards signal. (A similar situation exists with nuclear services river water pump B and its discharge valve.) Consideration should be given to removing the engineered safeguards block, or to some other method of eliminating this failure mode.

- LOCA Outside the Reactor Building (V-Sequence). Although this sequence is not a major contributor to core damage frequency at TMI-1, it could be reduced even further. Current testing procedures incorporate precautions and make operators aware of V-sequence hazards. They reduce the estimated risk by allowing the operator to detect leakage prior to fully opening the valves. The frequency of testing the DH-V-4A and DH-V-4B valves during operation should be investigated to determine if a reduction in risk could be achieved by a change in test frequency. Operator training and procedures should be modified to specifically address breaks outside the reactor building.

- Preventive Maintenance. Preventive maintenance is important for ensuring the reliable performance of components and systems. However, the time that a component or system is out of service for preventive maintenance is also one contributor to the unavailability of the system. In the case of some systems at TMI, this contribution is significant. For example, desilting the intake screen and pump house causes a large portion of the unavailability of the river water pumps, and the yearly overhaul of the emergency diesel generators significantly increases the time that the diesels are unavailable during TMI-1 operations. We recommend that the preventive maintenance program, policies, and practices be reviewed and revised, when necessary, to achieve the highest possible system availability (which means minimizing the sum of all of the contributors to unavailability).

- Operator Actions. 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 a portion of the scenarios. Some of these actions are discussed in other sections, with recommendations for improvement of the systems involved. Others included are:

- Failure to switch over from injection to recirculation after a LOCA is the dominant source of recirculation failure. The major portion of this failure is due to human error. The assumptions used in the human error calculation leading to this conclusion should be reexamined, and, if validated, several corrective actions should be pursued. One option would be to automate the opening of the sump suction valves on low BWST level. (Note: The reliability of this automatic action would also have to be calculated and factored into the calculation of core damage frequency.) Another option would be to improve training and procedures to allow the operators to perform this task with a higher reliability.

- Failure to provide HPI pump minimum-flow recirculation was discussed elsewhere with potential system improvements. If these system improvements are not feasible, then improvements in training, and procedures are in order to improve the reliability of this human action.

- Failure to initiate HPI cooling is the most significant cause of failure of the HPI core cooling mode. The human action analysis involved should be examined for any actions that increase the reliability of HPI cooling initiation. If no means of automating the action is feasible (and none has been suggested), efforts will have to be directed to operator training and emergency procedures.

- In many scenarios, recovery of failed or unavailable systems is important to preventing core damage. Some examples are recovery of offsite power or a diesel generator after a station blackout, recovery of river water systems after a loss of river water (intake screen clogging), recovery of control building ventilation, and recovery of decay heat removal systems. The ability to perform these actions could be improved by preplanning, stocking spare parts and emergency equipment, and training.

TABLE 3-1. OPERATOR ACTION FAILURES CONTRIBUTING SIGNIFICANTLY TO THE FREQUENCY OF CORE DAMAGE*

Operator Action Category (specific operator action)	Operator Action Category Contribution to Core Damage Frequency (percent)	Specific Operator Action Contribution (percent)
Operator Restoration and Recovery	30	
• Loss of CBV initiating event (includes operator fails to establish alternate cooling).		17
• At least one train of DHR starts and runs and one train of onsite AC power is recovered in 6 hours.		5
• Loss of river water initiating event from operator history data (includes operator fails to clear the screen before plant trip).		3
• Recover river water.		2
• Recover river water with steam-driven EFW pump failed.		1
• Recover onsite or offsite power during a station blackout with steam-driven EFW pump failed.		< .1
• Recover single train of onsite power or offsite power.		< .1
• Provide alternate ventilation after control building ventilation failure, given failure of nuclear services water.		< .1
• Recover single train of onsite power or offsite power with steam-driven EFW pump failed.		< .1
• Recover onsite or offsite power during a station blackout.		< .1
Manual Actions To Actuate Systems	12	
• Minimum-flow recirculation is established after successfully throttling HPI.		6
• Recirculation available and initiated within 1 minute of BWST low level alarm during a large or medium LOCA.		5

*Indicates failure of the action described.

NOTE: A system's contribution is calculated by adding the frequency of all sequences in which the failure of the system occurs and core damage results. This sum is then divided by the total core damage frequency from internal events only to calculate the percentage contribution from each system. Since more than one system failure may occur in each core damage sequence, the total percentage due to all system contributions exceeds 100%. These precentages are higher than would be obtained by basing them on the total core damage frequency.

TABLE 3-1 (continued)

Sheet 2 of 2

Operator Action Category (specific operator action)	Operator Action Category Contribution to Core Damage Frequency (percent)	Specific Operator Actior Contribution (percent)
• Operator initiates HPI cooling.		1
• Throttle makeup flow using MU-V16s before diesel gener tor train A fails.		< 1
• Operator identifies SGTR.		< 1
• Throttle makeup flow using MU-V16s.		< 1
• Cool the plant down to repair a small leak.		<.1
• Throttle makeup flow using MU-V217.		<.1
• Recirculation available and initiated within 10 minutes of BWST low level alarm during a small or very small LOCA.		<.1
• Throttle makeup flow using MU-V217, given that offsite power is lost after plant trip.		<.1
• Cool the plant down during an SGTR leak in RCS.		<.1
Manual Backup to Automatic Actuations	8	
• At least one pump started, given no offsite power, no instrument air, and only one train of emergency AC power available.		2
• Primary safety valves reclose after passing water, and operator throttles HPI flow.		2
• At least one pump started, given no offsite power and only one train of emergency AC power available.		1
• At least one pump started, given no offsite power and no instrument air.		1
• PORV recloses after passing water and operator throttles HPI flow.		< 1
• Given emergency AC train A or B and offsite power available.		<.1
Total Contribution to Core Damage Frequency of All Manual Actions	50	

4. REFERENCES

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, April 1983.

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

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

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

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

6. "Canvey: An Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock Area," U.K. Health and Safety Executive, May 1978.

7. 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.

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

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

10. Rogovin, M., and G. T. Frampton, "Three Mile Island, a Report to the Commissioners and to the Public," Government Printing Office, January 1980.

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

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

13. 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.

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

15. Pickard, Lowe and Garrick, Inc., "OPSA, Oyster Creek Probabilistic Safety Analysis," prepared for Jersey Central Power and Light Company, draft PLG-0100, August 1979.

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

17. 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.

18. Swain, A. D., and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August 1983.

19. Westinghouse Electric Corporation, "Westinghouse Owners Group Report, Reactor Coolant Pump Seal Performance Following the Loss of All AC Power," WCAP-10541, Rev. 2, November 1986.