NUREG/CR-5457
EGG-2572

A Review of the Three Mile Island-1 Probabilistic Risk Assessment

Prepared by H. J. Reilly, D. L. Schurman, H. J. Welland, R. C. Bertucio,
S. A. Eide, P. R. Davis, S. E. Mays, A. J. Buslik, N. C. Chokshi

Idaho National Engineering Laboratory
EG&G Idaho, Inc.

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 2120 L Street, NW, Lower Level, Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082

3. The National Technical Information Service, Springfield, VA 22161

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

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

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

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

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

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

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

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

NUREG/CR-5457
EGG-2572
RG

A Review of the Three Mile Island-1 Probabilistic Risk Assessment

Manuscript Completed: September 1989
Date Published: November 1989

Prepared by
H. J. Reilly, D. L. Schurman, H. J. Welland, R. C. Bertucio,[1]
S. A. Eide,[2] P.R. Davis,[3] S. E. Mays,[4] A. J. Buslik,[5] N. C. Chokshi[5]

Idaho National Engineering Laboratory
Managed by the U.S. Department of Energy

EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, ID 83415

[1]EI International, Inc. (presently with NUS Corporation)
[2]EI International, Inc.
[3]PRD Consulting
[4]Tenera
[5]U.S. Nuclear Regulatory Commission

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN A6892
Under DOE Contract No. DE-AC07-76ID01570

ABSTRACT

The Level 1 Probabilistic Risk Assessment that was prepared by Pickard, Lowe and Garrick for GPU Nuclear, and forwarded to NRC, was reviewed. The review included both plant internal events and three kinds of external events: plant fires, seismic events and river flooding. At the close of the review, the authors estimated the frequencies the core damage sequences would have if the recommended corrections were made to the data and assumptions. It was concluded that the recommended corrections would have a major effect on the estimated risk profile of TMI–1, including major increases in some sequence frequencies and major decreases in others.

FIN No. A6892—A Review of the
Three Mile Island–1 Probabilistic
Risk Assessment

EXECUTIVE SUMMARY

EG&G Idaho conducted a limited-scope review of the Level 1 Probabilistic Risk Assessment (PRA) of Three Mile Island Unit 1 (TMI–1). The PRA was performed by Pickard, Lowe and Garrick (PLG) for GPU Nuclear (GPUN) and submitted by GPUN to NRC. The review included the internal events analyses and three kinds of external events: plant fires, seismic events, and river flooding. At the close of the review, the authors estimated the frequencies that the core damage sequences would have if the recommended changes were made to the data. It was concluded that the recommended corrections would have a major effect on the estimated risk profile of TMI–1, including major increases in some sequence frequencies, and major decreases in others.

The following is a summary of the major conclusions, by subsection:

Initiating Events Review

Internal initiating events were reviewed for completeness, adequate grouping of initiators, and appropriateness of frequency values. It was concluded that the list of initiators was comprehensive, and that the grouping appeared reasonable. However, it was unclear how only two event groups—steamline break in the intermediate building and steamline break in the turbine building—can cover all possible feedwater and steamline breaks. The frequencies that were used for very small LOCA and loss of Nuclear Services River Water (NSRW) events appeared to be lower than they should have been. The V–sequence frequency values appeared questionable, although these sequences are small contributors to core damage frequency (CDF). The treatment of loss of control building ventilation was excessively conservative; it probably is not an important initiator at TMI–1. Review of documentation submitted to NRC in connection with Appendix R requirements supports this conclusion.

Event Tree Review

The event tree methodology was reviewed to evaluate the completeness and validity of the logic structure. No major errors were found. However, it was not possible within the scope of this review to verify the correctness of all the event trees.

Review of Assumptions

The PRA was studied to ascertain the validity and influence of major assumptions used in the PRA. It was difficult to find all the assumptions, because they do not appear in one place in the report, and because many of them were implicit assumptions not explicitly identified in the report. The assumptions regarding the effects of loss of control building ventilation were overly conservative. The assumption, that sequences involving loss of Decay Heat Removal (DHR) during shutdown conditions were unimportant, is not adequately supported and is inconsistent with analyses in other PRAs. Studies by Brookhaven National Laboratory (BNL) indicated that such sequences could be among the dominant contributors to core damage frequency at typical U.S. PWRs. The dismissal in the PRA of the impact of seismic Class II components falling and striking seismic Class I components is not adequately supported. The lack of an event tree for the V–sequence is considered to be a deficiency because the V–sequence, while only a small contributor to core damage frequency, can be important to offsite risk. The treatment of pressurized thermal shock was not adequately documented (however, PTS results were consistent with other studies).

Dependency Analysis

An independent dependency analysis was performed as part of the review. The plant piping and instrumentation diagrams (P&IDs) were obtained from NRC for this purpose. Generally, the dependencies in the PRA appeared to be those that were important to the core damage frequency; omitted dependencies appeared to be either unimportant or those affecting the Level 2 and 3 analyses (not part of the PRA).

Comparison with Crystal River 3 PRA

The methodologies and results of the TMI–1 and Crystal River–3 PRAs were compared. The two plants have similar designs. The TMI–1 PRA was performed using the support state method, whereas the CR–3 PRA used the fault tree linking method, therefore making the two PRAs difficult to compare. The two PRAs agree reasonably well regarding estimated CDFs for like sequences; the agreement is not as consistent regarding initiator frequencies and conditional core damage probabilities. The CR–3 PRA did not include fires, floods and earthquakes. Loss of control building ventilation sequences were not significant in the CR-3 PRA.

Comparison with B&W Owners' Group Evaluations

A comparison of the TMI-1 PRA with results of the B&W Owners' Group Safety and Performance Improvement Program indicated that the TMI-1 PRA addressed these common concerns adequately. The TMI-1 PRA estimates higher frequencies for core damage for the events of concern; the difference is attributed to the assumptions in the PRA relating to operator errors in throttling HPI flow following overcooling events. The TMI-1 PRA has higher frequency values than other PRAs for sequences initiated by in-plant fires and by loss of control building ventilation, because of conservative assumptions that are not appropriate to a rigorous PRA.

Comparisons with Generic and Unresolved Safety Issues

Comparisons were made to the anticipated NRC issue resolutions involving pressurized thermal shock (PTS), decay heat removal (DHR), failure of instrument air, failure of emergency feedwater, failure of the Integrated Control System (ICS) and Nonnuclear Instrumentation (NNI), reactor cooling pump (RCP) seal LOCAs as small-break initiators, loss-of-component cooling water, and RCP seal LOCAs as consequences of loss-of-seal cooling. The documentation of the treatment of PTS was not adequate; it appeared that an adequate methodological structure was developed to evaluate PTS, but there were some significant omissions that cannot be explained. However, in no event is PTS expected to be important in comparison with other contributors to core damage frequency at TMI-1. The treatment of DHR issues is adequate except for the neglect of possible accidents during shutdown conditions. The treatment of instrument air failures is confusing and the documentation is inadequate. Losses of power to ICS appear to be modeled correctly; other ICS failures, and failures of NNI, were not modeled.

The TMI-1 PRA frequency value for very small breaks appears to include RCP seal LOCAs. The review indicated that the PRA adequately modeled the issues involved in failures of cooling water systems. However, it appears that the PRA used a nonconservative RCP seal-LOCA model. If the model of the draft NUREG-1150 were used, the impact on CDF could be large, because the time available for recovery after loss of river water would be smaller. It appears that GPUN's procedures are based on the PRA model rather than the NRC model for RCP seal-LOCA model, which does not seem satisfactory to the reviewers. It is expected that when TMI-1 takes actions to comply with the forthcoming resolutions of Generic Issues involving RCP seals, this concern will be alleviated.

Component Failure Data

The component database in the PRA is proprietary; the details of its derivation were unavailable for review. However, the database was reviewed to compare it with information sources used in other PRAs. There were some differences, but the only ones identified as potentially significant in their effects on CDF (assuming that loss of control building ventilation is not an important sequence) were some beta-factors that were employed.

Human Factors

The review of the human response analysis (HRA) indicated that the initial screening process employed in the PRA for identifying human errors is not documented adequately. The review found that errors of omission in performing actions not covered by procedures, and errors due to failures of indicators in the control room during some sequences, were omitted, although this is fairly common in PRAs at the screening stage.

The review went on to compare 11 of the most important human actions quantified in the PRA with data from standard NRC databases. One error in the conservative (high error rate) direction was found. In this review, the error was corrected and fed back into the sequence requantification (see below). During a plant visit to TMI-1, several questionable and important human actions were walked-down. Except for the error noted above, it was concluded that most of the HRA unavailability values were slightly on the conservative side.

Uncertainty Analysis

The uncertainty analysis was identified as incomplete because no sensitivity analyses were performed. The range of uncertainty in CDF that is quoted in the PRA report was identified as much too small, especially given that the most-important sequences (loss of CBV, fires) in the PRA were obtained using analyses suitable only for screening purposes, and because the most-important sequence coming out of the review is river flooding above the Probable Maximum Flood (PMF)—the frequency of which is highly uncertain.

External Flooding

The review identified that the methodology employed for analysis of river flooding in the PRA was unsupportable. More recent analysis by the Corps of Engineers indicates a much higher frequency (5E–4/yr vs. 1E–5/yr in the PRA) for floods above the PMF. The review concludes that the frequency value is not only higher, but highly uncertain, because the estimate involves extrapolation of perhaps 250 years of data to estimate floods with return periods greater than 1000 years.

Fires

A review of the fire analysis in the PRA concluded that the analysis was poorly documented, contained several errors, and was not sufficiently detailed and rigorous to be considered adequate for a Level 1 PRA. The effects of seismically–induced fires do not appear to have been addressed. Based upon a plant visit, and a comparison with results of other PRAs, the reviewers felt that the estimated fire sequence frequencies may become smaller if improved analysis is done, but that this has not been substantiated.

Seismic Events

It was discovered, and acknowledged by GPUN, that the quantification of the seismic events contained errors that invalidated the results contained in the PRA report. Independent analyses were conducted as part of this review using seismic hazards curves from three different sources: the PRA, EPRI, and LLNL. All three of the analyses produced core damage frequencies larger than the value published in the PRA report.

Requantification

It was not possible to requantify the sequences during this review, because the computer programs used in the PRA are proprietary and were not provided to EG&G Idaho and the scope of the review did not permit independent requantification. However, some estimates of the changes in sequence frequencies caused by internal initiating events were made. The change in overall CDF for internally–initiated events was a decrease from 4.4E–4/yr to 2.9E–4/yr.

The frequency value for floods above the PMF was estimated to be 5.0E–4/yr instead of the PRA value of 7.50E–6/yr. The frequency for CDF caused by seismic events was estimated several ways. The value obtained using the hazards curves in the PRA report was 6.5E–5/yr, as compared to the PRA value of 2.70E–6/yr. The external events CDF is increased from 1.1E–4/yr to 6.6E–4/yr, making external events the dominant initiators at TMI–1.

Besides these changes, a number of other differences were listed, some of which were assessed as having a significant effect, that were not included in the estimates for various technical reasons. The most important of these are a) loss of river water sequences, in which the use of the NRC model for reactor coolant pump seal LOCA would have a major effect (increase) on the estimated core damage frequency, and b) fire sequences, which are important in the PRA and GPUN personnel feel will decrease significantly when a more detailed analysis is done.

Success of PRA in Meeting Stated Objectives

The TMI–1 PRA was to be a Level 1 PRA, including external events as defined by the NRC PRA Procedures Guide. The PRA had five specific goals to meet the overall objectives of the PRA. The first three of these goals related to the identification and quantification of dominant contributors (initiators and system failures) to core damage frequency. The review focused principally on the degree to which the PRA succeeded in accomplishing these three goals, in accordance with established methods as exemplified by the NRC PRA Procedures Guide. The overall conclusion of the review is that the PRA generally followed established methods and accomplished the goals, although there were the following problems:

1. The documentation, though extensive, was incomplete in some respects, prohibiting the reviewers from resolving some of the questions that arose in the review. All of the reviewers felt that the documentation was relatively difficult to understand, even for trained PRA analysts. Despite the extensive amount of documentation, pertinent information needed for a comprehensive review was often not present or was unobtainable. For these reasons, the reviewers found the documentation difficult to use for detailed technical review, and believe that it would be difficult to keep the documentation up to date in future uses at TMI–1.

2. Some of the analyses, especially those involving external flooding, in–plant fires, and

loss of control building ventilation, appeared to be appropriate only for initial screening purposes.

The PRA had two other goals, relating to development of a plant risk model and database suitable for future use by GPUN. The reviewers did not analyze the risk model and database; however, it was the opinion of the reviewers that the risk model would be relatively difficult for GPUN to use because of its complexity, the seeming incompleteness of the supporting documentation, and the errors existing in the risk profile.

ACKNOWLEDGEMENTS

The non NRC authors wish to express their appreciation to Dr. Arthur Buslik, the NRC Technical Monitor of this project, for his instruction, guidance, and timely delivery of documents that were needed during the course of this review. Dr. Buslik also contributed some of the work that is included in this report. Without his assistance, the review would not have accomplished as much as it did.

CONTENTS

FIGURES

TABLES

ACRONYMS

ABV	Auxiliary Building Ventilation
ac	Alternating Current
ADV	Atmospheric Dump Valve
ANL	Argonne National Laboratories
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
B&W	Babcock & Wilcox
B&WOG	B&W Owners' Group
BNL	Brookhaven National Laboratories
BWST	Borated Water Storage Tank
CBV	Control Building Ventilation
CCF	Common Cause Failure
CCW	Component Cooling Water
CDF	Core Damage Frequency
COE	Corps of Engineers
COMPBRN	Computer Code for Modeling Compartment Fires
CR-3	Crystal River Unit 3
CST	Condensate Storage Tank
CVCS	Chemical and Volume Control System
dc	Direct Current
DHCCCW	Decay Heat Closed Cycle Cooling Water
DHR	Decay Heat Removal
ECCS	Emergency Core Cooling System
EFW	Emergency Feedwater
EPRI	Electric Power Research Institute
ESAS	Engineered Safeguards Actuation System
ESD	Event Sequence Diagram
FHAR	Fire Hazards Analysis Report
FSAR	Final Safety Analysis Report
FW	Feedwater
GPUN	GPU Nuclear Corp.
HCR	Human Cognitive Reliability
HPI	High Pressure Injection
HRA	Human Response Analysis
ICCCW	Intermediate Closed Cycle Cooling Water
ICS	Integrated Control System
IE	Initiating Event
IEEE	Institute of Electrical and Electronic Engineers
IPE	Individual Plant Evaluation
LLNL	Lawrence Livermore National Laboratories
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPI	Low Pressure Injection
MCC	Motor Control Center
MFLIV	Main Feedwater Line Isolation Valve
MFW	Main Feedwater

MLD	Master Logic Diagram
MOV	Motor–Operated Valve
MP–3	Millstone Point Unit 3
MSIV	Main Steam Isolation Valve
MU	Makeup
NNI	Non–Nuclear Instrumentation
NRC	Nuclear Regulatory Commission
NSCCCW	Nuclear Services Closed Cycle Cooling Water
NSRW	Nuclear Services River Water
NUCLARR	Nuclear Computerized Library for Assessing Reactor Reliability
OATS	Operator Action Tree System
OTSG	Once–Through Steam Generator
P&ID	Piping & Instrumentation Diagram
PLG	Pickard, Lowe and Garrick
PMF	Probable Maximum Flood
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
RBIS	Reactor Building Isolation System
RCP	Reactor Coolant Pump
RCS	Reactor Cooling System
RHR	Residual Heat Removal
RPS	Reactor Protection System
RV	Reactor Vessel
RW	River Water
SAR	Safety Analysis Report
SETS	Set Equation Transformation System
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SLB	Steamline Break
SLRDS	Steamline Rupture Detection System
SNL	Sandia National Laboratories
SPIP	Safety and Performance Improvement Program
SRV	Safety Relief Valve
SW	Switchgear or Service Water
TCV	Turbine Control Valve
THERP	Technique for Human Error Rate Prediction
TMI–1	Three Mile Island Unit 1
TRC	Time Reliability Correlation
TSV	Turbine Safety Valve
V–SEQUENCE	Ruptures in ECCS piping which bypass the containment

A REVIEW OF THE THREE MILE ISLAND–1 PROBABILISTIC RISK ASSESSMENT

INTRODUCTION

Background

A Probabilistic Risk Assessment (PRA) of the Three Mile Island Unit 1 (TMI–1) was completed [1] by Pickard, Lowe and Garrick (PLG) under contract from GPU Nuclear Corporation (GPUN). The PRA was forwarded to the Nuclear Regulatory Commission (NRC) in December, 1987. [2] The PRA is a full–scope PRA, including external events, that has been completed through Level 1 (the determination of core damage frequency), but has a structure suitable for later extension to Levels 2 and 3 (the determination of the risk associated with core damage). EG&G Idaho contracted, through the Department of Energy Idaho Operations Office (DOE–ID), to review the document for NRC. It is EG&G Idaho's understanding that there are no regulatory decisions that are supported by the PRA—it is an informational document—although it may be part of GPUN's submittals in the forthcoming Individual Plant Evaluation (IPE) program.

Scope of the Review

Given the above status (relative to NRC requirements) of the PRA, a full–scope review was not deemed appropriate. The goals of the PRA were studied as an aid in determining the scope and objectives of the review. These goals, stated on the first page of the Introduction, Volume 1 of the PRA, were to (a) "develop...the likelihood of core damage and its associated uncertainty," (b) "identify the significant contributors to risk," (c) "rank plant systems and components...in terms of their contribution to the frequency of core damage," (d) "develop a plant risk model and the tools for its use by GPUN in future...," (e) "develop and organize a data base (for) the plant risk model..." It was also stated that the PRA is a Level 1 PRA as defined by the NRC PRA Procedures Guide. [3]

Statements in a "Caveats" subsection, in Volume 3 of the PRA report, indicated that the PRA was terminated prior to its completion; revisions to the data and models were ongoing at the time of the completion of the report and were not fully completed and integrated into the report. This circumstance, and the large size (more than 5000 pages) of the PRA report, argued against a detailed review. Therefore, EG&G Idaho decided that the review should attempt to assess the extent to which the PRA was successful in fulfilling the objectives of the PRA in accordance with established techniques as exemplified by NUREG/CR–2300.

It was decided that the review would not be a "phased" review, wherein some portion of the review would be completed and subsequently decisions made as to the cost and scope of the next phase, or phases, but that the entire review would be conducted according to the scope that is shown below.

The scope that was selected for the limited–scope review is as follows:

- Review and evaluate the scope, assumptions, and system analysis for internal events.
- Identify and develop a table of important assumptions used in the analysis and comment on their validity.
- Review the event trees for completeness and validity of logic structure.
- Review other information available on Babcock and Wilcox (B&W) plants, to help assess the completeness of the study and the validity of the assumptions made. Examine the accident scenarios developed for Crystal River Unit 3 for possible insights applicable to TMI–1.
- Review information developed in the study of various generic and unresolved safety issues (e.g., Unresolved Safety Issue A–45 on Shutdown Heat Removal and Generic Issue 23 on Reactor Coolant Pump. Seal Cooling Integrity) for pertinence. Issues of particular interest were:

1. Accident sequences involving pressurized thermal shock and overcooling transients.

2. Failures of the Integrated Control System and losses (partial or complete) of the Nonnuclear Instrumentation System.

3. Failures of the instrument air system.

4. Failures involving the Emergency Feedwater System.

- Perform a dependency analysis, on a train-by-train basis, to identify the dependency of front-line systems on support systems, and support systems on support systems.

- Review the sources of accident initiators and reliability data used for fault tree and event tree quantification.

- Evaluate the validity of the treatment of human errors.

- As time permits, requantify the sequences to the extent possible.

- Review and evaluate the uncertainty estimates reported in the PRA.

- For the seismic initiator, compare the hazard curves (frequencies of various peak ground initiators) used in the study to the hazard curves used in the Lawrence Livermore National Laboratory (LLNL) Seismic Hazard Characterization Project. This subtask was performed by NRC and the results were provided to EG&G Idaho.

- If possible within the time available, obtain independent estimates of the external flooding hazard function (frequencies of various flood levels).

- Review the methodology used, and the data, and briefly review the fire risk scoping study at Sandia National Laboratories (SNL) for insights as to the validity of the estimates of the fire-induced core melt frequency.

Additional Assumptions and Items of Scope

EG&G Idaho recommended selection of this Scope because these areas of the PRA were the most likely areas where significant errors or omissions would be found, given the statements in the Executive Summary (Volume 1 of the PRA Report) regarding the findings of the PRA. Sequences of small importance, and those having small importance in other PRAs, such as tornado-induced core melt sequences, were not reviewed. Generally the phenomenological analysis was not questioned, except wherein issues of interest to NRC (such as the RCP Seal Cooling Integrity issue) were specifically identified for their potential effect on the PRA.

Part of the database used in the PRA is a proprietary database that was not provided to NRC or EG&G Idaho. Therefore, this part of the review was limited to comparisons of the data in the report to data from other PRAs and databases. Proprietary computer programs were used but not provided for review.

The review included a plant visit by the NRC Technical Monitor, the NRC Project Manager for TMI-1, and members of the EG&G Idaho review team.[a] However, the review did not include meetings with PLG personnel who performed the PRA.

TMI-1 plant P&IDs were provided by the NRC Technical Monitor. Two copies of the PRA report, which is copyrighted by PLG, were provided. Additional documents were provided by the NRC Technical Monitor as needed during the review.

Documents submitted by GPUN to demonstrate compliance with Appendix R requirements were examined during the course of this review, because the documents provide information that relate to one of the dominant sequences in the PRA.

---

a. Letter from H. J. Reilly, EG&G Idaho, to Dr. Arthur Buslik, NRC, "Report of TMI-1 Plant Visit, October 18–19, 1988," November 8, 1988.

INTERNAL EVENTS ANALYSIS

Initiating Events

Review of the Three Mile Island Unit 1 (TMI–1) Probabilistic Risk Assessment (PRA) initiating events concentrated on three main concerns: completeness of the list, grouping of events, and appropriateness of the frequencies. Each concern is discussed below. This section is limited to internal events. External event initiators are covered elsewhere.

Initiating Event Identification and Completeness. The TMI–1 internal initiating events were identified by performing a detailed review of the plant design and industry experience. In addition, the search for initiators was guided by development of a master logic diagram (MLD). The resulting list of 41 initiators is presented in Table 1. The list of initiators is comprehensive. Coverage of reactor coolant system (RCS) inventory control failure events is especially extensive. In addition, many support system failures leading to a reactor trip and affecting multiple safety systems (often termed "special initiators") were identified. The only frequently–appearing special initiator not listed is loss of an emergency ac power bus (4160 or 480 Vac). Normally, omission of this event indicates that such an occurrence does not lead to a reactor trip. However, there is no documentation concerning this event, or the reason for its omission, from the initiating event list. Also, there is no explanation why dc bus A is an initiator, while dc bus B is not (During a plant visit to TMI–1, it was learned[a] that GPU performed procedure reviews, augmented by electronic simulator exercises, to verify that loss of an ac power bus or of dc bus B will not trip the reactor. This appears to support the assumptions in the PRA regarding the buses).

a. Letter from H. J. Reilly, EG&G Idaho, to Dr. Arthur Buslik, NRC, "Report of TMI–1 Plant Visit, October 18–19, 1988," November 8, 1988.

Table 1. TMI internal initiating events

Safety Function Threatened	Initiating Event[a]
1. Reactivity control	1. Uncontrolled rod group withdrawal
	2. Control rod ejection
	3. Control rod drop
	4. Inadvertent boration
	5. Inadvertent deboration
	6. Inadvertent reactor trip
2. Reactor coolant system (RSC) inventory control	7. Very small RCS pipe breaks
	7a. Small RCS pipe breaks
	8. Medium RCS pipe breaks
	9. Large RCS pipe breaks
	10. Inadvertent power–operated relief valve (PORV) or high point vent valve opening
	11. Letdown or sample line break
	12. Reactor vessel rupture

Table 1. (continued)

Safety Function Threatened	Initiating Event[a]
2. Reactor coolant system (RSC) inventory control (continued)	13. Steam generator tube rupture
	14. Excessive charging letdown
	15. Break in decay heat removal (DHR) dropline
3. RCS pressure control	16. Pressurizer heater failure
	17. Pressurizer spray failure
4. Core heat removal	18. RCP trip or shaft seizure/break
	19. Core internals vent valve fails open
	20. Core flow blockage
5. RCS heat removal	21. Turbine control valve opening
	22. Turbine safety valves (TSVs) close or turbine control valves (TCVs) throttle
	23. Loss of condenser vacuum
	24. Integrated control system (ICS) failure (bus ATA failure)
	25. Small steam line break (SLB) or inadvertent opening of atmospheric dump valve (ADV) or main steam isolation valve (MSIV)
	26. Small SLB inside containment
	27. Small SLB outside containment
	28. Large SLB inside containment
	29. Large SLB outside containment but upstream of MSIVs
	30. Large SLB outside containment and downstream of MSIVs
	31. Main feedwater (MFW) pump speed increase or control valve opening above demand
	32. MFW or booster pump(s) trip or MFW control or isolation valve closure
	33. Inadvertent MSIV closure

Table 1. (continued)

Safety Function Threatened	Initiating Event[a]
5. RCS heat removal (continued)	34. Feedwater line break upsteam of main feedwater line isolation valve (MFLIV)
	35. Feedwater line break downsteam of (MFLIV)
	36. Loss of control air (interruption of feedwater flow)
	37. Loss of river water
	38. Loss of offsite power
	39. Loss of dc power train A
	40. Loss of nuclear services closed cycle cooling water
	41. Loss of control building ventilation
6. Containment isolation	42. Such events were not considered to be initiating events
7. Containment pressure and temperature control	43. Such events were not considered to be initiating events
8. Control of excessive	44. The consequences of direct radioactivity releases from sources other than the core were considered to be insignificant

a. The TMI–1 study also includes an "other" category for each safety function threatened. However, these events were not used in the quantification.

In general, the initiating event list for TMI–1 appears to be comprehensive. However, documentation concerning the actual steps taken to identify events and ensure completeness is lacking. Specifically, the relevant documentation is contained mainly in one short paragraph as follows (page 2-3 of the Plant Model Report):

"The list of initiating events in Table 2–1 is the result of an extensive analysis by the TMI–1 probabilistic risk assessment team, backed up by many years of reactor safety research by the government and private industry. The list was produced by a detailed review of the plant design and industry operating experience. The plant design review included material contained in the systems descrip' ›ns in the Systems Analysis Report."

It is not clear what the plant design review included or what the extent of the review was.

Finally, inclusion of an "other" event in Table 1, under each safety function threatened, does not help when the initiating events are combined into a limited number of groups for event tree development. Initiating event grouping is performed to limit the event tree development and yet preserve significant differences in plant response requirements and initiating event effects on safety systems. The "other" initiating event categories in Table 1 cannot be placed into groups, because their characteristics are unknown. A solution to this problem might be to create an "other" initiating event group. However, in such a case, the plant response requirements and effects on safety systems of this "other" initiating event group, are unknown. Therefore, an event tree for such a group cannot be developed, and the significance of such a group on the core damage frequency cannot be determined. Completeness at the initiating event group level is ensured, to the extent possible, not by "other" events but by performing a comprehensive review of industry experience and a comprehensive review of plant design and system dependencies. It is not clear whether such a procedure was followed for the TMI-1 PRA.

Initiating Event Grouping. Initiating event groups for the TMI-1 PRA are listed in Table 2. Also listed in the table are the initiating events included in each group and the applicable categories from EPRI NP-2230 (for quantification purposes).[4] The 41 initiating events were combined into 19 groups (20 with the inclusion of reactor vessel rupture) for event tree development. The groups are typical for PRAs of pressurized water reactors (PWRs). However, it is not clear how feedwater breaks upstream and downstream of the main feedwater line isolation valve (MFLIV), and steam-line breaks, can all be covered by the single event tree for steam-line break in the intermediate building (in general, these events are not dominant contributors to core damage risk). Also, it is not clear how all types of letdown or sample line breaks can be modeled in the small loss-of-reactor-coolant system (RCS) inventory event tree.

Table 2. TMI-1 internal initiating event groups

Initiating Event Group	Applicable Initiating Events[a]	Applicable EPRI NP-2230 Events[b]
1. Large loss of RCS inventory	9. Large RCS pipe break	None
2. Medium loss of RCS inventory	8. Medium RCS pipe breaks	None
3. Small loss of RCS inventory	2. Control rod ejection	None
4. Very small loss of RCS inventory	7. Very small RCS pipe breaks	None
	7a. Small RCS pipe breaks	
	10. Inadvertent PORV or high point vent valve opening	
	11. Letdown or sample line break	
5. Containment bypass	15. Break in DHR dropline	None
6. Steam line break in intermediate building	25. Small SLB or inadvertent opening of ADV or MSIV	None
	26. Small SLB inside containment	
	28. Large SLB inside containment	
	29. Large SLB outside containment but upstream of MSIVs	
	34. Feedwater line break upstream of MFLIV	
	35. Feedwater line break down-stream of MFLIV	

Table 2. (continued)

Initiating Event Group	Applicable Initiating Events[a]	Applicable EPRI NP-2230 Events[b]
7. Steam line break in turbine building	21. Turbine control valve opening	None
8. Once through steam generator (OTSG) tube rupture	13. Steam generator tube rupture	None
9. Excessive main feedwater	31. MFW pump speed increase or control valve opening above demand	None
10. Loss of main feedwater	23. Loss of condenser vacuum	PWR 16. Total loss of feedwater flow (all loops)
	27. Small SLB outside containment	
	30. Large SLB outside containment and downstream of MSIVs	
	32. MFW or booster pump(s) trip or MFW control or isolation valve closure	Pump 24. Loss of condensate pumps (all loops)
		PWR 25. Loss of condenser vacuum
		PWR 27. Condenser leakage
		PWR 30. Loss of circulating water
11. Reactor trip	1. Uncontrolled rod group withdrawal	PWR 1. Loss of RCS flow (one loop)
	3. Control rod drop	PWR 2. Uncontrolled rod withdrawal
	4. Inadvertent boration	PWR 3. CRDM problems and/or rod drop
	5. Inadvertent deboration	PWR 6. High or low pressurizer pressure
	6. Inadvertent reactor trip	PWR 8. High pressurizer pressure
	14. Excessive charging letdown	PWR 11. Chemical and volume control system (CVCS) malfunction—boron dilution
	16. Pressurizer heater failure	
	17. Pressurizer spray failure	PWR 12. Pressure, temperature, power imbalance

Table 2. (continued)

Initiating Event Group	Applicable Initiating Events[a]	Applicable EPRI-NP-2230 Events[b]
11. Reactor trip (continued)	18. RCP trip or shaft seizure/ break	PWR 14. Total loss of RCS flow
	19. Core internals vent valve fails open	PWR 15. Loss or reduction in feedwater flow (one loop)
	20. Core flow blockage	PWR 17. Full or partial closure of MSIV (one loop)
		PWR 21. Feedwater flow instability—operator error
		PWR 22. Feedwater flow instability—miscellaneous mechanical causes
		PWR 23. Loss of condensate pumps (one loop)
		PWR 28. Miscellaneous leakage in secondary system
		PWR 36. Pressurizer spray failure
		PWR 37. Spurious auto trip—no transient condition
		PWR 38. Auto/manual trip due to operator error
		PWR 39. Manual trip due to false signals
		PWR 40. Spurious trips—cause unknown
12. Turbine trip	22. TSVs close or TCVs throttle	PWR 18. Closure of all MSIVs
	33. Inadvertent MSIV closure	PWR 33. Turbine trip, throttle valve closure, electro-hydraulic control problems
		PWR 34. Generator trip or generator caused faults
13. Loss of control air	36. Loss of control air	None
14. Loss of control building ventilation	41. Loss of control building ventilation	None

Table 2. (continued)

Initiating Event Group	Applicable Initiating Events[a]	Applicable EPRI NP-2230 Events[b]
15. Loss of bus ATA power	24. ICS failure (bus ATA failure)	None
16. Loss of one dc power train	39. Loss of dc power train A	None
17. Loss of off-site power	38. Loss of off-site power	None
18. Loss of nuclear services closed cycle cooling water	40. Loss of nuclear services closed cycle cooling water	None
19. Loss of river water	47. Loss of river water	None
20. Reactor vessel rupture[c]	12. Reactor vessel rupture[c]	None[c]

a. These events are from Table 1.

b. The EPRI categories were used to help generate the prior (industry) frequency. The categories are described in Reference 6. In some cases, EPRI categories existed for the initiating event group in question, but were not used because better sources were available. An example is the loss of off-site power.

c. This group is missing in Tables 2-2 and 2-3 of the Plant Model Report and Table 3-8 of the Data Report.

The reactor vessel rupture initiating event is often grouped separately as an event leading directly to core damage. The event appears in Table 1 but was not included in any of the 19 initiating event groups in the TMI-1 PRA. The event was dismissed, based on low frequency, in the process of initiating event grouping.

Assignment of EPRI NP-2230 initiating event categories to the TMI-1 groups (see Table 2) is reasonable. However, 13 of the 41 EPRI categories were not used, and no documentation is presented to explain why these were omitted.

Initiating Event Group Frequencies. Frequency distributions for the 19 TMI-1 initiating event groups are presented in Table 3. Also shown in the table are the generic (prior) mean frequencies and the TMI-1 experience used in the Bayesian update process. Frequencies were estimated based on several different methods and sources. Three groups (10, 11, and 12) were based mainly on data from Reference 5, with a Bayesian update to account for TMI-1 experience. Several other groups (3, 4, 7, 8, 13, 15, and 16) involved a review of *Nuclear Power Experience*[5] to obtain a prior generic frequency. One (group 9) utilized only Babcock & Wilcox (B&W) reactor experience to generate a prior frequency. Three groups (1, 2, and 6) involved prior distributions based on no events in 428 PWR years of operation. Finally, four groups (5, 14, 18, and 19) were quantified based on TMI-1 system models. (Although the report indicates five were quantified in this manner, a review indicated that loss of air systems was actually quantified based on *Nuclear Power Experience* rather than TMI-1 system models).

The loss-of-coolant-accident (LOCA) frequencies are typical for PWRs. However, the very small LOCA frequency of 5.1E-3/yr is approximately four times lower than the same group for the Zion and Seabrook PRAs.[6,7] This LOCA group normally includes reactor coolant pump (RCP) seal LOCAs, which are mainly a potential problem with Westinghouse RCPs. Although TMI-1 like Zion and Seabrook, has Westinghouse RCPs, no explanation for the four-fold decrease in frequency for TMI-1 is presented.

Three initiating event groups were quantified utilizing Reference 4 data to generate prior distributions. The three groups are turbine trip, total loss of main feedwater, and reactor trip. Utilizing the more recent EG&G Idaho update, this review estimates (without reviewing actual events for applicability to TMI-1) the following mean frequencies:

Table 3. TMI–1 internal initiating event group frequency distributions

	Generic (Prior) Mean Frequency	TMI–1 Evidence		Frequency Per Year (Posterior)			
Initiating Event Group	Per Year	Events	Years	Mean	5th Percentile	50th Percentile	95th
1. Large loss of RCS inventory	2.7E–4	0	4.5	1.9E–4	7.3E–6	7.4E–5	5.2E–4
2. Medium loss of RCS inventory	8.0E–4	0	4.5	4.2E–4	1.9E–5	1.9E–4	1.3E–3
3. Small loss of RCS inventory	3.6E–3	0	4.5	2.2E–3 (3.2E–3)[a]	2.7E–5	9.4E–4	1.1E–2
4. Very small loss of RCS inventory	5.2E–3	0	4.5	5.1E–3	2.7E–4 (2.2E–4)[a]	7.55E–3 (2.6E–3)[a]	1.4E–2
5. Containment bypass	—	0	4.5	1.0E–7 (4.6E–10)[a]	4.7E–10 (6.4E–9)[a]	6.6E–9	1.7E–7
6. Steamline break in intermediate building	8.0E–4	0	4.5	4.2E–4	1.7E–5 (1.9E–5)[a]	1.9E–4	1.3E–3
7. Steamline break in turbine building	—[b] (6.9E–3)[a]	— (0)	— (4.5)	—[b] (6.3E–3)[a]	—[b] (1.8E–4)[a]	—[b] (2.8E–3)[a]	—[b] (1.6E–2)[a]
8. OTSG tube rupture	1.4E–2	0	4.5	1.1E–2	4.0E–4	6.4E–3	2.8E–2
9. Excessive main feedwater	2.3E–1	0	4.5	1.2E–1	2.1E–2	7.9E–2	2.8E–1
10. Loss of main feedwater	5.5E–1	0	4.5	2.3E–1	5.1E–2	1.8E–1	4.8E–1
11 Reactor trip	6.6	3	4.5	1.4	6.7E–1	1.4	2.2
12 Turbine trip	1.9	7	4.5	1.6	7.8E–1	1.5	2.3
13. Loss of control air	—	0	4.5	6.0E–3	2.0E–4	1.9E–3	1.9E–2
14. Loss of control building ventilation	—	0	4.5	2.0E–4	5.4E–5	1.4E–4	4.2E–4
15. Loss of bus ATA power	7.2E–2	0	4.5	5.4E–2	5.2E–3	3.6E–2	1.7E–1
16. Loss of one dc power train	3.3E–2	0	4.5	2.8E–2	3.7E–3	1.9E–2	6.0E–2
17. Loss of offsite power	1.3E–1	0	4.5	7.1E–2	1.4E–3	5.0E–3	1.6E–1
18. Loss of nuclear services closed cycle cooling water	—	0	4.5	1.4E–2	4.6E–3	1.1E–2	2.7E–2
19. Loss of river water	—	—[c]	12.0	7.4E–3	3.5E–4	1.3E–3	2.2E–2
20. Reactor vessel rupture[b]	—[b]	—[b]	—[b]	—[b]	—[b]	—[b]	—[b]
	Total = 9.6			Total = 3.6			

a. The numbers in parentheses are from Table 3–8 of the Data Analysis Report.

b. These events and numbers are missing from Table 2–3 of the Plant Model Report.

c. The text in Section 3.5 of the Data Analysis Report indicates one event in 12 years, while Table 3–8 in the same section indicates zero events in 12 years.

1. Turbine trip—1.7/yr

2. Total loss of main feedwater—0.4/yr

3. Reactor trip—5.5/yr.

These results are close to the generic mean frequencies of 1.9, 0.55, and 6.6/yr used for TMI–1. The posterior mean frequencies for the three groups are 1.6, 0.23, and 1.4/yr, as indicated in Table 3. The total for these three is 3.2/yr, compared with plant–specific experience of 2.2/yr and generic experience of 9.1/yr.

TMI–1 experience from 1975 through half of 1979 indicated a very low yearly trip frequency of 2.2/yr. This was confirmed by reviewing Reference 8 for TMI–1 trips. During the same period, TMI–1 was listed in Reference 8 as having six trips. This compares with 10 trips listed in the TMI–1 PRA. Therefore, use of Reference 8 would produce an even smaller frequency for TMI–1 trips.

Loss of offsite power (LOOP) at TMI–1 has a site–based frequency of 7.1E–2/yr. The plant–specific experience is listed as zero events in 4.5 years. The most recent compilation of LOOP events, NSAC–111, was reviewed to verify this.[9] One possible LOOP event was listed for the TMI site through 1986. This event occurred on April 21, 1986 due to bus switching problems while in hot shutdown. If this event were to be included, the plant–specific experience would be one event in 11 years, which results in 9.0E–2/yr. Also, the industry average plant LOOP frequency is approximately 8.8E–2/yr, based on NUREG–1032 and NUMARC–8700.[10, 11] Therefore, the TMI–1 value of 7.1E–2/yr is reasonable.

The loss of air system mean frequency is listed as 6.0E–3/yr. This value was apparently obtained by reviewing Reference 10 from 1970 through 1985. No evidence of a total loss of air was found. The conversion of this information to the mean frequency of 6.0E–3/yr is not explained. The System Analysis Report, Section 18, contains an analysis of the loss of air frequency, based on the system analysis. The mean frequency is 1.5E–2/yr, with the dominant failure mode being failure of the dryer transfer valve and operator failure to then bypass the dryer. It is not clear why this analysis was not used to determine the loss of air system frequency. However, assuming no complete losses of air systems within the period examined, and approximately 500 PWR years of operation, the mean frequency would be less than 2.0E–3/yr.

The following four initiators were quantified based on TMI–1 system analyses:

1. Inadvertent opening of DHR valves.

2. Loss of control building ventilation.

3. Loss of nuclear services closed cycle cooling water.

4. Loss of river water.

Inadvertent opening of the DHR valves (the interfacing system LOCA event) has a mean frequency (see Table 3) of 1.0E–7/yr. Quantification of this group is explained in Section 3.5.2.4 of the Data Analysis Report. The two cold leg injection lines of the DHR system are the main contributors. Each line has two check valves and a normally–open motor–operated valve (MOV) in series. The analysis assumed that during normal operation, a very small leakage (not considered a failure) past the upstream check valve (nearest to the RCS) would result in the downstream check valve being subjected to RCS pressure on one side and low pressure on the other side. In such a case, the downstream check valve suffering a large internal leakage is the initiator. If the upstream check valve has already suffered a large internal leakage, or fails to close (with equal pressure on each side, the valve could have been "floating"), then an open path exists from the RCS to the low–pressure DHR system. Quantification of this event involves a subsequent unavailability calculation for the upstream check valve, involving large internal leakage over a one and one–half year test period, or a failure to close, and an initiator calculation for the downstream check valve. The large internal leakage mean failure rate was assumed to be 8.3E–9/h, based on a review of check valve leakage data. Also, the check valve failure–to–close value used was 2.1E–4/demand. Given these failure rates, the frequency of both check valves failing during a year is 1.9E–8/yr. Two of these lines then result in a rate of 3.8E–8/yr. In the PRA report, an extra factor of two is used, resulting in a rate of 7.6E–8/yr (Apparently, this value is rounded to 1E–7/yr, as mentioned above). It is believed that this factor of two, found in Equation (3.14), is in error. This factor is considered erroneous because the downstream check valve cannot be open (or suffer a large internal leakage failure) before the initiating event because the accumulator would begin to discharge. Such an event would be annunciated in the control room and appropriate repair actions would be taken. Therefore, the downstream valve can be the only initiator. If either valve were the initiator (and the other fail to close or fail because of a previously–undetected large internal leakage), then the factor of two would be appropriate. The discussion does not clearly describe how the result represents a yearly frequency. Finally, because the derivation of the check valve large internal leakage failure rate is considered to be proprietary, the value cannot be checked.

No credit was taken for possibly being able to close the normally–open MOV downstream of the check valves. Also, it was assumed that given failure of the check valves, a rupture would occur in the low–pressure DHR system. By accounting for both internal leakage and failure to close, there may be some double counting, depending on how data were collected for these failure modes. However, the check valve large internal leakage failure rate used is at least a factor of ten lower than that used in most recent PRAs. The report contains no information on the derivation of this value.

Finally, it should be noted that analyses of interfacing system LOCAs in previous PRAs have not been consistent. Equations and assumptions used have varied considerably. A major uncertainty arises from the interpretation and application of data for large internal leakages of check valves. For example, do such failures occur because of a previously–undetected failure to close, or because of a "random" disk rupture? In addition, can the disk rupture occur only if a large pressure differential exists across the valve, or can it occur with a small pressure differential? The TMI–1 analysis appears to have a balance of conservative assumptions, with potentially nonconservative data. The failure rate quoted is significantly lower than those used in previous PRAs (these sequences are also discussed in the Assumptions Section of this report).

Since the completion of the PRA, GPUN has submitted information [12, 13] to NRC relative to compliance with Appendix R, and NRC has reviewed the submittals. [14] These documents provide the results of tests and analyses showing that loss of control building ventilation (CBV) will not lead to core damage at TMI–1. However, the PRA has not been updated to reflect these changes. Therefore, some review of this initiator was done. In the TMI–1 PRA, the frequency for loss of control building ventilation as an initiating event was determined by requantification of the system models (Section 6, System Analysis Report). All support systems were assumed to be available. Although this is a nonconservative assumption, our opinion is that the effects are probably minimal. In the requantification, the initial component failure in each cut set was determined over an entire year (8760 h). Additional component failures that must occur in order to fail the system were evaluated over a mission time equal to the repair time of the initially failed component. The repair time used was either 24.9 or 32.9 hours, depending on the component. Credit was taken for the following types of recovery:

1. Realignment to either the open or recirculation mode of operation, depending on the type of flow path failure.

2. Manual start of a standby train.

3. Locally opening dampers which fail closed.

4. Establishing alternate ventilation using portable fans and elephant trunks.

At least five hours was assumed for recovery. This type of quantification procedure is believed to be the most appropriate for such initiating events. The resulting frequency, 1.95E–4/yr, seems reasonable. Dominant failure modes involve dependent failures of the chilled water system chillers or pumps, combined with an outside temperature greater than 95°F (failing alternate ventilation), and dependent failures of booster or exhaust fans with operator failure to establish alternate ventilation.

Several potential conservatisms were built into the loss of control building ventilation initiator. Probably the most limiting is the use of 104°F as the room temperature at which significant electronic failures will occur. More recent analyses indicate that loss of the ventilation may never result in component failures or a plant trip (page 6–48, Systems Analysis Report).

Loss of the nuclear services closed cycle cooling water initiating event includes the following systems (Section 4, Systems Analysis Report):

1. Nuclear services river water (NSRW), except for plugging of all intake screens, which was addressed separately.

2. Nuclear services closed cycle cooling water (NSCCCW).

3. Class I auxiliary building ventilation (ABV) system.

There are three NSRW pumps, three NSCCCW pumps, and two ABV trains. Following a plant trip, only one of three pumps, and one ABV train, are required. However, operational constraints require that the plant shut down if two pumps in either the NSRW or NSCCCW are lost. For convenience, the initiating event was defined as loss of all three pumps in either system (or other similar types of complete system failures). This simplification is acceptable as long as these systems affect other systems only when complete NSRW, NSCCCW, or ABV failure occurs, which appears to be the case at TMI–1.

In the PRA, quantification of the NSCCCW initiator was performed in a manner similar to that for loss of control building ventilation. All support systems were assumed to be available. The resulting frequency for the initiator is 1.4E–2/yr. Dominant contributors include system leakages, pump failures combined with check valve failures to reseat, isolation valves transferring closed, and dependent failures of all pumps in a system. The frequency seems high and is probably conservative. Quantification of leakage failures involves significant uncertainty, especially when determining what leakage rates should actually be considered as failures.

Finally, the loss of NSRW initiator was defined to include only failures resulting from plugging of the intake screens. In the PRA, this event was quantified by using plant–specific data for plugging and then applying a recovery action to account for unplugging of the screen before the water in the intake structure is depleted. One complete plugging event occurred in 12 years, resulting in a frequency of plugging of 8.3E–2/yr. Failure to unplug the screen within several hours was assigned a probability of 1.78E–1. The product of the two is 1.5E–2/yr. However, the report indicates a frequency of 7.4E–3/yr. It is not known why this frequency does not agree closely with 1.5E–2/yr, except that the data table indicates zero events in 12 years, rather than one (Table 3–8, Data Analysis Report).

Summary of Initiating Events Review. In general, the TMI–1 initiating event list (Table 1) is comprehensive. Grouping of initiating events (Table 2) appears reasonable. However, it is unclear how different types of feedwater and steam–line breaks can be covered by only two groups—steam–line break in the intermediate building and steam–line break in the turbine building. Finally, with the following exceptions, appropriate methods were used to quantify the initiating event group frequencies (Table 3):

1. The very small LOCA frequency is 5.1E–3/yr, which is about a factor of four lower than previously published PRA values.

2. A check valve internal leakage failure rate was used in the interfacing system LOCA (inadvertent opening of DHR valves) which is at least a factor of ten lower than values in previously–published PRAs. However, potential conservatisms in the analysis may offset this low value.

3. Loss of control building ventilation is probably not an initiating event based on this review report.

4. Loss of the NSCCCW may have a conservatively high frequency.

5. Loss of the NSRW may be twice as frequent as the value indicated in Table 3.

6. Loss of instrument air systems may have a conservatively high frequency.

The potential importance of these concerns is discussed in the section on Requantification.

Event Trees

The purpose of the event tree review was to evaluate the completeness and validity of the logic structure and the success criteria. The functional and support systems dependencies, along with the implicit assumptions associated with the model, were also included in the review.

Overview of TMI–1 PRA Methodology. The TMI–1 PRA used support state event trees to establish boundary conditions for the operation of the systems contained in the front line system event trees. Both sets of event trees used the support state methodology for modeling plant response to various initiating events. This methodology requires that dependencies between headings on event trees be explicitly modeled in the structure of the event trees, or that boundary conditions (referred to as split fractions) be used to account for dependencies. This methodology produces a very large number of sequences (or scenarios, as they are called in the TMI–1 PRA).

The support state event tree is the starting point for modeling plant response to an initiating event. The TMI–1 support state tree produces over 6000 sequences, representing the various combinations of support system successes and failures that the analysts deemed important enough to examine. A computer code was used to group these events into impact vectors, each having a specific affect on the front line systems. This was accomplished by comparing the status of support states from each sequence to the support system–to–front line system dependency table prepared by the analysts. This resulted in approximately

1100 distinct impact vectors. The analysts then combined groups of impact vectors into 39 support states, using qualitative and quantitative judgements, from which each front line system event tree was quantified.

For each initiating event, there is a main tree depicting the early response to the initiating event. For each tree, there are several subtrees that depict the long-term progression of events to either a stable condition or to one of several plant damage states. Each of the main trees for the transient events has over 1000 sequences. The subtrees vary in length but most of them have several hundred sequences each. Given that each of these sequences must be quantified for 39 different support states, the number of individual scenarios quantified in this analysis is very large.

Evaluation of Support State Modeling. The Plant Model Report contains the description of the analysis of support system dependencies and how they were accounted for in the quantification of sequences. The process begins with compilation of two tables. One is the support system-to-support system dependency table (Table 3-1), and the other is the support system-to-front line system dependency table (Table 3-3). The support system event tree was constructed from these two tables. It was structured to account for the support system interactions listed in Table 3-1 of the Plant Model Report. For example, electric power system headings appear before cooling system headings to account for the dependence of these systems on power. There are over 6000 sequences on the support state tree. This made review of each sequence impossible, given the resource limitations of this review. However, several key sequences were reviewed for consistency with the dependency tables; the event tree appears to be consistent with those tables.

The support state event tree was reduced by computer analysis to over 1000 unique impact vectors. The report does not provide a listing of these impact vectors with the corresponding support state sequences so that a verification of the groupings can be made. Furthermore, the number of impact vectors was too large to be practical for quantification of the front line trees. Therefore, the analysts grouped the impact vectors into support states using qualitative and quantitative measures designed to ensure that all impact vectors were considered in a conservative manner. Thirty-nine different support states were identified; their effects on the front line systems appear in Table 3-5 of the Plant Model Report. There is no one-to-one correspondence between the support state sequences and the impact vectors. The impact vectors are not documented in the report, except that certain vector designators appear in Table 3-5. The support states do not list all the impact vectors that were considered in deciding the groupings. Furthermore, there is no description of what system failures constitute each support state. Therefore, it is impossible to verify that the support states and their corresponding frequencies are correct.

Evaluation of Front Line System Event Tree. The TMI-1 PRA used event sequence diagrams (ESDs) as the analytical tool for construction of the front-line system event trees. An ESD is a graphical representation of the plant response to an initiating event, and isdesigned to depict the various ways that the initiating event can proceed to either a stable end state or to core damage. From this tool, the analyst constructs the event tree.

ESD to Event Tree Construction Comments. A typical initiating event would be expected to have an ESD and event tree in the Plant Model Report. However, some events have an ESD but no event tree (e.g., steam line break in the turbine building). In contrast, some events have an event tree but no ESD (large LOCA, reactor trip, turbine trip, and loss of nuclear services closed cycle cooling water).

Documentation of the event sequence diagrams and the event trees is uneven. While five pages of text are dedicated to the general transient ESD and three pages to the event tree structure, the ESDs and event trees for the initiating events actually quantified in the analysis receive scant description. In fact, only three of the front-line system event tree descriptions exceed one paragraph. In the majority of cases, this one paragraph merely references the general transient ESD and only vaguely describes any differences from that ESD or event tree. However, for the steam line break inside the intermediate building, the report dedicates 18 paragraphs to describing the ESD and event tree. The loss of power to the ICS power supply receives 12 paragraphs while the steam generator tube rupture receives only two paragraphs of description.

The large-LOCA paragraph appears below to serve as an example of this documentation approach:

> "Most of the alleviating actions that will take place following a large RCS pipe break are the same as those shown on the general transient ESD. Many of these actions, however, are not important to preventing core damage following a large pipe break. The only early action that is required to prevent core damage is the operation of the BWST [BW]. The long-term sump

recirculation actions and containment safety features, which determine to which plant damage state a core damage scenario initiated by a large pipe break will lead, are shown in the following subtrees:

LLA (see Section 4.3.4) when the BWST is available.

MLC (see Section 4.3.7) when the BWST is not available."

The concept that the plant response to a large LOCA is essentially similar to a general transient may be correct for TMI–1, but there is insufficient documentation to demonstrate this assumption is correct.

General Transient Event Tree Comments. The bulk of the event tree descriptions draw heavily from the general transient ESD and event tree. This section will discuss the general transient ESD and event tree, followed by specific comments about other ESD/event trees.

On Sheet 5 of the ESD, there is a path where HPI is running, but the primary safety valves do not pass water from the system. The note for the subsequent minimum flow choice indicates that no 1600 psig signal was generated and that the minimum flow would therefore be available. However, several of the paths leading to that point have had low–pressure signals generated, implying that for some cases, minimum flow is unavailable.

Sheet 7 indicates that, for HPI cooling, manual start of the HPI pumps is required. However, several paths leading to HPI cooling already have 1600 psig signals, which would start the HPI pumps anyway. It is not clear why additional HPI pump operation would make PORV–only relief a success.

Sheet 8 indicates that a stuck open relief valve would lead directly to core damage. If this assumption is based on the idea that pressure will become too low for effective HPI operation, then a choice for LPI operation should be made.

Sheet 11 deals with ATWS events. The ESD shows that reactor coolant pump (RCP) trip leads to core damage (as does the event tree). However, the description of the ESD, and the success criteria description, indicate otherwise, as Page 4.1–6 acknowledges.

On Sheet 12, which is a continuation of the ATWS condition, the ESD indicates that with secondary steam relief, EFW operation, primary system relief, and the BWST available, failure of the 4 psig containment signal leads to core damage. The next sheet indicates that manual starting of the HPI pumps is a possible success path. Therefore, it is not clear why failure of the high containment pressure signal constitutes a core damage condition. Also, Sheet 11 indicates that even if MFW runs, it will run out of water in 26 minutes. Because its source of water is the CST, the EFW on Sheet 12 must be getting water from a source not shown on the ESD.

Section 4.1.2 of the Plant Model Report describes the process that was used to transfer the information contained in an ESD to an event tree. It includes a list of six steps for this process. Apparent inconsistencies between the ESDs and event trees were examined in light of these six steps to see if the inconsistencies could be explained on this basis. However, some events or paths on the ESD do not appear in the event tree and some events or paths on the event tree do not appear in the ESD. For example, the RV heading exists on the event trees to assess the likelihood of reactor vessel failure from pressurized thermal shock (PTS) events. This event is implied but not shown on the ESD. The MR heading for reestablishing HPI minimum flow following an overcooling event is not specified on the ESD.

The only success paths involving the general transient tree that are not on the main tree occur on subtree A. All other sequences going to all other trees result in core damage. This is not a trivial number of sequences. For example, subtree B contains over 1000 sequences that have no success paths for preventing core damage. There are many sequences from the transient main tree that have subtree B as their long–term conclusion. This results in many thousands of sequences, that have no impact on core damage frequency, being part of the overall quantification. The remainder of this event tree review will not examine subtrees without a success state.

Subtree A represents the long–term actions required to successfully cool the core, assuming that HPI cooling was in progress. Basically, this is the recirculation tree. The event tree contains two events (BA and BB) for which no choices are made for any sequence. There is no explanation for this condition in the text. The events do not appear on the ESD. According to the split fraction table for this tree, the quantitative values for headings DH and CS depend on operation or failure of BA and/or BB. However, no decisions are made on these headings.

Sequence 47 indicates that a failure to close the containment purge valves during a feed and bleed operation of the primary system can lead to successful core cooling if recirculation is properly aligned. This event would seem to allow for escape of reactor coolant to the atmosphere. In this case, it may be possible that a significant amount of water needed for recirculation would not be available.

The general transient ESD and event tree are documented as the basis for all subsequent ESDs and event trees in the Plant Model Report. The inconsistencies in the general transient ESD and event tree suggest that further detailed review might uncover errors that would cause the calculated core damage frequencies to be in error.

Specific ESD/Event Tree Comments. The remainder of the discussion of ESD and event tree modeling focuses on initiator-specific conditions that affect the structure of the analysis. As the other trees are based in such large part on the general transient tree, the comments from this tree apply also.

The following comments on various ESDs and event trees focus on initiators other than external events and control building ventilation events. This allows for comparison of the TMI-1 event trees to Level 1 analyses from other PRAs.

Large LOCA—The general discussion above has already discussed issues relating to the large LOCA initiator.

Medium LOCA—The medium LOCA ESD develops conditions for failure to scram following the initiator. It is not clear why this is done. The probability of such an event using the TMI-1 data is approximately 8E-8, which could be reasonably screened out of the analysis. Furthermore, the key issue for PWRs in ATWS scenarios is the ability to inject boron via the high-pressure injection system while preventing a catastrophic failure of the reactor vessel during the pressure surge. With the normal pressure relief available, and additional pressure relief via the break, this does not appear to adversely impact either scenario more than the more likely loss of feedwater or other events. Nevertheless, the ESD indicates that successful EFW flow in 5 seconds, and secondary steam relief, are sufficient to transfer this event back to the non-ATWS flow path. Failure to do so leads to core damage on the ESD. However, the event tree has no headings for RT, EF-, nor SD.

The ESD has an event for preventing boron precipitation in the core (DT). Failure of DT leads to core damage. The mechanism and justification for this decision is inadequate. Furthermore, if DT is required for success following a medium LOCA, then it should also appear in all transient sequences involving HPI cooling since open cycle primary recirculation is occurring there as well. The treatment of DT is, therefore, inconsistent.

Several headings on the event tree are not shown on the ESD. Specifically, BA/BB, SA/SB, and C3 are not on the ESD. Additionally, the ESD (Sheet 3) accounts for possible manual starting of the HPI pumps but does not similarly treat the LPI pumps.

Steam Generator Tube Rupture—The SGTR event tree is a "reduced" representation of the total tree, as is the case for all the other main trees that follow the general transient tree format. In the other cases, the logic duplications that are not shown explicitly on the trees are indicated by a "XFRn" indication at the end of the sequence, and a number somewhere else in the tree that shows the logic structure that should be followed. This method of representation is documented in Section 4.1.2 of the Plant Model Report. However, none of the "transfer" points are labeled on the SGTR tree.

Excessive Feedwater—After control building ventilation failures and external events, this tree contains a significant dominant sequence. There is very little discussion of the details of this sequence.

Sheet 2 of the ESD contains a block labeled "Terminate Overspeed." It seems that this should indicate overfeed instead. It is not apparent why this block should not appear before the EFW block on the ESD. If overfeed is terminated, then EFW is not required. If EFW is needed, then main feedwater must have already failed and the "terminate whatever" block is unnecessary. It is not clear why the logic on the ESD for overfeed conditions differs from the logic for overfeed on the general transient tree.

The ESD indicates by use of a dashed line that the SLRDS is not to be considered on the event tree. SLRDS is included on the event tree despite rule number 5 from Section 4.1.2, which states:

> "Dashed blocks on the ESDs do not become event tree top events."

Steam-Line Break in the Intermediate Building—The main steam line break in the intermediate building, main tree discussion, contains a paragraph that indicates that the SLRDS operates to stop feed flow to the steam generators and thereby limits overcooling. It states that the SLRDS does this operation so quickly that "the transient is limited and does not cause an excessive cooldown, as manifested by a low RCS pressure engineered safeguards actuation." On the next page of the discussion this section states:

> "On a steam line break, the high pressure injection system receives a start signal due to the excessive cooldown and results in low RCS pressure caused by the break."
>
> It appears that some text must be missing.

Review of Event Tree Quantification. The quantification process includes the assignment of split fractions, for each support state, to the main and sub tree headings. For each main and sub tree, there is a table in the PRA report that lists the support state numbers across the top and the heading down the side. For some reason, some of the headings are duplicated many times in the tables. There does not appear to be any reason for the duplication. This appears to be a problem in the computer printout for the boundary condition tables.

These tables are where the boundary conditions for the headings are entered into the code for quantifying the event trees. Therefore, it would be reasonable to expect a one-to-one correspondence between the number of split fractions (other than the default) in the table for a given support state, and the support state table developed earlier. The review found that this is not necessarily the case. For example, the turbine trip boundary condition table (Table 4.2.12-2) does not compare favorably with the support state table (Table 3-5), in several areas. The MF- heading in Table 3-5 indicates 32 states that impact this heading, but the boundary table only shows 31 (support state 34 is not included). For the EF- heading, both tables indicate 30 cases where there are support state impacts on the heading. However, they are not the same 30 headings. Support states 5 and 6 appear to be extraneous in the boundary condition table; support states 10 and 30 show no impact. In the case of the TH heading, the boundary condition table has 27 impacts, whereas the support state table shows 24 impacts. The boundary condition table has nine impacts listed that are not shown in the support state table, and six impacts that are in the support state table but not in the boundary condition table.

It was not feasible in this review to check the agreement of all the boundary condition tables with the support state table. However, the headings noted above (main feedwater underfeed, emergency feedwater underfeed, and operator throttling of HPI) would be expected to receive considerable attention in the quantification process. The report contains a general description of how tables like Table 4.2.12-2 are derived, but so many numbers and operations are involved that it was not possible to trace the derivations of the numbers in these tables.

The final step in the review was to verify that the calculations of individual sequence frequencies were correct. Table 6-5 of the PRA report lists the top 100 sequences from the quantification process. Several sequences from this list were examined to see if the frequencies stated are accurate, provided input data and models are correct. No mistakes were found in the quantifications of these sequences.

In summary, the quantification process for the TMI-1 PRA was very complex. It was not possible, using the available information, to verify the quantification of the PRA, except in a general fashion. There are questions about the translation of information from the support state tables to the main- and sub-tree inputs that suggest questions about the accuracy of this step in the process. In this review, the quantification results presented in Table 6-5 were traced to the extent of the split fraction headings and the presumed support state frequencies. The multiplications of the values listed in Table 6-1 and the support state Table 3-7, for the sequences reviewed, were correct.

Summary of Event Tree Evaluation. The event trees in the TMI-1 PRA report were developed in a form specifically adapted for solution using computer programs. For a large, complicated plant like TMI-1, event trees like these are difficult to review in detail. There is a lack of complete traceability even in a document as lengthy as the TMI-1 PRA report. In the limited review that was performed, some minor inconsistencies between the ESDs and event trees were identified, and some assumptions were questioned. Some questions were raised about the support states appearing in the event trees. However, no major errors were found. Therefore, it is concluded that this event tree review has not revealed any major changes that are needed in the event trees published in the TMI-1 PRA report.

Important Assumptions

Introduction. PRAs rely, in general, on numerous assumptions in order to allow the computation of risk results. These assumptions are usually employed for one of two reasons: (1) to simplify the analysis, or (2) to provide necessary input when data and information is lacking in a particular area. The uncertainties and unknowns in these assumptions can be accounted for by performing sensitivity studies to quantitatively estimate the influence of uncertainties in the assumptions, and then making appropriate adjustments to the overall results to reflect these uncertainties.

This section reviews those potentially important general, or global, assumptions which were made in the PRA and were not necessarily reviewed in the other sections of this review report. Particular attention was focused on assumptions which are unique to this PRA, which appear to be inconsistent with current information, which appear to be particularly significant, or which appear to have inadequate bases. Assumptions specific to a particular system, model, analysis, data application, quantification, etc., are considered separately in appropriate sections of this report.

In the TMI–1 PRA, a large number of assumptions were found. Many of these assumptions are aggregated in specific sections or subsections of the report. However, others were found scattered throughout the text. In some cases, the assumption is specifically identified, but in other cases assumptions are characterized by "engineering judgement," "it is reasoned that," or some other descriptor. In a few cases, the assumption is merely a statement of what was done in the assessment without any indication that an assumption was made. As a result, it was somewhat difficult to identify all important assumptions.

In most cases, the TMI–1 PRA provides a qualitative indication of the influence of the assumption, and, in a few cases, a quantitative estimate is provided. In a majority (but not all) of these cases, the assumption is characterized as conservative (i.e, the assumption would tend to increase the risk result over the "true" value), but not overly significant (characterized as "slightly conservative" or "not overly conservative"). In a few cases, no evaluation is provided of the influence of the assumption. In some cases, further study is called for to support the validity of the assumption, or provide the basis for a revised assumption, if the assumption is subsequently determined to be important to the overall result.

In some cases, what is described in the PRA as an assumption is actually a boundary condition, or a condition related directly to the actual design of the plant, or the consequence of the occurrence of a previous condition (e.g., the primary coolant pumps are assumed to be inoperable following loss of offsite power). While these stated conditions may fit the overall definition of assumptions in a general context, they are of no interest in this evaluation since they are not associated with uncertainty or questionable bases.

In order to focus available resources on those assumptions with the greatest potential for influencing the results, an evaluation of the risk profile of the TMI–1 plant, as estimated in the PRA, was undertaken. The PRA contains a significant amount of condensed information to facilitate such an evaluation. The evaluation consisted of identifying those initiating events, accident sequences, system failures, etc., which were important contributors to the overall results in terms of core damage frequency (CDF). The results of this evaluation are presented in the following sections.

TMI–1 Risk Profile. The "risk profile" of a plant generally refers to a significance ranking of individual contributions from the following elements: (1) accident sequences, (2) initiating events, and (3) system failures in terms of contribution to overall risk. An evaluation of the relative ranking of the individual contributions within these elements was undertaken as part of the review of assumptions. This allowed the available resources to focus on those assumptions associated with the risk dominant contributions. It should be noted that a risk profile can also be further subdivided to include the significance of human actions and component failure rates which contribute to the overall estimated risk from the plant. These elements are considered separately in the sections on Human Responses and Failure Data.

Dominant Accident Sequences. Table 4, developed from a similar table in the TMI–1 PRA, illustrates the top 11 accident sequences. The distribution of contributors is rather peculiar in that a single sequence (loss of control building ventilation) is a very large contributor (33.3%) to the total CDF. Furthermore, the next most dominant sequence is a rather small contributor (5.5%), followed by two more sequences with small contributions (3.6% each). Following the fifth sequence, the remaining individual sequence contributions drop dramatically to <2%. Thus, the top five sequences contribute almost half (48.4%) to the overall CDF, while a similar contribution is provided by low probability sequences. Any assumption with the potential to influence the probability of the single most dominant sequence would be expected to have a significant influence on the overall CDF. On the other hand, assumptions associated with any other individual sequence would have to increase the probability of the sequence dramatically before any significant increase in the overall CDF would occur. For example, a factor of 10 increase in the probability of the second most dominant sequence (sequence #2 in Table 4) would increase the overall CDF by only 50%. Changes in assumptions which would reduce any but the most dominant sequence would have an insignificant impact, even if the sequence were eliminated. In fact, if all sequences except the most dominant were eliminated, the overall CDF would only be reduced by a factor of three, not a very significant change in view of the estimated uncertainties discussed in this report.

Some assumptions will obviously influence more than one sequence, and therefore could be important. For example, sequences 2 through 4 all have fires as the initiating events. Thus, any assumption which influences the estimated frequency or subsequent control of fires can change the probability of each of

Table 4. Dominant scenarios from TMI-1 PRA

Description	Mean Frequency Per Reactor-Yr	Total (%)
Loss of control building ventilation and failure to establish alternate room cooling	1.83E-4	33.3
Fire in auxiliary building. MCC area AB-FZ-6	3.00E-5	5.5
Fire in control building. SW room 1S	2.00E-5	3.6
Fire in control building. ESAS cabinet area	2.00E-5	3.6
Med. LOCA and fail to establish sump recirculation	1.30E-5	2.4
Excessive main feedwater, leading to HPI; fail to provide HPI min-flow recirculation after HPI flow throttling, leading to HPI pump failure; and failure of RCP seal cooling to seal LOCA with no HPI	1.02E-5	1.9
Fire in control building. IE SW room	1.00E-5	1.8
Loss of air; failure of RCP seal injection and cooling	6.26E-6	1.1
Large LOCA and fail to establish sump recirculation	5.95E-6	1.1
SGTR and fail one train of DHR and opposite train of DHCCCW, leading to loss of long-term DHR	5.88E-6	1.1
Very small LOCA and fail both trains of DHCCCW, leading to loss of long-term DHR	5.78E-6	1.1
	Subtotal 3.1E-4	56.5
	All others 2.4E-4	43.5
	Total 5.5E-4	100.0

these sequences. (See the External Events Section for an evaluation of the external events analysis, including fire methodology). However, except for the top four sequences, a rather large probability increase in a significant number of sequences would be required to produce a significant change in the total CDF.

Dominant Initiating Events. Table 5, extracted from the PRA, shows the ranking of accident initiating events. As would be expected, based on the preceding discussion of dominant accident sequences, loss of control building ventilation dominates the accident initiator contributions to CDF. In fact, the probability of the second most dominant initiator (steam generator tube rupture) would have to be raised by over a factor of five to become as important as the loss of control building ventilation initiator.

Dominant System Failures. The contribution of individual system failure probabilities can add further perspective on the risk profile. Table 6, taken from the PRA, shows the relative ranking of system failure contributions to the CDF. Unlike the dominant accident sequences and initiating events discussed previously, there is no single system which overshadows the risk contributions. The top seven systems all contribute over 20% to the frequency of CDF. After the seventh

Table 5. Dominant initiating events from TMI–1 PRA

Description	CDF, Mean Frequency Per Reactor–Yr	Total CDF (%)
Loss of CBV	2.00E–4	36.4
Loss of other support systems	4.53E–5	8.2
Loss of offsite power	2.90E–5	5.3
Loss of river water to pumphouse	1.58E–5	2.9
All other transients	6.09E–5	11.1
Very small LOCAs including SGTR	5.58E–5	10.1
All larger LOCAs	3.58E–5	6.5
LOCA outside containment	1.00E–7	<0.1
Fires explicitly modeled	8.64E–5	15.7
All other fires and all internal floods	<1.00E–5	<2
Earthquakes	2.70E–6	0.5
External flood	7.5E–6	1.4
Tornado	1.2E–8	<0.1
Turbine missile	2.3E–7	<0.1
Aircraft crash	1.0E–7	<0.1
Toxic chemical	2.6E–7	<0.1

Table 6. Systems contributing to core damage frequency, from internal initiators, TMI–1 PRA

System	Contribution to CDF from Internal Events[a] (%)
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

a. Total percent sums to more than 100, because more than one system failure may occur in a given core damage sequence.

highest system, the contribution drops significantly (down to 9%). Specific assumptions relative to plant modeling and system reliability associated with these systems are considered in other sections of this report.

Evaluation of Major Assumptions. This section evaluates the major assumptions made in the TMI–1 PRA, with particular attention given to the risk dominant contributors identified in the preceding discussion. In addition, assumptions made in the area of the overall scope of the PRA study are included.

Scope. The scope of the study conforms generally with traditional PRA studies. Only one aspect of the scope was found to be questionable and selected for evaluation. This aspect is the limitation of the study to consideration of core damage events which may be initiated only from elevated power levels.

Specifically, the study limits consideration of accidents, according to page 1–10 of Volume 2, to those initiated from power levels above 15% (the power threshold, according to the study, for automatic feedwater control). The study further states (page 1–11) that the PRA team considered accident initiating events from shutdown conditions to be "insignificant." However, no basis is given for this judgement.

In recent years concern has been developing, among the NRC and others, that core damage frequency due to accidents initiated during shutdown conditions may be significant enough to warrant consideration. This concern appears to have been generated primarily from event reports indicating instances where the integrity of decay heat removal during shutdown conditions has been compromised, most recently in the incident at Diablo Canyon.[15]

As a result of this concern, the NRC established Generic Issue 99, "Improved Reliability of RHR Capability in PWRs," to examine the issue. In support of the on-going resolution of this issue, Brookhaven National Laboratory performed a study of the frequency of core damage due to insufficient decay heat removal under shutdown conditions.[16] Their study concluded that the frequency of such events was 5.22E-5/yr for PWRs. While the study used the Zion plant as a model and data in Reference 17 as a framework, the results were considered as representative of "most" U.S. PWRs. This result, if it applies to TMI-1, would represent an approximate 10% contribution to the core damage frequency estimated in the TMI-1 study (mean frequency 5.5E-4/yr) and would thus become the second most dominant contributor.

As a result of these considerations, the TMI-1 PRA assumption that the frequency of core damage accidents from shutdown conditions is "negligible" is considered questionable, and the basis for it (judgement of the PRA team) inadequate.

Initiating Event Frequencies. As indicated above, a single initiating event, loss of control building ventilation, is by far the most significant initiating event in the PRA. In efforts to obtain additional information to assist in evaluating the loss of control building ventilation sequence, additional documents were obtained which are relevant to the issue.[12, 13] These documents were prepared by GPUN Corporation in support of their assessment of the compliance of the TMI-1 plant to Appendix R (fire protection). They were not submitted in support of the PRA, and the PRA is not discussed in the documents. However, the documents do provide a rather detailed evaluation of the control building heat-up rate following loss of ventilation and also provide additional data to support the conclusion that much of the equipment in the building can survive temperatures in excess of 104°F. The basic conclusion from the evaluations is that the loss of control room ventilation will not result in loss of the core cooling function for times up to 72 hours, although some minor human actions would be necessary, including opening doors and turning off lights in the control room. This conclusion is supported by detailed analysis supplemented by test data. The evaluation appears to be reasonable and consistent and has been accepted on the basis of an NRC review.[14] An analysis of the effects on the PRA would require substantial effort and was therefore not undertaken as part of this review. However, on balance it appears that the contribution to core damage from the loss of control building ventilation accident sequence is grossly overestimated in the PRA and is probably negligible.

As a result of this review of material related to Appendix R, the assumptions in the PRA relating to sequences involving loss of control building ventilation appear to be moot. Some review of these assumptions was done and appears here as Appendix A to this review report. Additional assumptions relative to other initiating events are provided in the Initiating Events Section of this report.

Miscellaneous General Assumptions. This section identifies and evaluates miscellaneous general assumptions which are considered to be inconsistent or unusual compared to standard PRA practice, or are considered questionable on other grounds. Only general, or global, assumptions are considered here which are not specific to individual elements of the PRA. These more specific assumptions, as noted previously, are considered in other relevant sections of this report.

Omitted Dependencies. The PRA states on page 1-8, Volume 2 that "certain dependencies...were judged to be insignificant contributors 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." However, Volume 7 does include consideration of high energy line breaks in the spatial interactions analysis, failure of non-seismic Class I components causing failure of Class I equipment has been found to be an important contributor in other PRAs, but high energy line break flooding has not.[18, 19]

V-Sequence. It is assumed in the PRA (page 1-11) that the V-sequence accident (rupture of the primary system into the low pressure RHR system, causing RHR pipe rupture) leads directly to core damage, and is therefore not treated explicitly in its own event tree. The basis for this assumption is that the sequence has a very low frequency. The frequency of the event was found elsewhere in the PRA (Volume 5, page 3-17,18) to be 7.89E-8/yr. While this assumption is conservative and may not have a significant influence on the overall PRA results (which exclude consideration of offsite consequences), it should be recognized that this accident sequence can result in very large offsite consequences, depending on the plant configuration in the vicinity of the RHR line break. On the other hand, a recent analysis for a different PWR indicates that this sequence may not rupture the RHR piping; instead, this sequence will result in a much more benign sequence with reduced core damage probability and lower source terms even if the core does melt.[20] It would appear appropriate, especially if the PRA is to be extended into a Level 3 risk assessment, to evaluate this sequence in more detail.

RV Rupture. The potential for reactor vessel rupture from pressurized thermal shock (PTS) conditions has become a safety issue of concern in recent years, particularly for older plants. Thus, assumptions regarding the treatment of this issue in the PRA were examined. On pages 1–13 & 14 of Volume 2, the general approach to the issue is discussed, and it is stated that "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 5E–4. The event is accounted for by including reactor vessel rupture on all event trees where PTS might occur." The PRA also assumes (page 1–14) that no credit is given for mitigating reactor vessel ruptures. A more detailed discussion of excessive cooldown events and PTS is given on page 4.1–12 and 13 of Volume 3. Here it is stated that "In each situation where an excessive cooldown occurred, the likelihood of reactor vessel rupture was considered. The basis for this likelihood is the pressurized thermal stress analysis done by Babcock & Wilcox and GPUN and documented in the Systems Analysis Report (Volume 4), Section 19." However, the B&W analysis was not in the PRA report—it was to be provided at a later time. Thus, the specific treatment of PTS in the PRA could not be reviewed completely. See the section on Comparisons with Generic and Unresolved Safety Issues for more discussion.

Dependency Analysis

Introduction. This dependency analysis was performed to determine if all of the frontline support systems and their support systems were modeled in the analysis.

Review Approach. System dependencies are discussed in Volume 3, Chapter 3 and Volume 4, Chapter 1 of the TMI–1 PRA. Volume 3, Chapter 3 identifies the frontline and support systems and describes the system dependencies. Volume 4, Chapter 1 provides tables listing the frontline systems, support systems, and the systems screened from the PRA because they did not support safety functions. Some of the system description chapters in Volume 4 also describe some of the system dependencies. A major problem encountered in the review of the dependency analysis was that the PRA did not describe all of the TMI–1 systems—most of the system descriptions only discussed the failure events—thus, it was very difficult to evaluate the PRA–identified dependencies. The PRA should have provided enough of a system description to allow an independent evaluation of their conclusions, and to tell the user what the system configuration was at the time of evaluation. If this information had been provided the PRA user could determine easily if the analysis still applied to a particular system or if the system has been modified since the PRA. It was necessary to obtain the P&ID's and FSAR to determine the system functions and their support systems.

For this review, the system dependencies were determined independently by selecting the systems designated as frontline systems in Table 1–1 of Volume 4, Chapter 1 and using the P&IDs and the FSAR to identify all of the support systems for the frontline systems. The support systems were then examined to identify their support systems. The P&ID's were then reviewed to determine if there were any other systems that could be important to safety but were not included in the frontline or support systems found in the above investigation. The system dependencies discussed in the TMI–1 PRA were then compared with the dependencies found above to determine if all of the support systems were considered in the analysis.

Electrical Dependencies. The electrical dependencies of the frontline systems and their support systems were identified in the individual system discussions of Volume 4, books 1, 2, and 3. The electrical dependencies for all frontline and support systems, except the systems discussed below in the discussion of the mechanical system problems, were identified in the PRA. The electrical power supplies identified in the PRA for several of the systems, and some of the components for other systems, were checked against the P&IDs and the FSAR and found to be correct.

Mechanical Dependencies. The following mechanical support systems are not discussed in the TMI–1 PRA but they appear to be important systems:

- Fuel Oil and Feed Pump Seal and Leak Off System
- Turbine Lube Oil System
- Diesel Generator Services
- Diesel Generator Lube Oil Systems
- Diesel Generator Jacket & Air Cooler Coolant System
- Diesel Generator Gear Box Lube Oil System

- Fuel Oil Unloading Stations.

The Feed Pump Seal and the Turbine Lube Oil systems support the main feedwater pumps. The only accident sequences that could be non-conservatively affected by not considering these systems are the sequences involved with maintaining enough feedwater to the steam generators with the main feedwater pumps. Accident sequences involved with failure of the main feedwater pumps contribute about 14% to the core damage frequency; however, only 0.1% of those failures involve main feedwater pump failures that are not guaranteed failures such as "operator trips main feedwater pumps," or "main steam isolation valves closed." Based on the small contribution of main feedwater pump failures to the core damage frequency, including the affects of the feed pump seal and lube oil systems would probably not have a significant impact on the core damage frequency. Other main feedwater pump accident sequences are involved with overcooling, thus not considering a possible failure mode would be conservative.

Diesel Generator Support Systems. The systems associated with the diesel generators will affect the availability of the diesel generators; however, all but the Fuel Oil Unloading Stations and the Fuel Transfer Pumps are an integral part of the diesel generators and are considered in the development of the diesel generator failure rate. The TMI–1 PRA used plant specific experience in the development of diesel generator "fail to start" and "failure during first hour of operation" failure rates, and generic failure rates for the the "failure after one hour of operation" failure rate. Because the lube oil and coolant circulating systems are integral to the diesel generators, their failure rates will be part of the plant specific and generic failure rates. The fuel transfer pumps and fuel storage tanks are plant specific, and they are not required until three hours after the diesels are started, thus their contribution to the diesel generator failure rate will not be included in the plant specific or generic failure rates. The mission time of the diesel generators is 24 hours, and the diesel generator day tanks have about a 3–hr fuel supply; thus the pumps must start and fill the day tanks seven times during the 24–hour mission. Each diesel generator has a dc and ac powered fuel transfer pump with automatic start based on day tank fuel level. The pumps are powered by the Engineered Safeguards buses. Diesel generator failures contribute about 9% of the core damage frequency. But given the dual power sources for the pumps, their unavailability is probably very small.

Other Dependencies. The following mechanical support systems are listed in the TMI–1 PRA as not important to safety and not considered further, but they appear to be important to the frontline or support systems they support:

- Station Fire Protection System
- Penetration Pressurization System
- Fluid Block System.

The Station Fire Protection system is listed as not important to safety; however, it is the backup coolant supply for the Instrument Air Compressor. In fact, the PRA indicates in another chapter that the Instrument Air Compressor cooling system has such a small failure rate that it can be ignored because of the backup cooling system. Listing the Fire Protection system as not important to safety is an error in the system description only; the analysis results pertaining to the Instrument Air Compressor are correct.

The Penetration Pressurization System and the Fluid Block System are parts of the Reactor Building Isolation System (RBIS). Although the RBIS will not contribute to preventing core damage and need not be considered in a Level 1 PRA, the TMI–1 PRA lists the RBIS as a frontline system and calculates an unavailability for the system. Not considering the Penetration Pressurization and the Fluid Block system ssurization System pressurizes all electrical penetrations, the fuel transfer tubes, the equipment access in the RBIS unavailability could be a serious underestimate of the RBIS failure rate. The Penetration Prehatch, and the normal and emergency personnel air locks, and the Fluid Block System backs up the containment isolation system valves by pressurizing the piping between the valves and/or the valve bonnets. Loss of these systems could open significant leakage paths from the reactor building to the environment.

Some other minor discrepancies found during the dependency review are noted below:

Table 1–1 of Volume 4, Chapter 1 lists the frontline systems. The frontline systems listed on the table do not agree with the frontline systems identified in Volume 3, Chapter 3. Frontline systems identified on Table 1–1 that are not identified as frontline systems in Chapter 3 are: BWST, PORV/SRV, Reactor Building Emergency Cooling, High Pressure Injection, Low Pressure Injection, Main Steam Safety Valves, Reactor Building Sump, Electrohydraulic Control, Make Up, Seal Injection, and Condensate.

Parts or components of some of the systems are discussed in Chapter 3, and the write-up of Chapter 3 indicates the Condensate System is considered in the Main Feedwater System, but it is very difficult to determine if all important system components were considered in the dependency analysis.

Table 1-2, Support Systems Analyzed, indicates that the Condensate Polishing and Condenser Circulating Water systems were analyzed as support systems. Volume 3, Chapter 3, Support System Model does not indicate these systems are support systems. They are shown in some of the figures of Volume 4, Book 2, Chapter 10, Main Feedwater and Integrated Control System Analysis, but not discussed.

Plant Visit to TMI-1. During the plant visit to TMI-1,[a] a brief tour of the buildings containing safety-related equipment was conducted. The equipment appeared to be adequately separated and free of obvious common cause failure dependencies that might be activated by internal fires, flooding, seismic or other environmental shocks. Most safety-related valves appeared to be operable by handwheels as well as by motors. The only obvious common cause failure mechanism was flooding above the PMF elevation of 310'—the equipment required for safe shutdown is consistently protected up to this elevation.

Conclusions. The TMI-1 PRA considers all important support systems except for systems supporting the diesel generators, the main feedwater pumps, and the RBIS. The fuel transfer system for the diesel generators is required to function during the 24 -hr mission time; thus not considering it could conceivably have a significant impact on the core damage frequency because failure of the diesel generators contributes 9% to the core damage frequency. But the fuel transfer system appears to be very reliable: each diesel has two pumps, one ac powered and one dc powered, with the power supplied by the Engineered Safeguards Buses. The feedwater-pumps failures contribute less than 0.1% to the core damage frequency; thus, increasing the feedwater pump failure rate to include the seal and lube oil system failure rates would probably not cause a significant change to the core damage frequency. The RBIS support systems not considered by the TMI-1 PRA should have been factored into the development of the RBIS failure rate; however, the RBIS does not contribute to the prevention of core damage.

Comparison With Crystal River 3 PRA

An important feature of the review of any PRA is to compare the results to the results of other PRAs performed for similar plants. In this case, the Crystal River 3 (CR-3) PRA serves as the comparison tool.[22] The purpose of this comparison is to evaluate whether or not the estimates of core damage frequency for the two PRAs produce any insights that indicate a difference in either the design and operation of the plants or the performance of the PRAs.

The method of comparison in this review focuses primarily on the differences in the results and methodology of the two PRAs. This is due to the fact that TMI-1 and CR-3 are Babcox and Wilcox (B&W) plants of almost identical design. Table 7 shows the major systems analyzed by both PRAs and indicates the similarity between the plants. The only obvious differences are in the cooling water systems, the use of two motor driven EFW pumps at TMI-1 whereas CR-3 uses one motor driven EFW pump, and different vendors for the RCPs. Review of the success criteria for the major systems and functions indicates no significant differences. This comparison discusses the similarities and differences between the two PRAs and notes the areas where significant differences exist.

Analysis. Both the CR-3 and the TMI-1 PRA reports indicate that they were Level 1 PRAs.[1] A Level 1 PRA is an evaluation of the likelihood of core damage for a nuclear plant and includes technical analyses as outlined in the PRA Procedures Guide.[3] As noted elsewhere in this review, the TMI-1 PRA includes much more analysis than is necessary for a Level 1 PRA. The systems analysis and event tree models from the TMI-1 PRA went beyond the end state for a Level 1 PRA and included evaluations of systems that have no impact on the estimation of core damage frequency. The analysis was typical of that performed prior to a Level 2 or 3 analysis in which systems relating to containment performance and post-core damage phenomenology are included. This results in more complex event trees and makes comparison of the results of the two PRAs more difficult.

In addition to the fact that the TMI-1 PRA examined sequences beyond the scope of a Level 1 PRA, the method of analysis for the two PRAs is different. The TMI-1 PRA uses support state event trees

a. Letter from H. J. Reilly, EG&G Idaho, to Dr. Arthur Buslik, NRC, "Report of TMI-1 Plant Visit, October 18-19, 1988," November 8, 1988.

Table 7. Comparison of Crystal River-3 and TMI-1 systems

System or Function	TMI-1	CR-3	Comments
Reactor vendor	Babcock and Wilcox	Babcock and Wilcox	TMI-1 is rated at 2772 MWt, CR-3 is 2560 MWt
Reactor coolant system	Two hot loops, four cold loops	Two hot loops, four cold loops	
Reactor coolant pumps	Four Westinghouse pumps	Four Byron-Jackson pumps	
Steam generators	Two B&W OTSGs	Two B&W OTSGs	
High pressure injection/make-up	Three pumps with one normally running	Three pumps with one normally running	
Low pressure injection/DHR	Two pumps and heat exchangers	Two pumps and heat exchangers	
HPI/LPI control	ESAS	ESAS	
Power conversion system	Turbine bypass, main condenser, two steam driven feedwater pumps	Turbine bypass, main condenser, two steam driven feedwater pumps	
PCS control	B&W integrated control system	B&W integrated control system	
Emergency feedwater	One turbine driven and two motor driven pumps	One turbine driven and two motor driven pumps	
Emergency ac power	Two emergency diesel generators	Two emergency diesel generators	
Emergency dc power	Two emergency dc batteries	Two emergency dc batteries	
Cooling water systems	NSCCCW, NSRW, DHCCCW, and DHRW	NSCCW, NSSW, DHCCCW, and DHSW	TMI-1 has 3 pump trains for NSCCW and NSRW while CR-3 has five NSCCW pumps. DHCCW are similar. Both have 3 pumps dedicated to NSSW and one to each DHSW train.

combined with front line event trees: the support state methodology (large event tree/small fault tree) approach. This approach relies on the analyst to either explicitly depict all dependencies between event tree headings, or to develop appropriate models of the systems for specific boundary conditions (referred to as split fractions). This method produces a very large number of sequences to estimate the core damage frequency. The CR–3 PRA uses the fault tree linking (small event tree/large fault tree) approach to modeling the plant response. In this method, dependencies between headings are accounted for by including the common events in the fault trees for each of the systems and using a computer code to generate sequence cut sets that appropriately account for them. Comparison of the results of two PRAs that use such distinctly different methods requires that care be exercised to insure a fair comparison.

With the systems analyses so different, the most practical points of comparison between the two PRAs are at their beginnings and at their ends. The initiating events and the core damage frequency estimates provide a framework for examining the differences between the two PRAs.

Initiating Events Comparison. Another section of this review examines the details of the TMI–1 initiating event analysis. This section compares the starting points for the two PRA analyses without examining the details. There are three general areas for PRA initiating events: loss of coolant accidents (LOCAs), transients, and special initiators. This section compares the treatment of these events by the two PRAs.

The TMI–1 PRA includes initiating events for four LOCAs and for steam generator tube rupture (SGTR) events. The TMI–1 LOCAs are classified as large, medium, small, and very small LOCAs. The CR–3 PRA uses only two classifications, large and small, along with the SGTR event. The frequencies for these events in the two PRAs are comparable, with TMI–1 frequencies for the small and very small LOCAs slightly higher (factor of 2) and large and medium LOCAs slightly lower (factor of 1.5).

The general transients for the two plants correspond. They include turbine trips, reactor trips, feedwater disruptions, and steam line breaks. The frequencies for the TMI–1 events are similar to the CR–3 events, with the exception of reactor– and turbine–trips and loss–of–feedwater events. The TMI–1 frequencies for these initiators are approximately a factor of 2 lower than the CR–3 frequencies. Data for the TMI–1 PRA included only the years of operation prior to the accident at TMI–2 that resulted in the shutdown of TMI–1 for several years. It is not known what the impact of the year of operation that occurred after restart would have on these values.

Special initiators evaluated by both PRAs included loss of offsite power, loss of air, loss of ICS power, and loss of river water. The CR–3 PRA included loss of air in its loss of feedwater initiator since its only impact was on the feedwater system. TMI–1 separated loss of air because of impacts on systems not related to core damage prevention. The CR–3 PRA also included loss of a single ac bus, spurious ES actuation, and spurious low pressure signal initiating events. Although the TMI–1 PRA did not explicitly model these events, the results of the CR–3 analysis indicate that they were not contributors to the dominant sequences. Thus, their omission does not appear to be significant.

A special class of events that is considered in PRAs is anticipated transients without scram (ATWS) events. Some PRAs treat these events as initiating events, while others treat them as part of the event trees. In the case of the TMI–1 PRA, each of the event trees for transient initiators includes sequences relating to ATWS mitigation. The CR–3 PRA relies upon thermal–hydraulic analyses that indicate that the most severe ATWS scenario would result in a LOCA with the HPI and LPI systems unaffected. Thus, they conclude that the analysis of LOCAs bounds the response for ATWS events. It appears that the treatment of ATWS events explicitly in the TMI–1 PRA reflects the more standard approach. However, ATWS events are not part of the dominant contributors from the TMI–1 sequences.

In summary, the TMI–1 PRA compares favorably with the CR–3 PRA with respect to initiating event selection and frequency evaluation. The TMI–1 overall transient frequency appears to be a factor of 2 lower than the CR–3 frequency. The differences in special initiator selections appear to be due to reasonable grouping preferences of the analysts. The lack of dominant sequences involving these initiators from either PRA indicates that disparities in this area are not significant.

Comparison of Dominant Sequences. As noted earlier, there was a significant difference in the manner in which the two PRAs analyzed the plant response to initiating events. The TMI–1 PRA included analyses relating to containment systems. The TMI–1 PRA examined the effects of fires and floods. In addition, a significant increase in the core damage frequency for the TMI–1 PRA was caused by the assumption that a loss of control building ventilation would lead to core damage due to failure of the electric power to the seal injection and cooling systems. Another part of this review report concluded that this assumption was unnecessary.

For the remainder of this section, comparison of the two PRAs will ignore the effects of several events in the TMI–1 PRA that were not included in the scope of the CR-3 PRA. Table 5-1 of the TMI-1 Technical Summary Report details the effects of initiating events on the core damage frequency estimate. Excluding control building ventilation failures, fires, floods, and earthquakes reduces the core damage frequency estimate from 5.5E-4/yr to approximately 2.5E-4/yr. The remaining sequences are the basis for comparing the results of the TMI-1 PRA with the results of the CR-3 PRA.

The ANL review of the CR-3 PRA, including unpublished information that ANL referred to as the "updated" PRA, concluded that some of the sequence frequencies should be different from those published in the CR-3 PRA.[23] The principal changes recommended by ANL involve a) frequency of small-break LOCAs, b) frequency of turbine trip, c) several errors they found in the CR-3 fault trees. Regarding small-break LOCAs, we commented earlier (see Initiating Events section) that the frequency for TMI-1 should be higher than that used in the PRA. Regarding frequency of turbine trip, the TMI-1 PRA used plant-specific data. It remains to be seen whether future operation of TMI-1 will continue to have such low values for reactor and turbine trip. Finally, if errors existed in the CR-3 fault trees that caused the conditional core damage frequencies to be erroneously small, that would serve to explain some of the difference that we noted above regarding the comparison between conditional core damage frequencies for CR-3 and TMI-1.

Table 8 compares CR-3 and TMI-1 results, using the values reported in the ANL review for CR-3. Generally, the agreement in estimated CDFs for given initiators is quite good. However, there are larger differences when the initiator frequencies and conditional core damage probabilities are compared.

Table 8. Comparison of Crystal River-3 and TMI-1 PRA results

	TMI-1[a]			CR-3[b]		
Initiating Event	IB Freq.	Est. CDF	Cond. Prob.	IB Freq.	Est. CDF	Cond. Prob.
Turbine Trip	1.64E0	1.28E-5	7.8E-6	—	—	—
	—	—	—	6.7E0	1.20E-5	1.8E-6
Reactor Trip	1.38E0	2.1 E-5	1.5E-5	—	—	—
Loss of MFW	2.33E-1	3.18E-6	1.4E-5	1.40E0	7.60E-6	5.4E-6
Excessive MFW	1.18E-1	1.8E-5	1.5E-4	—	—	—
LOSP	7.10E-2	2.90E-5	4.1E-4	3.50E-2	3.40E-5	9.7E-4
SGTR	1.13E-2	3.84E-5	3.4E-3	8.60E-3	3.80E-6	4.4E-4
Loss of Air	6.00E-3	1.98E-5	3.3E-3	—	—	—
Loss of RW/SW	7.41E-3	1.58E-5	2.1E-3	5.60E-3	2.10E-5	3.8E-3
Large LOCA	1.91E-4	8.24E-6	4.3E-2	5.0E-4	6.4E-6	1.3E-2
Med LOCA	4.20E-4	1.97E-3	4.7E-2	—	—	—
Small LOCA	2.20E-3	7.27E-6	3.3E-3	3.00E-3	1.40E-5	4.7E-3
Very sm LOCA	5.19E-3	1.74E-5	3.4E-3	—	—	—

a. TMI-1 PRA.

b. ANL review of CR-3 PRA.

Comparison of the sequences remaining in the TMI–1 PRA when external events and the control building ventilation sequences are removed reveals that the top ten sequences for TMI–1 are similar to those for CR–3. While the relative order between the two varies slightly, the basic features are the same. Each of the sets of sequences contains transient events with core damage occurring due to seal LOCAs and failure to makeup to the primary system. Each contains LOCAs with failure of recirculation switchover. Steam generator tube ruptures with failure of decay heat removal are in both sets of sequences. Thus, it appears that the two PRAs produce similar dominant sequences when the external events and control building ventilation events are excluded from the TMI–1 analysis.

There are some important differences in the manner in which the two PRAs treat the seal LOCA events. The dominant seal LOCA scenario from the TMI–1 PRA involves events which result in overcooling of the primary system, leading to an HPI initiation. This is due to shrinkage of the primary coolant volume resulting in reduced pressurizer level, which causes pressure to drop. The TMI–1 analysis asks the question as to whether or not the operator will take action, in accordance with his procedures, to throttle HPI flow before overpressurizing the primary and causing the power operated relief valve (PORV) or safety relief valves (SRVs) to open. Assuming that the operator has properly diagnosed the condition and is throttling HPI flow, the analysis then assumes that the operator will have created a condition wherein the minimum flow valves must be reopened. The core damage sequence results when the operator does not reopen these valves within the time allotted in the Human Analysis Report. Furthermore, the analysis assumes that all three HPI pumps in this scenario fail simultaneously and catastrophically so that all HPI is lost. Failure of the seal barrier cooling subsequent to this event results in seal degradation and loss of inventory from the primary system. The CR–3 analysis assumes a scenario in which seal LOCAs occur when barrier cooling fails subsequent to HPI failures from other causes.

Summary. Comparison of the TMI–1 PRA results to those from the CR–3 PRA was difficult in spite of the fact that the plants are very similar in design and operation. This was due principally to the fact that the two PRAs used different methods of modeling and quantification.

Taking into account these limitations, the dominant sequences for the two plants, when external events and control building ventilation are excluded, are similar in regard to the nature of the events and the relative contributions to core damage frequency. The comparison is not as good when the conditional probabilities of core damage are compared for different initiators. For some initiators, TMI–1 is higher; for others, CR–3 is higher. Considerably more work would be required to ascertain all the reasons for the differences.

Comparison with B&W Owners' Group Evaluation

Introduction. The purpose of this review is to compare the issues raised in the B&W Owners' Group (B&WOG) evaluation of plant trip frequency and severity to the TMI–1 PRA. The B&WOG Safety and Performance Improvement Program (SPIP) investigated a large number of issues relating to B&W reactor trips and the severity of the responses to those trips. The Owners' Group report BAW–1919 contains their analysis and recommendations.[24] The NRC report NUREG–1231 contains the staff's review of this work.[25]

Analysis. The B&WOG program addressed the issues relating to the frequency of transients at B&W plants and the severity of the posttrip plant response. The program examined operating history of trips and the subsequent plant response. In addition, the program examined the root causes of these trips as well as the design criteria of the systems that could mitigate the impacts of the trips. The SPIP also produced a scale for measuring the severity of plant response to trips based on the response of key parameters such as reactivity control; reactor coolant system pressure, temperature, and inventory; and secondary system pressure and inventory.

The primary focus of the B&WOG activity was to examine ways to reduce the likelihood of complex transients such as the June 9, 1985, Davis–Besse loss of feedwater event and the December 26, 1985, Rancho Seco overcooling transient. Comparison of this effort with the PRA for TMI–1 is limited because the PRA focused on core damage rather than prevention of complex transients. However, it is reasonable to compare the types of events that were examined by the B&WOG with the PRA to determine whether or not the PRA analysis included them as part of the envelope of events for estimating core damage frequency.

Part of the SPIP examined the potential core damage risk associated with the occurrence of the more severe Category C events (i.e., events wherein one or more Abnormal Transient Operator Guideline response indicators are significantly beyond the normal posttrip response, so that nonroutine operator or safety system action is required to mitigate the transient). The analysis used event trees developed primarily from the Oconee and Crystal River PRAs, with plant specific system unavailabilities where such values were available from existing or ongoing PRA efforts. In addition, the NRC review of the SPIP work included an analysis by Brookhaven National Laboratory (BNL) of the potential risk from Category C transients.

Comparison with Category C Parameters. Comparison of the six key parameters for classifying events in the SPIP with the headings from the general transient event tree provides insight into the coverage of B&WOG issues by the PRA. The following discussion examines each of these areas and how the PRA addresses them.

Reactivity control is a key parameter in the SPIP classification of transient response. A Category C event here would be one in which recriticality occurred. The TMI-1 PRA only addresses recriticality in terms of long-term response to LOCA initiators. This is done under the heading for preventing boron precipitation in the core during long-term recirculation. The PRA does address reactivity control in transient cases by evaluation of ATWS sequences. The SPIP scope did not include ATWS events.

Reactor Coolant System (RCS) temperature control conditions leading to Category C designation by SPIP included two cases: events resulting in overcooling so that the plant's Pressurized Thermal Shock (PTS) limits are exceeded, and events where subcooling margin is lost due to overheating.

There are several headings in the PRA dealing with overcooling events. These include secondary pressure relief, excessive main feedwater, and excessive emergency feedwater. While the PRA does not examine the frequency of exceeding the PTS limits, it does include a heading for evaluating the likelihood of reactor vessel rupture from such overcooling.

Loss of subcooling margin occurs if secondary heat removal is less than heat input into the reactor coolant system. The headings from the PRA that deal with this issue include main feedwater underfeed and emergency feedwater underfeed. The PRA does not explicitly calculate the frequencies of loss of subcooling margin events. However, the occurrence of a sustained loss of main and emergency feedwater will lead to such an event.

A Category C event also occurs if RCS inventory limits are exceeded. This can occur when pressurizer level is off-scale (low) with a loss of subcooling margin, or when the PORV or safety valves open. For non-LOCA initiators, failure of the operators to start a second makeup pump and control makeup flow can lead to loss of pressurizer level. The PRA assumes that starting the second pump will occur for every transient (i.e., the probability of failure is low enough to not consider the failure specifically in the analysis). Thus, the PRA does not address this variety of Category C event. However, the PRA does have sequences where HPI has failed when required and a seal LOCA occurs. These sequences would lead to loss of pressurizer level but are not transients examined by the SPIP. The other mechanism for exceeding the inventory limits is lifting of the PORV or safeties. This can occur following a transient in two ways: to overfill the primary system due to operator failure to throttle HPI flow, or by failing to remove sufficient heat via the steam generators. This leads to heating and expansion of the primary inventory until pressure relief is needed. The PRA addresses all these cases.

Category C events also occur if the OTSG pressure exceeds ASME code limits or if pressure drops to the point where isolation of the generator occurs. The first condition could only occur if the secondary safety valves failed to open when required. The second condition could occur if any of the steam relief paths (bypass valves, atmospheric vent valves, or safety valves) remained open too long. Each of these scenarios is addressed in the PRA.

The last characteristic of plant response that can lead to a Category C event is loss of all feedwater to both OTSGs or overfeeding one or both generators beyond 95% of the operating range. The PRA accounts for this mechanism in the MF+, MF-, EF+, and EF- headings on the transient trees.

Comparison with B&WOG Risk Assessment. The SPIP examined the potential risks that Category C events pose to the B&W plants. While this effort was not a full-scale risk assessment, it did use risk assessment techniques to approximate the contribution that Category C events would be likely to make to the plants' overall risk profiles. This was based in part on completed risk assessments for Oconee and Crystal River, and on risk assessments that were in progress at other plants. In addition, NUREG-1231 included an independent review by BNL to validate the Owners' Group work.

These efforts indicate that Category C transients do not dominate the risk profile at B&W plants. The

TMI–1 PRA tends to support this assessment. There is some disagreement between the TMI–1 PRA and the B&WOG and BNL reviews with respect to overcooling events. The B&WOG and BNL reviews concluded that overcooling is not an important contributor to risk, although it would occur more frequently than the more severe undercooling events. The TMI–1 PRA indicates that they are important due to their assumption that the operator has a high likelihood of failure to establish minimum recirculation flow after throttling the HPI system following an overcooling event. This assumption is reviewed in other parts of this review report. With the exception of this difference, the major conclusions of the risk assessments as they relate to Category C events are comparable.

As noted elsewhere in this review report, the absolute value of the core damage frequency for TMI–1 is higher than in risk assessments of other B&W plants. Conservative assumptions relating to control building ventilation effects, operator error after throttling HPI, and fire effects, appear to be some of the reasons for the differences. The B&WOG and BNL reviews produced estimates of the core damage frequency from Category C events that compare favorably with the TMI–1 PRA. The B&WOG estimates the core damage frequency from Category C events to be 1.5E–5/yr, while the BNL review estimates the contribution at 1.9E–6/yr. The PRA estimates that the core damage frequency from excessive feedwater to be 1.0E–5/yr (this value is the sequence summary value for dominant contributors from Table 5–3 of the Technical Summary Report and does not represent all sequences resulting from this initiator). While this is the only transient sequence contained in Table 5–3 of the Technical Summary that is similar to the events analyzed by the B&WOG and BNL reviews, all of the TMI–1 PRA sequences from transient events that lead to core damage would (by definition) be considered as Category C events. Summing the core damage frequencies for the same transient initiators used in the B&WOG and BNL reviews (reactor/turbine trip, loss of MFW, excessive MFW, and loss of ICS power) produces a frequency of 6.4E–5/yr. As noted in the Technical Summary Report, a significant part of this value is due to the HPI throttling scenario described earlier.

Summary. The B&WOG SPIP examined many issues relating to the frequencies and severities of transients at B&W plants. The TMI–1 PRA addressed these issues in the construction of the event trees and evaluation of the sequence frequencies. Both the TMI–1 PRA and the Owners' Group (and NRC review) agree that the complex transients, as defined by the SPIP, are not the dominant contributors to the risk profiles of B&W plants. There are differences in absolute values between the TMI–1 PRA frequencies for similar sequences and the B&WOG/BNL evaluations, with the TMI–1 values being approximately four times higher. Some of the differences are because of the TMI–1 PRA assumptions relating to operator errors following overcooling events. Another section of this review report points out that review by ANL of the CR–3 PRA indicates it underestimates some sequences, which would tend to make the contingent probabilities agree better.

Comparisons with Generic and Unresolved Safety Issues

This part of the review focuses on the manner and extent to which the TMI–1 PRA modeled selected generic safety issues. The particular issues of interest are:

- Pressurized Thermal Shock
- Decay Heat Removal
- Failures of Instrument Air
- Failures of the Integrated Control System and Non Nuclear Instrumentation
- Generic Issue 23—RCP seal LOCA
- Generic Issue 65—Loss of Component Cooling Water leading directly to core damage
- Reactor Coolant Pump Seal Performance during Loss of all Cooling Conditions.

The manner in which each of these issues was handled in the PRA is discussed in the following sections. The preferred format is to establish a standard for analysis of each issue, by referencing NRC sponsored research on each subject, or by identifying other established analysis to serve as a basis for comparison. The manner in which the TMI–1 PRA evaluated each issue is then compared to the standard, differences are noted, and the quantitative impact of conservatism or deficiencies is estimated, if possible.

Pressurized Thermal Shock. Pressurized thermal shock (PTS) as evaluated in the TMI–1 PRA was compared to the work documented in NUREG/CR–3770, a PTS evaluation of Oconee Unit 1, performed by Oak Ridge National Lab for the NRC.[26] This work was chosen as a basis for comparison because Oconee and TMI–1 are both Babcock and Wilcox reactors.

Pressurized thermal shock refers to a scenario of events where a reactor vessel is cooled to low temperature and is then repressurized by the initiation of safety injection flow, thus creating the possibility that the fracture toughness of the vessel is insufficient to provide vessel integrity. PTS is possible because the ductility of a reactor vessel decreases as the temperature is reduced. Severe overcooling transients present the potential to cool the reactor vessel to the point where normally-induced pressures can induce enough stress to propagate existing weld flaws into through-wall cracks. The probability of PTS in the early years of reactor life is very small but increases significantly as neutron fluence on the reactor vessel increases with age.

Vessel rupture at a point below the core would prevent successful reflood of the core by the ECCS. The probability of core damage due to PTS is very plant specific and depends on the following:

- Frequency and severity of over cooling transients
- Copper content of weld material
- Weld location and neutron fluence accumulation
- HPI flow streams and mixing potential.

The Oconee study in NUREG/CR-3770 addressed all of these issues. The frequency of core damage due to PTS was calculated to be 2.2E-7/yr after 7 effective full power years, increasing to 4.5E-6/yr at 32 effective full power years. These frequencies do not take into consideration the effect of any neutron flux reduction programs.

The frequency of overcooling transients at Oconee was calculated to be quite high due to two specific design features at Oconee: a) there are no main steam isolation valves on the steam generators, and b) there are no feedwater isolation circuits. Isolation of steam generators in overcooling events must be accomplished by operator action. The Oconee study used very high human error probabilities for these actions, which obviously increased the core damage frequency.

TMI-1, on the other hand, is provided with MSIVs and a steam line rupture detection system (SLRDS) to isolate all FW from the SGs upon indication of overcooling. The overall Oconee frequency of 4.5E-6/yr is not directly applicable to TMI-1 by reason of these design differences. However, based on modifying the Oconee results to account for the SLRDS and the MSIVs, an estimated core damage frequency of 6E-8/yr at end of life could be expected at TMI-1. This is an estimate and does not consider the specific fracture toughness of the TMI-1 vessel versus the Oconee vessel, nor the specific weld locations or weld fluence levels of the TMI-1 vessel.

The TMI-1 PRA calculated core damage frequency due to PTS to be insignificant. A specific frequency for core damage due to PTS could not be found in the report. Questions for reactor vessel rupture due to PTS were asked on nearly all the event trees when events combined to produce overcooling conditions. Vessel failure is even asked for overpressure conditions when overcooling does not exist. However, conditional probabilities of vessel failure for TMI-1 are at least an order of magnitude less than those in the Oconee study for similar transients.

The Oconee report provides fracture mechanics calculations, specific to Oconee, which calculate conditional probabilities of vessel failure ranging from 1E-7 for excessive FW events to 5.4E-3 for steam-line breaks without feedwater isolation. The TMI-1 PRA uses B&W analysis documented in Section 19 of the TMI-1 SAR for vessel failure probabilities. The probabilities range from 2E-10 for excessive feedwater events, to 5.8E-4 for events representing stuck open secondary safeties with failure to isolate feedwater. The TMI-1 study also uses a value of 8E-17 for vessel failure under pressurized conditions when no overcooling is present (such as HPI cooling and PORVs fail to open). The TMI-1 calculations were not reviewed, so it is not possible to comment on the reasons for the differences.

In summary, the TMI-1 PRA estimates that PTS is a negligible contributor to core damage frequency. The values used for conditional probability of vessel failure upon overcooling question the sufficiency of the TMI-1 evaluation. However, based on an NRC sponsored analysis of PTS at Oconee, (NUREG/CR-3770), in no event is PTS expected to be important compared to the other contributors to core damage frequency at TMI-1.

Decay Heat Removal (Task Action Plan A-45). NUREG/CR-4713 was used as a basis to review the TMI-1 PRA treatment of decay heat removal issues. NUREG/CR-4713 is a Sandia study of Arkansas Nuclear One-Unit 1, which is a Babcock and Wilcox PWR.[27] The study was done in support of resolution of Unresolved Safety Issue A-45. The study evaluates the probability of core uncovery due to loss of decay heat removal after small break LOCAs and transients.

The study considered failures of main feedwater, auxiliary feedwater, low– and high–pressure injection recirculation systems, and pressurizer PORVs. The study finds that the core damage frequency at ANO–1, due to failure of these systems to remove decay heat, is 8.32E–5/yr. The study also identifies eight specific vulnerabilities that contribute to this core damage frequency. These are:

- Failure of the turbine driven AFW pump
- Common cause failure of valves in safety systems
- Common cause failure of pumps in safety systems
- Diesel generator faults
- Common cause battery failure
- Random failure of the RHR pumps
- Operator error to feed and bleed
- Unavailability of the Borated Water Storage Tank.

In addition, they consider loss of decay heat removal after external events such as fire, seismic, external floods, sabotage, and other events.

The total core damage frequency from the internal initiated events is 8.3E–5/yr. Due to the detail of the analysis, these results must be considered specific to the ANO–1 system configurations and the data used in the study.

The TMI–1 PRA analyzed all of the internal initiating events considered in NUREG/CR–4713. The TMI–1 PRA also analyzed the more important external events such as fires, floods, and seismic. The TMI–1 PRA analyzed all of the systems considered in NUREG/CR–4713, probably in greater detail. The presentation of results in the TMI–1 PRA is not similar to that of NUREG/CR–4713, so it is not easy to derive comparable results. However, Table 5–4 in Volume 3 of the TMI–1 PRA shows the contribution of various systems to core damage frequency. These contributions compare well with the frequencies in the A–45 study.

After reviewing the fault trees, event trees, and results, it is concluded that the TMI–1 PRA adequately incorporates all the issues and vulnerabilities identified in NUREG/CR–4713 into the TMI–1 system and sequence models. The results of the TMI–1 study may not be the same as those of the ANO–1 study, but this is to be expected. The TMI–1 study results reflect plant specific system configurations, data, and human error probabilities.

Failures of Instrument Air. Loss of instrument air at TMI–1 fails all RCP seal cooling due to closure of the injection valves on the seal injection line and closure of the valve on the ICCCW line to the thermal barrier coolers. Both of these failures are recoverable by local operator actions.

There is no established analysis for loss of instrument air which can be used as a basis for comparison with the TMI–1 analysis.

The TMI–1 PRA included loss of instrument air as an individual initiating event. The frequency of the event is stated as 1.5E–2/yr in the systems analysis chapter (Volume 4), 6.0E–3/yr in the initiating event table (Table 2–3; Volume 3) and 2.0E–3/yr in Table 6–1 of Volume 3 (mean values of split fractions). Table 6–2 of Volume 3 indicates 6.0E–3/yr was used in the final quantification. The total frequency of core damage from loss of instrument air is 2.0E–5/yr. This is relatively high compared to many other plants and results in a conditional probability of core damage upon loss of instrument air of about 3E–3. A conditional probability of core damage in this range is relatively high, and ranked higher than the value for most other transient initiators considered in this study.

Documentation of the loss of instrument air event tree is very sparse and it is difficult to understand the effect of loss of instrument air on the plant, particularly the auxiliary and main feedwater systems. The treatment of the back–up air bottles is also confusing. It is not clear which components are supplied with back–up air bottles, and which system models they were included in. It appears the EFW control valves and the secondary safeties are supplied with the same back–up air bottles, but it also appears from the dependency diagram on Page 3–51 that the air bottles were included as part of the EFW only. The EFW and event TC are modeled independently, which is not correct if they are both dependent on the air bottles.

Failures of Emergency Feedwater. As with instrument air, there is no established analysis to use as a basis for evaluation of EFW modeling.

The system model for EFW was reviewed. It appears to address all pertinent issues of EFW operability and performance. The probability for failure of all

EFW when all support systems are available is 3.8E–5. This value is on the low end of expected unavailability for a 3 train system, but appears to be reasonable when compared to other recent PRAs.

Failures of the Integrated Control System and Non–Nuclear Instrumentation. Loss of power to the ICS was evaluated as a specific initiating event. It has a frequency of 5.4E–2/yr and results in core damage frequency of 1.2E–5/yr. Approximately one third of this core damage frequency involves a stuck open PORV. A preliminary review of the event tree for loss of ICS power indicates the interactions between the ICS and the plant systems were modeled correctly.

The TMI–1 PRA did not model failures of the ICS due to individual component failure. The PRA did not model loss of power to non–nuclear instrumentation, nor did it model random failure of nonnuclear instrumentation. It is not known if failure of the power supply to the ICS umbrellas all other failures of ICS and NNI. However, the initiating event frequency for loss of ICS power, and the core damage frequency due to this event, are relatively high compared to other plants.

EG&G Idaho examined the effects of loss of Class 1E or non–Class 1E bus power to ICS and NNI as part of an audit of TMI–1 compliance with NRC Bulletin 79–27. The licensee has reviewed the ICS/NNI power buses and other plant buses and made hardware and procedural changes as a result. Based on these changes, the draft audit report gave reasonable assurance that the failure of any single Class 1E or non–Class 1E bus that supplies power to plant instrumentation and control circuits will not result in a plant condition requiring operator action and the simultaneous loss of the control room indication (on which the required action is based).[a] There is also reasonable assurance that a safe (cold) shutdown condition can be achieved by using existing procedures following the loss of power to any single Class 1E or non–Class 1E bus that supplies power to plant instrumentation and control circuits.

Generic Issue 23. Generic Issue 23 addresses the possibility of reactor coolant pump seal failure as a small break and thus as a contributor to core damage.

a. Alan C. Udy and Harry Reilly, personal communication, November 1988.

This issue is different from Generic Issue 65, which involves loss of cooling water systems leading to simultaneous RCP seal failures and failure of ECCS.

TMI–1 has Westinghouse reactor coolant pumps. Complete seal failure in one pump will result in a leak rate of about 500 gpm. This is put into the very small break category of initiating events. The very small break IE category in the TMI–1 PRA has a frequency of 5.1E–3/yr. The recently published NUREG/CR–4550, Rev. 1, Vol. 3, calculates a random seal failure probability in PWRs of 3.9E–3/yr, based on historical experience.[28] The TMI–1 frequency for very small breaks appears to include this contributor.

The model used for reactor coolant pump seal failure upon loss of all seal cooling is discussed later in this section.

Generic Issue 65. This generic issue involves failure of cooling water systems which can lead directly to core damage by causing an RCP seal LOCA (due to loss of cooling) and simultaneously failure of all ECCS (due to loss of component cooling).

TMI has Westinghouse reactor coolant pumps. Cooling to the thermal barrier is provided by the Intermediate Closed Cycle Cooling Water System. Seal injection flow is provided by the charging pumps, which can be cooled by the Decay Heat Closed Cycle Cooling System or the Nuclear Services Closed Cycle Cooling System. These closed cycle cooling water systems in turn are cooled by other cooling water systems. The dependencies are as follows[b]:

	Seal Injection Flow	
RCP Thermal Barrier Cooling	Chg Pump 1A/1C	Chg Pump 1B
ICCCW	Decay Heat CCW	Nuc. Serv. CCW
NSRW	Decay Heat RW	Nuc. Serv. RW
River Water (RW)	RW	RW
(Inst. Air)	(Inst. Air)	(Inst. Air)

b. These dependencies are from Page 3–50 of Volume 3. Instrument Air was included in this exercise because it can fail all seal cooling and has dependencies on cooling water systems.

Candidate Systems for Issue 65 are the following:

Loss	Fail Therm Barrier	Fail Seal Inj Flow	RCP Seal Vulnerable	Fail HPI Flow	Issue 65 Candidate
ICCCW	Yes	No	No	No	—
NSRW	Yes	No	No	No	—
DHCCCW	No	Yes	No	No	—
DHR	No	Yes	No	No	—
RW	Yes	Yes	Yes	Yes	Yes
Inst Air	Yes	Yes	Yes	No	—

This table indicates the only system failure that can lead directly to core damage via seal failure and HPI failure is the River Water System.

Loss of River Water was included as an individual initiating event with a frequency of 7.4E–3/yr including a factor of 0.17 for non–recovery (cleaning of intake screens) within 4 hours. A check of the results in Table 6–5 of Volume 3, shows core damage Sequences 8 and 9 are Loss of River Water with failure to recover in the appropriate time period. Sequence 8 has the additional failure of EFW, and thus has a shorter recovery time, while Sequence 9 is just the initiator and non–recovery. The frequencies of these sequences are 3.9E–6/yr and 3.5E–6/yr, respectively.

It appears that the TMI–1 PRA has adequately modeled and addressed the issues raised by Generic Issue 65. However, it is not clear that an acceptable seal LOCA model was used in this analysis. The choice of seal LOCA model determines the time of seal failure and the leak rate. The leak rate in turn determines the amount of time for system recovery before core uncovery occurs. The amount of time for recovery in turn determines the probability of non–recovery, and thus influences core damage frequency.

In the loss of river water sequence, the recovery factor for the case where EFW is available is 9.3E–4. This presumes a mean recovery time of 10–12 hours. This value is clearly optimistic in light of current seal LOCA analysis performed by NRC for the NUREG–1150 program. If an alternate seal LOCA model with a smaller recovery time were used, the impact on core damage frequency could be significant.

In summary, it appears issues related to Generic Issue 65 have been included in the TMI–1 PRA. However, the seal LOCA model used to determine recovery times, and thus determine recovery probabilities, appears to be optimistic compared to recent NRC work on this issue. Use of an alternative seal LOCA model could have a significant affect on the frequency of some sequences. The seal LOCA model is discussed in the next section.

Reactor Coolant Pump Seal Model. TMI–1 is supplied with Westinghouse Reactor Coolant pumps. These pumps have a three stage seal assembly which uses a film riding controlled leakage stage and two rubbing face seals. Sealing is provided by seal injection flow with controlled leak off between stages. In the event that seal injection flow is lost, back leakage through the seals will amount to about 20 gpm per pump. This has been determined by analysis (NUREG/CR–4294) and verified in tests.[29] In the event that seal injection flow is lost, CCW to the thermal barrier heat exchanger can provide seal cooling. As back leakage flows over the thermal barrier heat exchanger, it is cooled, and thus cooled water flows through the seals.

In the event that both seal injection flow and CCW to the thermal barrier are lost, the seals will gradually heat up and are subject to failure. Maximum leak rates under the worst failure conditions can be 450 gpm. The actual timing of seal failure, and the expected leak rate, have been the subject of much disagreement within the last four years. The Westinghouse research documented in WCAP–10541, Revision 2 provides one perspective, but this document is proprietary and as such was not available to EG&G for review (although it is available to the NRC). Another seal LOCA model has been developed by the NRC in support of the NUREG–1150 program.[30] It predicts seal failure may occur between 90 minutes and 150 minutes after loss of all cooling. The total probability of seal failure is 0.73. Average leak rate is about 250 gpm per pump. The estimated time to core uncovery is about 3.5 hours after loss of all seal cooling (see Appendix B).

The seal LOCA model used in the TMI–1 PRA was documented only as a note to the Event Sequence Diagram for the Loss of River Water event tree. The seal leak rate was assumed to be 20 gpm per pump for the first ten hours and 300 gpm per pump after that. This implies seal success (i.e., the seals retain their integrity) for 10 hours, and then a large seal failure. An adjunct assumption to this model is that if seal injection flow is restored any time up to 10 hours, all seal leakage will stop. This model is much more optimistic then the referenced NRC model. Substitution of the NRC model in the TMI-1 PRA would be expected to significantly reduce allowable recovery times and cause a noticeable increase in core damage frequency.

Component Failure Data

Introduction. This section provides a review of the data used in the TMI-1 PRA, as provided in the Data Analysis Report (Volume 5). The Data Analysis Report presents four general areas of data-related information, including: (1) component failure rates, (2) common cause failure (CCF) parameters, (3) component maintenance frequency and duration, and (4) initiating event frequencies. The first two of these areas will be considered in this section. The other two areas are considered elsewhere in this review report. An overall evaluation of the data analysis approach as described in Section 2 of the Data Analysis Report will be provided first.

The data evaluated here is limited to data considered in the Data Analysis Report of the PRA. Certain other types of data, such as human error rates, are evaluated elsewhere in this report consistent with their use in specific applications in the PRA.

Data Analysis Approach. The data analysis approach used in the TMI-1 PRA, as described in Section 2 of the Data Analysis Report (Volume 5), involved the following principal elements:

a. The Bayesian update method was used to combine generic and plant specific data

b. Lognormal distributions were assumed for failure rates

c. Mean values were used

d. The Multiple Greek Letter method was used for common cause failure

e. A PLG proprietary data base was used as the principal source of generic data in establishing failure rates.

Elements (a) and (b) above are generally standard assumptions made in PRAs and are considered acceptable.

Element (c) is also considered acceptable, since the use of mean values is now generally standard practice in PRAs (some early PRAs were criticized for using median values). In discussing the use of mean values, the Data Analysis Report indicates on Page 2-21 that "recommended" values from the IEEE data base [31] were interpreted to be median values. This interpretation was employed because (1) estimators probably had in mind median values when estimating recommended values, and (2) this interpretation would produce conservative results, since mean values used in the PRA would be higher than the recommended (assumed to be median) values from the IEEE data base. Since details regarding the use and weighting of the IEEE data are not provided in the PRA, the extent of this conservatism could not be established. However, it would be expected to be less than a factor of two in terms of overall core damage frequency, since mean values are typically less than a factor of two greater than medians for data employed in PRAs.

Element (d) is considered adequate, because the Multiple Greek Letter method is an accepted method (see Reference 32 for discussion) for estimating common cause failures. This method is an extension of the simpler beta-factor model. The two models are equivalent when estimating CCFs among two components.

Element (e) could not readily be evaluated, since details of the TMI-1 PRA data base development are based on proprietary PLG documentation which was not made available for this review. Instead, the component failure rates and common cause model parameters contained in this database, as reported in the TMI-1 PRA, were compared with data from other sources to determine if any significant deviations existed. These comparisons are provided in the following sections.

Component Failure Rates. The component failure rates used in the TMI-1 PRA are presented in Section 3 of Volume 5 (Data Analysis Report). These failure rates were described (Page 3-7) as having been developed by combining generic distributions (obtained primarily from the proprietary PLG database) and TMI-1 plant-specific failure data. Since the PLG database is proprietary, it was not provided for review. Thus, the review consisted primarily of comparing the PRA component failure rates with comparable failure rates from other sources which have been developed for, and used in, various PRAs for nuclear power plants. The significance of any deviations was estimated by examining the impact the failure rate would have on system failure probabilities, accounting for the relative influence of the specific system failures on core damage frequency.

Table 9 illustrates the results of the comparison described in the preceding discussion. The first column provides the component description, and the second column the failure mode. The third column provides the failure data from the TMI–1 PRA, and the final three columns provide comparative data from other sources. The failure rates are all mean values; the operational failure rates, except as noted, are per hour. The "RANGE" column gives the range of values as provided in Reference 21. This range is stated to be from past PRA and safety studies. The ASEP column refers to the values derived in the NRC's Accident Sequence Evaluation Program, and was developed from a variety of data sources. These data were used in the recent NRC effort to estimate risks from a group of nuclear power plants.[33] The last column lists data from a recent PRA which employed an independent database developed by Westinghouse Electric Corporation. This PRA has been reviewed by NRC contractors.[34]

The data values in Table 9 were examined to identify any large differences between the TMI–1 PRA data and the other sources. Table 10 lists the major differences. The criteria used to identify a major difference was a factor of about 5 or greater between the TMI–1 data and other sources.

The failure rate differences in Table 10 were examined to determine if further evaluation of the data would be appropriate. The examination consisted of a qualitative evaluation, based primarily on how the failure rates might affect the systems and components which were found in the TMI–1 PRA to be significant contributors to risk. On this basis, none of the failure rate differences in Table 10 appear to be significant enough to influence appropriate system failure rates to an extent that would result in significant change to the core damage frequency as it is currently estimated in the TMI–1 PRA. For those TMI–1 PRA failures rates for which no comparative value was found, all important rates appear to be reasonable.

Common Cause Failure Rates. As noted above, the TMI–1 PRA employs the multiple Greek letter CCF model. This model uses two parameters, a beta-factor and a gamma–factor, to quantify common cause contributions. The beta–factor is defined as the probability that the cause of a component failure will be shared by one or more additional components. The beta–factor is the dominating parameter in estimating CCFs for the cases of interest, and it is the only factor used when only two components are involved, which occurs frequently in system analysis for nuclear power plants. The gamma factor is defined as the conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more components in addition to the first. For a three train system, it can be shown that for a typical gamma–factor of 0.5 (most of the TMI–1 PRA gamma factors are 0.5), the system failure probability would be increased by only 25% over the estimated failure rate using only the beta–factor analysis.[32] Furthermore, gamma factors for comparison to the TMI–1 PRA values could not be found in existing PRA literature. For these reasons, this evaluation will be limited to an evaluation of the beta–factors used in the TMI–1 PRA.

In order to evaluate the numerical values of the beta–factors used in the TMI–1 PRA, a comparison with other sources of beta–factors for nuclear power plants was used. These sources included a previous PRA for a PWR,[7] a report which includes generic beta–factors from the Electric Power Research Institute Institute,[32] a recent NRC sponsored effort in which beta–factors are recommended,[33] and one additional source for diesel generators.[35] It should be noted that the purpose of the comparison is not to imply that the TMI–1 PRA values are suspect if they don't compare well with the others, but rather to identify any large differences between them and evaluate further the significance of these differences. Details of the development of the TMI–1 beta–factors could not be reviewed because the database used for the derivation is proprietary.

The beta–factor comparison is provided in Table 11. From the comparison, the following conclusions and implications can be drawn:

Ventilation Fans Fail to Start or Operate. The TMI–1 beta–factor for ventilation fans (.05) is significantly lower than the value (.13) in NUREG/CR–4780. This implies that systems with multiple ventilation fans would be estimated in the TMI–1 PRA to have a lower failure probability than would be the case using the NUREG/CR–4780 value.

According to volume 2, Table 5–4 of the TMI–1 PRA, failure of the control building ventilation system is the most dominant system contributing to core melt (43%). Further, Table 5–4a (Volume 2) of the PRA estimates that CCF of the ventilation fans contributes about 19% to the initiating event of interest (loss of

Table 9. Comparison of component failure rates

		Rate			
			NUREG/CR-4550(3)		
Component Description	Failure Mode	TMI-1	Range	ASEP	MP-3(4)
Air Compressor	Failure during operation	8.10–5			
Air Compressor	Failure to start on demand	3.29–3			
Air Dryer—Compressed Air System	Failure during operation	1.66–7			
Air Filter (ventilation)	Failure during operation	5.83–6			
Air Filter (oil removal)	Failure during operation	1.76–5			
Air Filter (compressed air system)	Failure during operation	3.54–5			
Battery Charger	Failure during operation	1.63–5		1.3E–7	
Bistable	Failure to operate on demand	4.40–5			1.6–6 to 2.4–6
Battery (125 V dc)	Failure of output on demand	1.29–5			
125 V dc Battery	Failure of output on demand	4.84–4			
Electrical Bus	Failure during operation	4.98–7			1.5–6 [a]
Circuit Breaker (ac 480 V and above)	Failure to close on demand	1.61–3			
Circuit Breaker (ac 480 V and above)	Failure to open on demand	6.49–4			
Circuit Breaker (ac 480 V and above)	Transfers open during operation	8.28–7			
Circuit Breaker (ac 480 V and above)	Failure to close on demand	2.27–4			
Circuit Breaker (ac of dc, LT. 480 V)	Transfers open during operation	2.68–7			
Circuit Breaker (reactor trip)	Failure to open on demand	2.50–3			3.4E–4
Single Control Rod Assembly	Failure on demand	3.11–5			
Cavitating Venturi	Failure during operation	2.66–6			
Diesel Generator	Failure to start on demand	1.58–2	8.0–3 to 1.0–1	3.0–2	
Diesel Generator	Failure during first hour of operation	6.58–3	2.0–4 to 3.0–3	2.0–3[b]	
Diesel Generator	Failure after first hour of operation	2.50–3	2.0–4 to 3.0–3	2.0–3[b]	
Pneumatic Damper	Failure to operate on demand	1.52–3			
Pneumatic Damper	Transfers open/closed during operation	2.67–7			
Fire Damper	Inadvertent actuation	4.20–8			
Gravity Damper	Failure to operate on demand	1.52–3			
EFW Valve Control Circuit	Failure on demand	2.41–4			
EFW Enable	Failure during operation	4.54–5			
EFW Actuation Circuit	Failure on demand	2.41–4			
EFW Level Switch	Failure during operation	5.69–6			
EFW Signal Isolater	Failure during operation	8.75–6			

Table 9. (continued)

		Rate			
			NUREG/CR–4550(3)		
Component Description	Failure Mode	TMI–1	Range	ASEP	MP–3(4)
EFW Actuation/Control Signal	Failure during operation	2.07–5			
Expansion Joint	Failure during operation	1.64–6			
Feedwater Hand/Auto Station	Failure to switch to manual control(#)	8.07–4			
Feedwater Hand/Auto Station	Failure during operation	1.30–5			
River Water Screen	Plugs during operation	4.51–2			
Flow Transmitter	Failure during operation	6.25–6			3.9–5
ICS Feedwater Module	Failure during operation	1.30–4			
Fuse	Failure during operation	9.20–7			4.4–7
Ventilation Fan	Failure during operation	3.63–5			
Ventilation Fan	Failure to start on demand	2.94–3			
Heat Exchanger	Plugs during operation	7.49–7			
Heat Exchanger	Leaks/ruptures during operation	7.49–7			
ICS Integrated Master Module	Failure during operation	5.21–5			
Inverter	Failure during operation	1.83–5	1.0–4 to 1.0–6	1.0–4	
Steam Generator Water Level Controller	Failure during operation	2.66–5			
ESAS Load Sequencer	Failure to operate on demand	2.40–6			
Limit Switch	Failure to operate on demand	4.28–4			1.0–4
Level Transmitter	Failure during operation	1.57–5			4.3–5
Manual Loader	Failure during operation	2.66–5			
Reactor Building Spray Nozzles	Plugs during operation	7.06–8			
Offsite Grid	Failure on demand, given plant trip	2.66–4			
Pushbutton Switch	Failure to operate on demand	2.40–5			4.0–7
Piping, GE, 3–inch Diameter	Failure per section	8.60–10			
Piping (3–inch Diameter)	Failure per section per hour	8.60–9			
Power Supply Failure	Failure during operation	1.71–5			
Pressure Switch	Failure to operate on demand	2.69–4			
Pressure Transmitter	Failure during operation	1.57–5			6.5–5
Normally Operating Motor–Driven Pump	Failure to start on demand	3.49–3			
Normally Operating Motor–Driven Pump	Failure during operation	6.69–6			
Standby Motor–Driven Pump	Failure to start on demand	1.83–3	5.0–4 to 1.0–2	3.0–3	
Standby Motor–Driven Pump	Failure during operation	4.48–5	1.0–6 to 1.0–3	3.0–5	

Table 9. (continued)

		Rate			
			NUREG/CR-4550(3)		
Component Description	Failure Mode	TMI-1	Range	ASEP	MP-3(4)
Turbine-Driven Emergency Feed Pump	Failure to start on demand	3.31-2	5.0-3 to 9.0-2	3.0-2	
Turbine-Driven Emergency Feed Pump	Failure to run	9.30-4	8.0-6 to 1.0-3	5.0-3	
Turbine-Driven Main Feed Pump	Failure to start	2.23-2	5.0-4 to 9.0-2	3.0-2	
Turbine-Driven Main Feed Pump	Failure during operation	6.90-5	8.0-6 to 1.0-2	5.0-3	
Normally Operating River Water Pump	Failure to start	3.05-3			
Normally Operating River Water Pump	Failure during operation	3.02-5			
Standby River Water Pump	Failure to start	4.11-3			
Standby River Water Pump	Failure during operation	4.41-5			
Vacuum Pump	Failure to start	2.35-3			
Vacuum Pump	Failure to run	3.36-5			
Relay	Failure to operate on demand	2.41-4			4.0E-6
Relay	Failure during operation	4.20-7			2.7-8 to 1.2-7
Reactor Sump	Clogs/fails during operation	1.00-5			
Service Water Strainer	Failure during operation	3.23-6			1.0E-5
Seal Injection Line Filter	Plugging during operation	3.23-6			
Signal Modifier	Failure during operation	2.94-6			
Shunt Trip Coil	Failure to operate on demand	1.40-4			
Timing Circuit	Failure to operate on demand	2.40-6			
Time Delay Relay	Failure to operate on demand	2.41-4			
Temperature Element	Failure during operation	7.50-7			
Turbine Exhaust Boot	Failure during operation	2.66-6			
Temperature Monitor Loop	No output	3.41-6			
Tank	Rupture during operation	2.45-8			8.0-10
ICS Unit Load Demand Module	Failure during operation	1.43-4			
Ventilation Chiller	Failure to start on demand	1.11-2			
Ventilation Chiller	Failure during operation	4.86-5			
Motor-Operated Valve	Failure to operate on demand	3.51-3	1.0-3 to 9.0-3	3.0-3	
Motor-Operated Valve	Transfers open/closed during operation	9.27-8			2.2-6 to 4.6-6
Solenoid Valve	Failure to operate on demand	2.43-3	3.0-4 to 2.0-2	1.0-3	
Solenoid Valve	Transfers open/closed during operation	4.95-7			
Air-Operated Valve	Failure to operate on demand	2.16-3	3.0-4 to 1.0-3	1.0-3	

Table 9. (continued)

		Rate			
			NUREG/CR-4550(3)		
Component Description	Failure Mode	TMI-1	Range	ASEP	MP-3(4)
Air-Operated Valve	Failure to modulate to control pressure	1.62-2			1.4-6 to 4.3-6
Air-Operated Valve	Transfers open/closed during operation	3.24-6			1.4-6 to 4.3-6
Air-Operated Valve	Transfers open/closed during operation	2.62-7			
Air-Operated Valve	Failure to transfer to failed position	2.66-4			
Electrohydraulic Valve	Failure to operate on demand	1.57-3			
Electrohydraulic Valve	Transfers open/closed during operation	2.67-7			
Stop Check Valve	Failure to operate on demand	9.13-4			
Stop Check Valve	Transfers open/closed during operation	1.04-8			
Check Valve (other than stop)	Failure to operate on demand	2.11-4	1.0-4 to 6.0-3	1.0-4	
Check Valve (intermediate cooling)	Failure to operate on demand	5.09-4			
Check Valve (river water)	Failure to operate on demand	2.08-3			
Check Valve (other than stop)	Gross reverse leakage during operation	9.78-7			
Check Valve (intermediate cooling)	Gross reverse leakage during operation	1.81-4			
Check Valve (river water)	Gross reverse leakage during operation	1.06-6			
Check Valve	Gross reverse leakage during operation	7.24-5			
Check Valve (other than stop)	Transfers closed; plugs during operation	1.03-8			
Check Valve (intermediate cooling)	Transfers closed; plugs during operation	1.04-8			
Check Valve (river water)	Transfers closed; plugs during operation	1.04-8			
Manual Valve	Failure to open on demand	7.40-4			
Manual Valve	Transfers open/closed during operation	2.14-8			4.9-7 to 2.2-6
Relief Valve (other than PORV or safety)	Failure to operate on demand	2.42-5			
Relief Valve (other than PORV or safety)	Premature open	6.06-6			
Pressurizer Safety Valve	Failure to open on demand (passing steam)	2.92-4			
Pressurizer Safety Valve	Failure to open on demand (passing water)	2.92-4			
Pressurizer Safety Valve	Failure to reseat on demand (passing steam)	1.53-3			3.0E-3[c]
Pressurizer Safety Valve	Failure to reseat on demand (passing water)	1.01-1			
Pressurizer Safety Valve	Transfers open/closed	3.03-6			1.9-6
PORV	Failure to open on demand (passing steam	4.10-3		1.0-5	
PORV	Failure to open on demand (passing water)	4.10-3		1.0-5	
PORV	Failure to open/reseat on demand (passing steam)	2.05-2	1.0-1 to 3.0-3	3.0-2	
PORV	Failure to reseat on demand (passing water)	1.01-1			

Table 9. (continued)

		Rate			
			NUREG/CR-4550(3)		
Component Description	Failure Mode	TMI-1	Range	ASEP	MP-3(4)
PORV	Transfer closed during operation	3.03-6			
Turbine Stop/Control Valve	Failure to operate on demand	1.25-4			
Pressure Control Regulating Valve	Transfer closed during operation	1.69-5			
Air Compressor Transfer Valve	Failure to operate on demand	1.52-3			
Y-Type Strainer	Failure during operation	2.66-6			
Transformer (GST/UAT/RAT)	Failure during operation	1.26-6			2.8-6[d]
Transformer (station service/480 V to 4,160 V)	Failure during operation	4.28-7			2.8-6[d]
Transformer (instrument/120 V to 480 V)	Failure during operation	1.55-6			2.8-6[d]

a. Transfers open.

b. Time not specified.

c. Phase of water being passed not specified, assumed to be steam.

d. Type and size specified.

Table 10. Major differences between TMI–1 data and other data sources

Component	Failure Mode	TMI–1	Other (Source)
1. Air Operated Valve	Transfers open/closed during operation	2.62E–7	5.7E–6 (MP–3)
2. Manual Valve	Transfer open/closed during operation	2.14E–8	2.7E–6 (MP–3)
3. PORV	Fails to open on demand	4.1E–3	1.0E–5 (NUREG/CR–4550)
4. Pushbutton Switch	Fails to operate on demand	2.4E–5	4.0E–7 (MP–3)
5. Turbine Trip (MF)	Fails during operation	6.9E–5	5.0E–3 (NUREG/CR–4550)
6. Relay	Fails to operate on demand	2.41E–4	4.0E–6 (MP–3)
7. Temperature Element	Fails during operation	7.5E–7	8.3E–6 (MP–3)
8. Tank	Rupture during operation	2.45E–8	8.0E–10 (MP–3)
9. Motor Operated Valve	Transfer open/closed during operation	9.27E–8	6.8E–6 (MP–3)
10. Battery Charger	Fails during operation	1.63E–5	1.3E–7 (NUREG/CR–4550)
11. Battery	Failure on demand	1.29E–5	4.0E–4 (NUREG/CR–4550)
12. Circuit Breaker (reactor trip)	Fails to open	2.5E–3	3.4E–4 (MP–3)
13. Heat Exchanger	Plugs	7.49E–7	5.7E–6 (NUREG/CR–4550)

Table 11. Comparison of beta-factors

		Source[a]				
Component	Failure Mode	TMI-1 PRA	NUREG/ CR-4780	Seabrook PRA	NUREG/ CR-2099	NUREG/ CR-4550
Air compressor	Fails during operation	0.05	—	—	—	—
Air compressor	Fails to start on demand	0.01	—	—	—	—
Bistable	Fails to operate on demand	0.05	—	—	—	—
Circuit breaker	Fails to open on demand	0.185	0.19	0.111	—	0.08
Diesel generator	Fails to start on demand	0.049	0.05	0.015	0.08	0.02
Diesel generator	Fails during first hour of operation	0.041	0.05	0.033[b]	—	—
Diesel generator	Fails after first hour of operation	0.041	0.05	—	—	—
Pneumatic damper	Fails to operate on demand	0.10	—	—	—	—
Ventilation fan	Fails to operate on demand	0.05	0.13	—	—	—
Ventilation fan	Fails to start on demand	0.05	0.13	—	—	—
Heat exchanger	Plugs during operation	0.05	—	—	—	—
Pump—motor driven, normally driven	Fails to start on demand	0.056	0.025 to 0.076	—	—	—
Pump—motor driven, normally operating	Fails during operation	0.014	—	—	—	—
Pump—motor driven, standby	Fails to start on demand	0.162	0.03 to 0.17[c]	0.067 to 0.125	—	0.01 0.07[d]
Pump—motor driven, standby	Fails during operation	0.034	0.03 to 17[c]	0.118	—	—
Pump—turbine driven	Fails to start on demand	0.024	—	—	—	—
Pump—turbine driven	Fails during operation	0.032	—	0.118	—	—
Pump—river water, normally operating	Fails to start on demand	0.056	—	—	—	—
Pump—river water, normally operating	Fails during operation	0.014	—	—	—	—
Pump—river water, standby	Fails to start on demand	0.056	—	—	—	—
Pump—river water, standby	Fails during operation	0.014	—	—	—	—
Emergency FW pump	Fails to start on demand	0.026	0.03	—	—	0.01
Emergency FW pump	Fails during operation	0.034	0.03	0.118	—	—
Relay	Fails to operate on demand	0.10	—	—	—	—
Service water strainer	Fails during operation	0.10	—	—	—	—
Time delay relay	Fails to operate on demand	0.05	—	—	—	—
Ventilation chiller	Fails to start on demand	0.05	0.11	—	—	—
Ventilation chiller	Fails during operation	0.10	0.11	—	—	—
Motor operated valve	Fails to operate on demand	0.081	0.08	0.042	—	0.03
Stop check valve	Fails to operate on demand	0.10	0.06	—	—	—
Relief valve (not PORV or safety)	Fails to open on demand	0.10	0.07	—	—	0.03
Pressurizer safety valve	Fails to open on demand (steam)	0.05	0.07	—	—	0.03
Pressurizer safety valve	Fails to open on demand (water)	0.05	0.07	—	—	—
Pressurizer safety valve	Fails to reseat on demand (steam)	0.05	—	—	—	—
Pressurizer safety valve	Fails to reseat on demand (water)	0.05	—	—	—	—

a. See references for details.

b. Time not specified.

c. Range for various pumps; RHR = 0.11, containment spray = 0.05, service water = 0.03, safety injection = 0.17, auxiliary feedwater = 0.03.

d. Range for various pumps; RHR = 0.05, containment spray = 0.02, service water = 0.01, safety injection = 0.07.

control building ventilation). On this basis, the core damage frequency from loss of control building ventilation would be about 30% greater if the NUREG/CR-4780 beta-factors were used. However, this would only raise the overall core damage frequency by 10%, not a large change. Also, (see Initiating Events and Assumptions Sections) the core damage sequences which involve containment building ventilation do not appear valid since loss of this system would most likely not lead to core damage. Therefore this change in beta-factor would no longer be important.

Standby Motor Driven Pumps Fail to Start. The TMI-1 beta-factor for this component (.162) is somewhat higher than the range (.01-.07) given in NUREG/CR-4780 for motor driven pumps. In examining the dominant system contributions, it appears this failure mechanism would have only a small effect (a few percent) on the core damage frequency, with the TMI-1 result being slightly higher than that which would be obtained by using the lower beta-factors.

Turbine Driven Pumps Fail During Operation. The Seabrook PRA beta-factor for turbine driven pumps (.118) is higher than the TMI-1 value (.0317). However, CCF of turbine driven pumps does not appear significant at TMI-1 based on the discussion in Section 5 of the PRA report.

Ventilation Chillers Fail to Start. The NUREG/CR-4780 beta-factor for this component (.11) is higher than the TMI-1 value (.05). However, this difference does not appear significant based on dominant system failures and their operating modes from Section 5 of the PRA report.

For those TMI-1 beta factors in Table 11 for which values were not given in the sources used for comparison, none appear to be unusual or questionable. All are within the range of beta factors given in the sources used for comparison, although this range is quite large (0.01 to 0.10).

Human Factors

Introduction. Review of the Three Mile Island Unit 1 (TMI-1) Probabilistic Risk Assessment (PRA) Human Response Analysis (HRA) concentrated on four major objectives:

- To assess whether the errors analyzed in the HRA are a reasonably complete set
- To assess whether the quantification of the human errors is credible and well-supported in the PRA
- To assess whether the treatment of post-accident recovery is proper
- To survey the methods used by the PRA and characterize them by comparison to standard methods.

Each of these objectives is addressed separately below. The scope of this review was not such as to allow revision to the HRA performed in the PRA, other than one major human error probability discussed under the topic of credibility of the quantification of human errors.

Human Error Identification and Completeness. There are two steps in common use to identify which human errors to include in the quantification of a PRA. The first step is to determine which human errors to include in the initial screening. The second step is to perform a coarse screening to determine which human errors to examine in more detail, and to quantify them.

The identification of human errors to include in the initial screen is usually based on engineering judgement, plant history, and literature reviews, as was done in the TMI-1 PRA. However, the engineering judgement is usually performed in some clearly systematic fashion. The system underlying these judgements is relatively inscrutable in the TMI-1 PRA.

In addition, several types of human error were specifically excluded. For example, errors of omission for those actions not covered by procedures or written instructions (an important category, according to industry experience) were excluded. Errors due to failures of indicators in the control room during some sequences were not believed to be within the capabilities of human response analysis at the present time.

Initial (Coarse) Screening Techniques. Initial screening of human errors was performed by deriving values from NUREG/CR-1278 and by obtaining consensual judgement on "realistic to conservative" probabilities.[36] Then the contribution of the human errors so quantified to overall risk was evaluated by some unstated rule. The PRA only states (page 2-2, Human Action Analysis) that the human errors "identified in the initial quantification rounds as being important" were retained for detailed evaluation.

Credibility and Supportability of Human Error Quantification. Eleven of the most important human actions were investigated in detail. One human action value that was very important in the PRA was questioned. For HSR–3 (failure to switch to sump recirculation following a medium LOCA), the value that was used was the value HSR–1 (failure following a large LOCA).

Treatment of Post Accident Recovery. With human actions, there are two types of recovery to consider. There is the recovery of mistakes or misdiagnoses on the part of the operators, and there is recovery of systems or components. The review looked at both types.

Recovery of Mistakes or Misdiagnoses. The PRA states "it is assumed that all such initial misdiagnoses are eventually successful and the accident sequence correctly rediagnosed." Since the Human Cognitive Reliability (HCR) model is being used, there is no such assumption.[37] Both the HCR and the Time–Reliability Correlation (TRC) models account for correct rediagnosis in the models and in the benchmarking of the models, so that recovery from misdiagnoses is not an issue.[38] The THERP model presents explicit methods for analyzing the probability of recovery from an error.[36]

Recovery of Systems or Components. The adequacy of the treatment of these post–accident recoveries are addressed elsewhere in this review. From the Human Reliability Analysis point of view, these recoveries are handled properly, if conservatively.

Survey of Methods Used. The methods that were used in this PRA included: 1) Technique for Human Error Rate Prediction (THERP), 2) Human Cognitive Reliability (HCR), 3) Operator Action Tree System (OATS), and 4) Confusion Matrix method.[39]

Summary. Major strengths of the HRA of this PRA include the full documentation of the human actions that were analyzed—allowing requantification of questionable values—and the detail of discussion of the actions analyzed. Weaknesses include the inscrutability of the initial screening process. No major errors were found.

Uncertainty Analysis

Uncertainties in a probabilistic risk assessment (PRA) are often grouped into three classes: completeness, data, and modeling. The Three Mile Island Unit 1 (TMI–1) PRA has attempted to minimize completeness uncertainties by using proven methodologies and experienced PRA practitioners. This attempt appears to be successful, based on the conclusions of the other sections of this review report.

Data uncertainties involve the uncertainties in initiating event frequencies, component failure rates, and human error rates. Modeling uncertainties involve questions such as success criteria for systems. Two typical methodologies for handling these two types of uncertainties are outlined below:

1. Evaluate data uncertainty effects on core damage frequency by a formal uncertainty analysis using a Monte Carlo or discrete probability distribution method. Then evaluate the effects of modeling uncertainties by performing sensitivity analyses
2. Evaluate both data and modeling uncertainties in a combined formal uncertainty analysis. (Various modeling assumptions are given weights in such analyses).

The TMI–1 PRA used the first methodology. However, no sensitivity analyses were performed. The TMI–1 uncertainty analysis should be considered incomplete to the extent that it did not incorporate or investigate modeling uncertainties.

The PRA estimated a mean core damage frequency of 5.5E–4/yr, with a 95th percentile of 9.4E–4/yr and a 5th percentile of 2.6E–4/yr (Table 12). The range factor, based on the 95th percentile and median, is 2.1. As discussed previously, this distribution does not account for modeling uncertainties. Also, some of the data uncertainties may be underestimated. Examples include the uncertainties in internal fire frequencies and some of the transient initiator frequencies.

Table 12. TMI–1 core damage frequency distribution

Percentile	Core Damage Frequency Per Year
5th	2.6E–4
50th (median)	4.5E–4
Mean	5.5E–4
95th	9.4E–4

Compared to estimates for other reactors, the above range of uncertainty (less than a factor of four) is small. For example, in the recently completed revision of NUREG/CR–4550 for the Surry plant, the range of uncertainty for core damage frequency caused by internal events is more than 20: from 6.7E–6/yr to 1.4E–4/yr.[40] And in a review by ANL of the updated PRA for CR–3,[22] a similar plant, the estimated range of uncertainty is a factor of ten: from 2.5E–5 to 2.5E–4/yr. The authors of that report emphasize that the estimate includes only uncertainties in the database used in the review. And the CR–3 PRA addressed only internally initiated events, whereas the TMI–1 PRA includes external events.

In the TMI–1 PRA, all external events apart from in–plant fires are estimated to have very small contributions to the CDF. This review indicates that core damage sequences initiated by in–plant fires are among the dominant sequences in the TMI–1 PRA. Also this review indicates that river flooding may be a dominant initiator, with a large uncertainty. If an event is a large contributor to mean CDF, it will normally be a large contributor to the overall range of uncertainty in CDF. The uncertainty in overall CDF will increase if sequences having large uncertainties become dominant.

We concluded that the uncertainty range quoted in the TMI–1 PRA is unrealistically small, even for core damage sequences initiated by internal events. Also, the uncertainty range may increase greatly if river–flooding becomes a dominant initiator, because of the large uncertainty in the frequency of flooding above the PMF.

EXTERNAL EVENTS ANALYSIS

External Flooding

TMI–1 is designed for a Probable Maximum Flood (PMF) of 1,625,000 cfs at TMI (1,750,000 at Harrisburg), corresponding to an elevation of 310 ft at the upstream end of the island. The PMF was selected prior to the 1972 hurricane Agnes, which produced a stream flow of 1,020,000 cfs and a maximum elevation of approximately 302 ft. Review of the TMI–1 and TMI–2 FSARs indicated that the TMI FSARs were updated to address the 1972 flood. However, the value of the PMF was not changed.

TMI–1 proposes to accommodate floods > 305 ft by installing gasketed cover–plates, that are kept available, over doors to buildings containing equipment essential for safe shutdown, by inflatable door seals, and by dikes around outdoor equipment. (The island has dikes that protects it against flooding for floods 300 ft–305 ft.)

The PRA report estimates the frequency of the PMF by plotting the frequencies of the 3 largest floods, occurring in 1936, 1964 and 1972, on a semilog scale; i.e., flood elevation vs. log frequency. These floods are said to be the greatest since 1784 and possibly since 1740. A straight line is drawn between the two largest flood elevations and extrapolated to estimate the frequency of exceedance of the PMF to be approximately 1E–05/yr. This value is referred to as both the mean value and the frequency of exceedance. There is no justification or discussion as to the validity of this method of estimating the PMF. The quoted uncertainty band is a factor of 25, without reference as to how this value was obtained. The PRA estimates the probability of recovery for floods above 310 ft as 0.5, based on an assumption that there is equal probability of any value between 0 and 1. The PRA also estimates a frequency 1.5E–04/yr for floods between 305 ft and 310 ft—an event tree is constructed to estimate the probability of core damage given such a flood. Considerable credit (a factor of about 40 overall) is claimed for possible protective actions in the event of a flood 305–310 ft.

The FSAR does not address the probability of the PMF. However, the TMI–2 FSAR states that the 1972 flood has a return frequency of about 400–500 years. The curve that is shown for flood frequency is not extrapolated to lower frequencies. The curve has a slight negative curvature, so that extrapolation would be very uncertain, but the frequency of a 1,625,000 cfs flood would certainly be less than 1E–04/yr based on this curve.

A Corps of Engineers (COE) report prepared in 1975 estimates the frequency of a flood greater than 1,750,000 cfs at Harrisburg to be approximately 7E–04/yr, based on a figure which is reproduced here as Figure 1.[41] This frequency estimate is based on plotting hurricane and non–hurricane floods separately. The curve drawn through the hurricane flood data has a much steeper slope than that through the non–hurricane flood data. Note that the curve passes below the 1972 flood data point; this feature of the curve is consistent with the methodology recommended for Federal agencies.[42]

The U.S. Water Resources Council reviewed flood data for the Eastern U.S. and recommended that the data be fit using a "Log Pearson III" equation[42], i.e.,

$$\log_{10}Q_p = m + s(k_{g,p}) \qquad (1)$$

where

$\log_{10}Q_p$	=	the fitted logarithmic discharge having exceedance probability p
$k_{g,p}$	=	the standardized Pearson Type III deviate with skew g and exceedance probability p, which is tabulated in Reference 42
m	=	the sample (logarithmic) mean
s	=	the sample (logarithmic) standard deviation
g	=	the skewness of the logarithms of the data.

In a personal communication between COE and NRC,[a] the COE stated that, using all data up to 1983, they estimated the parameters of such an equation to be log mean = 5.4475, standard deviation = 0.1559, skew coefficient = 0.90, where units of flow are cfs. This equation predicts the exceedance frequency of the PMF to be about 3.2E–04/yr, with an uncertainty factor of 5, see Figure 2 (the expected value

a. Letter from Arthur Buslik, NRC, to Mr. Harry Reilly, EG&G Idaho, Inc., October 7, 1988.

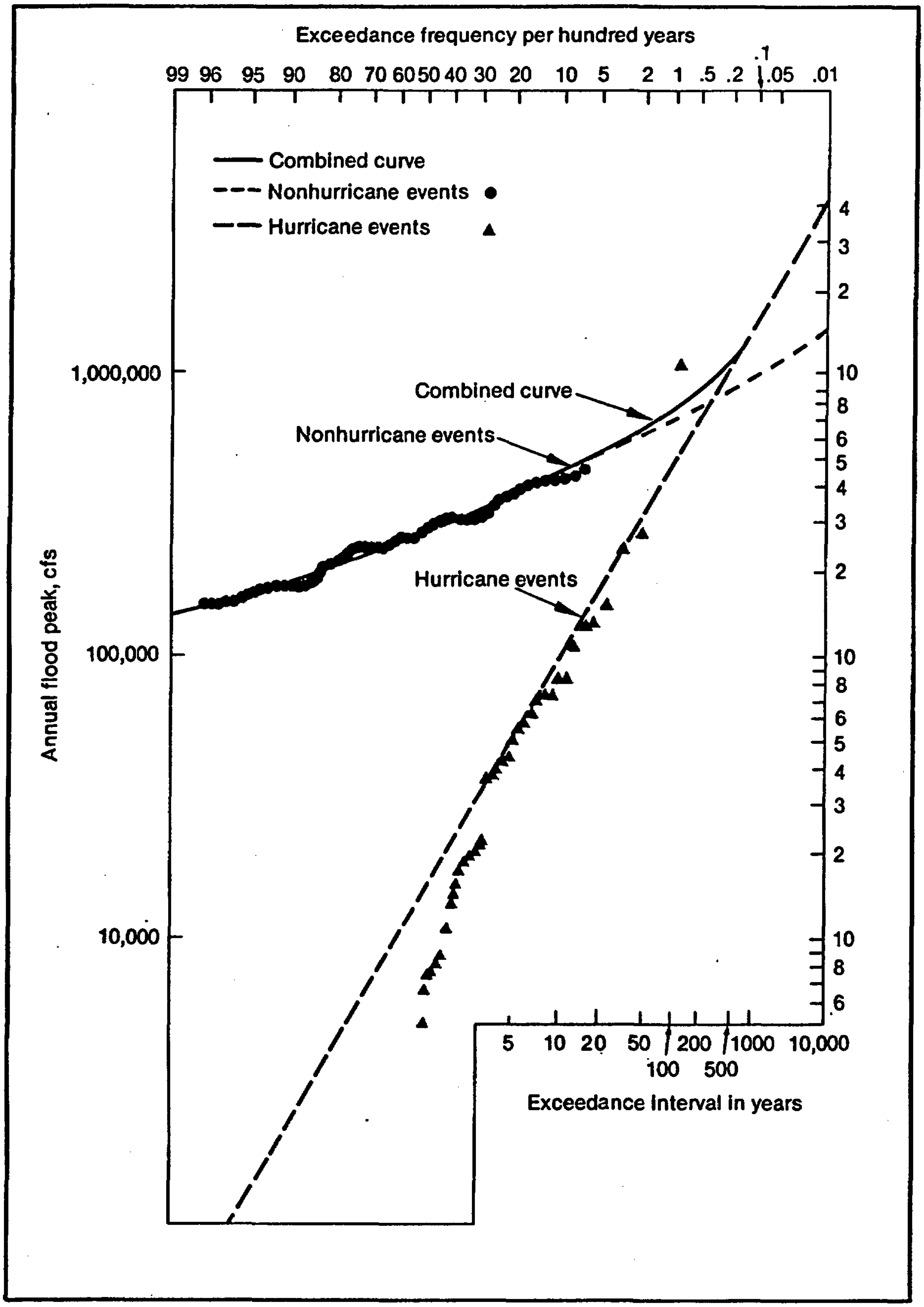

Figure 1. Nonhurricane and hurricane frequency curves.

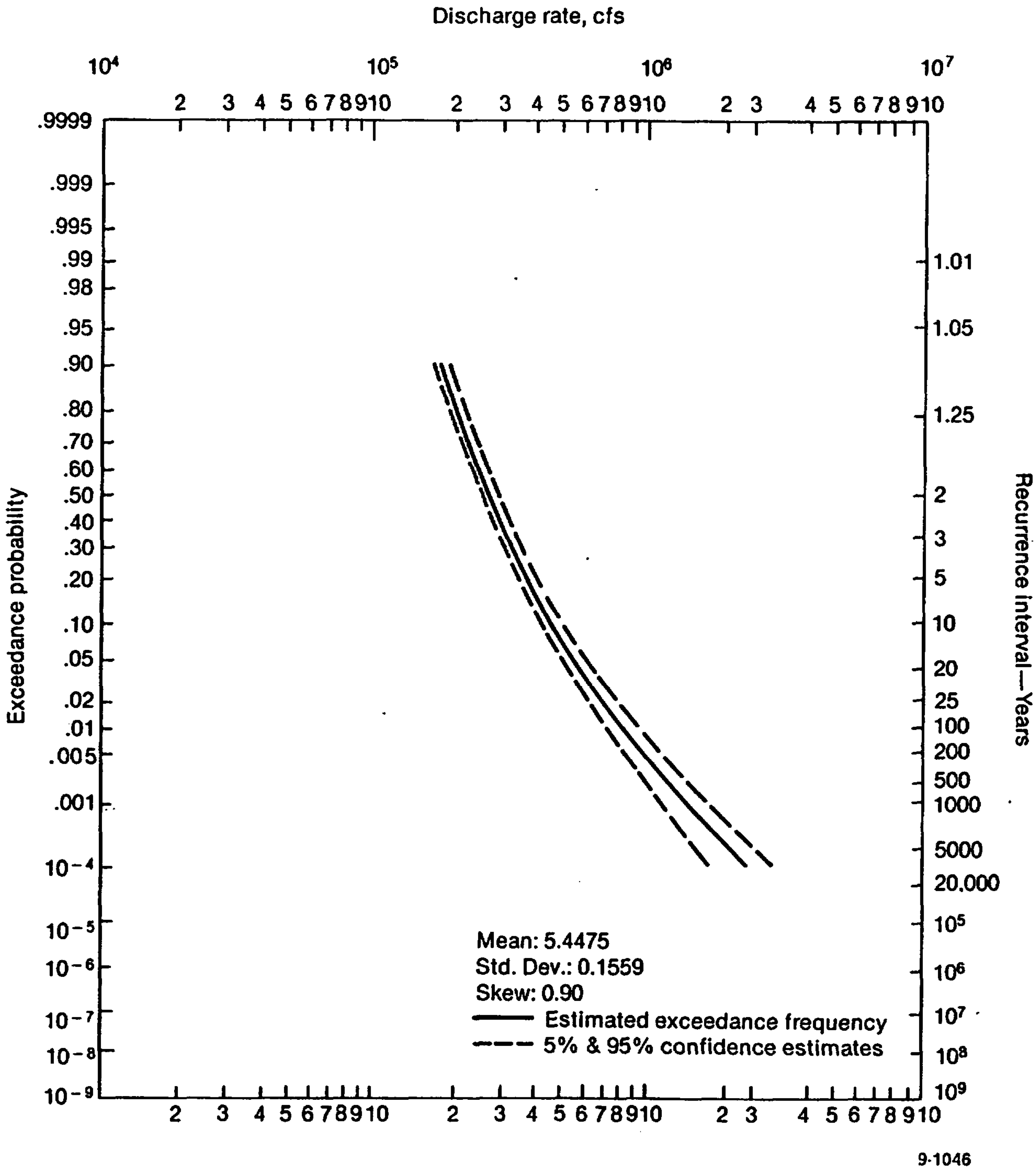

Figure 2. Estimated frequency curve for Susquehanna River at Harrisburg, PA, in accordance with Bulletin 17B.

corresponding to 3.2E–4/yr is 5E–4/yr, based on Reference 42). Of course, these uncertainty values are valid only if the underlying distribution is Log Pearson III.

The conclusion we draw from these comparisons is that the frequency of floods greater than the PMF is very uncertain, but may be much higher than the value (1E–05/yr) that was reported in the PRA. It seems unlikely that the plant can withstand a flood greater than the PMF—during a plant visit to TMI–1 it was observed that the protective cover–plates, dikes, and air intakes, are designed for 310 ft. Therefore, the CDF due to floods greater than the PMF is equal to the frequency of the floods.

It is also appropriate to address the frequencies of core damage due to floods 305–310 ft. These frequencies will be greater than shown in the PRA if the COE equation or the curve of Figure 2 is used—i.e., about 8E–4/yr. The PRA takes substantial credit for protective actions (early warning, shutdown, installation of cover plates) in the event of a flood 305–310 ft. During the plant visit, the personnel at TMI–1 indicated they did not practise installing the cover plates. The PRA assumed that a hurricane is unlikely to produce the PMF at the site, and that the emergency closure actions (top event SL) could be considered routine (sufficient time) rather than dynamic. However, it appears to us that the PMF is more likely to be produced by a hurricane. It seems the approach of the hurricane–induced flood, with the emergency closure taking place, would be accompanied by loss of offsite power along with heavy rain and high winds on site. The personnel would have one chance to make proper installation because after the arrival of high water, the island would be flooded, leaving little if any chance to correct any deficiencies. The PRA estimates the human error rates with a recovery factor of 0.19 to account for potential recovery in the event any steps in the emergency closure (top event SL) have failed. Our review indicates that the human response analysis results would not be changed for the decrease in warning time that would be involved in a hurricane–caused PMF. The human response analysis did not consider the likelihood of a cover plate or air–inflatable seal being defective and nonrepairable within the available time. The PRA may be optimistic in this regard. However, on a best estimate basis, the floods 305–310 ft are not as important as those above 310 ft.

The opinions of experts on the accuracy of frequency estimates for floods beyond the PMF should be noted. In a recent review of the literature, the reviewers concluded:

"The literature review indicates that extrapolation of the frequency curve does not provide experientially defensible estimates of flood probabilities much beyond those defined by the length of record."[43]

And in a review for NRC by LLNL:

"The best summary of the current situation is probably that extrapolations beyond the historical record are difficult except in those few (site–specific) situations where good regional data and a good local site model allow defensible analyses. In any event, extrapolations to values of F_P (the mean frequency of the flood) in the range, say, about 0.001/year, are highly uncertain."[44]

Our perspective is that the upper bound on the frequency of the PMF for TMI–1, assuming that the underlying frequency distribution has not changed during the last two centuries and is not changing now, must be in the vicinity of 5E–3/yr; if it were higher than that, the PMF would probably have occurred during the last two centuries.

Based on this information, the best–estimate frequency for river floods above the PMF is much higher than estimated in the PRA – 5E–4/yr rather than 1E–5/yr. External flooding may become a dominant sequence. And the large uncertainty band on the flooding frequency should cause an increased uncertainty in the total CDF.

In–Plant Fires

Introduction. Review of the Three Mile Island Unit 1 (TMI–1) Probabilistic Risk Assessment (PRA) internal fire analysis concentrated on three major concerns: methodology, data, and comparison with the draft "Fire Risk Scoping Study."[45] Each concern is discussed below.

Internal Fire Analysis Methodology. The TMI–1 PRA internal fire analysis is documented in the Environmental and External Hazards Report, under the section "Analysis of Spatial Interactions." The spatial interaction analysis involved determining area boundaries, identifying components and electrical cables in each area or zone (location), identifying the types of environmental hazards (fire, flood, steam, pipe whip, missiles, and others) in each area, performing a screening analysis for each hazard in each area, and performing a more detailed analysis for the dominant events. In addition, some fires were considered in the system fault trees (as events occurring during a mission time) while others were considered to be contributors to initiating events in the internal event analysis.

For the spatial interaction analysis, the TMI–1 PRA used fire areas, zones (within areas), or locations as appropriate boundaries. This is consistent with the approach taken in previous PRAs. Also, a wealth of component and electrical cable location information from Fire Hazards Analyses Reports (FHARs) is available, based on these locations. In addition to the safe shutdown equipment considered in the FHAR, the PRA also considered the following systems and components:

1. Reactor building spray system
2. Power–operated relief valves (PORVs) and associated block valves
3. Emergency safeguards actuation circuits
4. Condensate pumps
5. Instrument air system
6. Turbine stop and control valves
7. Borated water storage tank (BWST)
8. Condensate storage tanks
9. Control building HVAC Units AH–E–17A and AH–B–17B
10. Offsite power.

These additional components and systems were included because they were used in the various event trees developed for the internal event analysis. Cable routings for these components were not always known and in some cases had to be estimated. Again, this is typical of PRA fire analyses.

Two systems modeled in the internal event analysis were not included in the spatial interaction task: the reactor protection system (RPS) and the reactor building isolation system (RBIS). For the RPS, the following statement is made (see pp. 3–2 and 3–3 of the Environmental and External Hazard Report):

> "From an evaluation of the RPS, it is concluded that it is highly unlikely for any of the hazards considered in this analysis to fail the RPS so that the control rods would be prevented from inserting or the reactor trip circuit would be prevented from being energized."

A similar assumption was made for the RBIS. However, the RBIS is not believed to be needed for the Level 1 analysis.

Hazard identification for each fire area included consideration of fire, smoke, flood, steam, water jet, water spray, high energy line break, explosions, missiles, and falling objects. For the fire analysis, only fire and smoke are applicable. Potential inadvertent operation of sprinkler systems is considered to be part of the internal flooding analysis. Fires were considered to be possible if transient combustibles, electrical cabling, or electrical panels are present. Some PRA fire analyses have ignored one or more of these potential fire sources, so consideration of all three is a comprehensive approach.

During the investigation of fire hazards, modes of detection and suppression were identified. Also, propagation paths to other locations were considered. It appears that the most likely mode for fire propagation from one area to another is through doors left open or opened while fighting a fire.

Potential fire scenarios, in general, were quantified using the following equation:

$$F_{cd,i} = (F_{fi,i})\,(S_{su,i})\,(G_i)\,(S_{se,i})\,(O_i), \qquad (2)$$

where

$F_{cd,i}$	=	core damage frequency per year from fire scenario "i"
$F_{fi,i}$	=	fire frequency in area of concern for fire scenario "i"
$S_{su,i}$	=	nonsuppression probability for fire in fire scenario "i"
G_i	=	geometric factor (usually fraction of floor area of fire area from which a fire has the potential to damage essential cables or equipment) for fire in fire scenario "i"
$S_{se,i}$	=	security factor (judgement as to potential for nonsuppressed fire to be able to damage vital cables or equipment) for fire in fire scenario "i"

O_i = other event failure probability (covers additional human errors or component failures which must occur in order for core damage to occur) for fire scenario "i".

Fire frequencies for fire areas were estimated from historical evidence, as evaluated in Reference 46. The fire frequencies from this source are summarized in Table 13.

As is typical of most PRA fire analyses, frequencies of fires in areas within a building were often estimated by applying varying fractions of the total building fire frequency to each fire area. The fractions were usually estimated based on fraction of floor area, concentration of electrical equipment, personnel traffic, amount of transient combustibles present, and other factors. In some other cases, as indicated in Table 13, fire area frequencies were assigned values ranging from 1.0E-4/yr to 3.0E-3/yr.

The multipliers $S_{su,i}$, G_i, and $S_{sc,i}$ were estimated from experience with past PRAs (presumably Seabrook, Zion, and Indian Point). Screening values for $S_{su,i}$ ranged from 0.2 to 1.0. Values for G_i ranged from 0.01 to 1.0. Finally, $S_{sc,i}$ ranged from 0.03 to 1.0.

For fire scenarios with screening core damage frequencies greater than 3.0E-6/yr (less than 1% of the internal events core damage frequency), it is stated that a more refined analysis was performed. The six dominant fire scenarios are presented in Table 14. Also presented in Table 14 are two (of many) scenarios that were screened out: a control room fire and a relay room fire. The six dominant core damage sequences have a total core damage frequency of 1.0E-4/yr. This total is compared with results from selected previous PRAs in Table 15. The TMI-1 results are higher than any previous study except for Indian Point 2. It is not clear why this is the case. However, in the TMI-1 PRA it is stated that the dominant fire scenarios did not receive as much attention as would have been desired. It is possible that more refined analyses of these scenarios might reduce their frequencies. One interesting note is that most of the dominant scenarios result in the loss of reactor coolant pump (RCP) seal cooling, leading to an eventual RCP seal LOCA with no coolant injection possible.

Table 13. TMI-1 internal fire frequency comparison

	Frequency Per Year		
Location/Component	TMI-2	Seabrook PRA	Fire Risk Scoping Study
Auxiliary Building	4.8E-2	4.8E-2	6.4E-2
Turbine Building	1.6E-2	1.6E-2	3.2E-2
Control Room	4.9E-3	4.9E-3	4.4E-3
Cable Spreading Room	6.7E-3	6.7E-3	2.7E-3
Diesel Generator	7.4E-4/start	7.4E-4/start	—
Reactor Coolant Pump	7.4E-3	7.4E-3	—
"Typical" Room	1.0E-3	—	—
Larger Room (or with more electrical equipment)	3.0E-3	—	—
Smaller Room (or with less electrical equipment or less visited)	3.0E-4 or 1.0E-4	—	—

Table 14. TMI–1 internal fire dominant core damage sequences

Location	Description	Fire Initiator Frequency Per Yr	Geometric Factor	Severity Factor	Non–Suppression Factor	Other Factor	Core Damage Frequency Per Year	Notes
AB–FZ–6	Fire in Auxiliary Building MCC A fire area (originating in MCC 480V–ESV–1A), and a resultant hot short which fails all RCP seal injection and the thermal barrier cooling to at least 1 RCP, resulting in an RCP LOCA with no high pressure injection capability	0.001 (MCC Fire)	1.0	1.0	1.0	0.03 (hot short)	3.0E–5	
CB–FA–3a	Fire in Control Bldg 4160 Vac switchgear 1D (train A) fire area, failing train A of several safety systems, & a random failure of train B, resulting in core damage	0.003 (switchgear fire)	1.0	0.1	0.5	0.08 (random	2.4E–5)	The Technical Summary Report indicates this failure of train B sequence has a negligible frequency. However, the fire analysis tables indicate 2.4E–5/yr. The discrepancy is not understood.
CB–FA–2b	Fire in Control Bldg Switchgear Room 1S (train B of electrical power) leading to failure of all RCP seal cooling & eventual RCP seal LOCA with no high–pressure injection	0.003 (cabinet fire)	1.0	0.03 (must burn cables outside cabinet)	0.2	1.0	2.0E–5	
CP–FA–3c	Fire in Control Bldg ESAS area & failure of remote shutdown, resulting in an RCP LOCA with no high–pressure injection	0.002 (cabling or transient combustible fire)	1.0	0.1	0.5	0.2 (failure of remote shutdown)	2.0E–5	
CB–FA–3b	Fire in 4160 Vac switchgear 1E room & a hot short, resulting in an RCP seal LOCA with no high–pressure injection	0.003 (cable, cabinet, or transient combustible fire)	1.0	0.05	0.2	0.3 (hot short)	1.0E–5	

Table 14. (continued)

Location	Description	Fire Initiator Frequency Per Yr	Geometric Factor	Severity Factor	Non-Suppression Factor	Other Factor	Core Damage Frequency Per Year	Notes
CB-FA-2d	Fire in east battery charger area resulting in ?	0.003 (cable, cabinet, or transient combustible fire)	0.3	0.03	0.2	1.0	5.0E-6	
CB-FA-4b	Fire in control room panels failing the remote shutdown capability, combined with undefined operator error resulting in ?	0.0049 (cable, cabinets, or transient combustible fire)	0.01 (must occur in 2 of many panels)	1.0	1.0	0.05 (undefined operator error)	3.0E-6[a]	
CB-FA-3d	Fire in relay room, combined with failure of remote shutdown	0.007	0.05	0.1	0.3	0.2	2.0E-6[a] (failure of remote shutdown)	

a. These sequences were eliminated in the screening process and were not considered to be dominant.

Table 15. TMI–1 internal fire core damage frequency comparison

PRA Fire Analysis Study	Internal Fire Core Damage Frequency Per Year
TMI–1	1.0E–4
Seabrook	2.6E–5
Indian Point Unit 2	2.0E–4
Indian Point Unit 3	6.3E–5
Millstone Unit 3	3.1E–6
Limerick	2.3E–5
Oconee	1.3E–5

In general, the methodology used to identify and quantify important fire–induced core damage sequences is appropriate and is similar to the Seabrook PRA. However, several differences exist. First, the screening process for TMI–1 was performed manually, while the Seabrook PRA incorporated an automated SETS location–transformation process to identify potentially important single fire areas and adjacent pairs of fire areas. Both methods are appropriate. The manual method of screening might be more prone to error; however, the SETS methodology may require the use of simplified system fault trees and event trees (the Seabrook PRA utilized simplified models for the SETS location–transformation).

Secondly, the TMI–1 analysis appears to have been stopped after the screening phase. The six dominant fire scenarios do not appear to have been quantified in any more detail than the scenarios that were screened out. It is clear that no plant specific COMPBRN analyses were performed, as opposed to detailed COMPBRN analyses in the Seabrook PRA.[47]

The third aspect is that the TMI–1 fire analysis documentation is extremely abbreviated. This issue is examined more closely in the latter part of this section.

The final aspect is that the screening frequency of 3.0E–6/yr appears to be inadequate. If the frequencies of the already screened out fire–induced core damage sequences are summed, the result is 5.0E–5/yr, which is 50% of the core damage frequency from the six dominant fire sequences. This total is much too high. A screening frequency of less than 1.0E–6/yr would have been more appropriate.

Data Comparison. Fire frequencies utilized in the TMI–1 PRA are summarized in Table 13. Also presented in Table 13 are corresponding frequencies from Reference 45. The TMI–1 values are based on reported fires in commercial nuclear power plants up through 1981. Reference 45 includes an update through June 1985. Both sources agree within a factor of two. This difference is not large compared with the uncertainty in apportioning building fire frequencies among various fire areas.

For $S_{su,i}$, G_i, and $S_{se,i}$, the TMI–1 ranges are consistent with other studies. This is not surprising considering that no plant–specific values were generated for TMI–1; values from other PRAs were used instead.

Comparison with Fire Risk Scoping Study. The draft Fire Risk Scoping Study identified several areas of concern for probabilistic fire analyses. These areas of concern are listed below:

1. Control system interactions
2. Effectiveness of manual fire fighting
3. Total environmental equipment survival
4. Seismic–fire interactions
5. Adequacy of fire barriers
6. Adequacy of analytical fire tools.

Each of these is discussed below with respect to the TMI–1 PRA fire analysis.

The Fire Risk Scoping Study identified unanticipated control system interactions as a potential weakness in past probabilistic fire analyses. Such interactions include control room failures that may result in failure of remote shutdown, or hot shorts that may fail systems or components not actually damaged by a fire. The TMI–1 analysis attempted to consider some types of system interactions. For example, hot shorts have been considered for several of the fire scenarios (see the dominant fire sequence in Table 14). Also, the single control room scenario involves cabinet damage that fails remote shutdown. However, documentation is much too sparse to determine either the level of detail of such modeling or the comprehensiveness of the search for such interactions.

The effectiveness of manual fire fighting is another issue of concern. Some past PRAs may have taken too much credit for manual suppression, given the potential for smoke and misdirected efforts. Five of the top six TMI–1 fire sequences in Table 14 include credit for manual suppression. The documentation is too brief to evaluate the nonsuppression estimates; however, the lowest value used is 0.2.

Total environment equipment survivability refers to the concern that equipment may actually be damaged indirectly by a fire or fire suppression agent, rather than by direct exposure to the fire. Again, the TMI–1 documentation is not detailed enough to evaluate whether such concerns were adequately covered.

Seismic–fire interactions are not discussed in the TMI–1 fire analysis. A review of the seismic documentation produced the same result. Therefore, it appears that the potential for seismic–fire interactions was not considered in the TMI–1 PRA.

The Fire Risk Scoping Study addressed the concern that fire barriers, especially doors and cable penetration seals, may not withstand actual fire conditions. Specifically, if a significant pressure differential is created across the fire barrier, then premature failure may occur. Such a pressure differential could be created under fire conditions. The Fire Risk Scoping Study indicates that a barrier failure probability of 0.01 may be too optimistic, and that 0.1 might be more appropriate. It appears that the TMI–1 fire analysis considered fire door failures, but mainly from doors left open or opened to fight a fire. Otherwise, the screening analysis assumed fire door failure probabilities of 0.01 or lower. Therefore, the TMI–1 study may be nonconservative in this respect.

Finally, the Fire Risk Scoping Study evaluated the adequacy of COMPBRN I and III. Several coding errors and instances of nonphysical behavior were found in COMPBRN III. Conclusions that were drawn from this study indicate that when any of the versions of COMPBRN are combined with fire suppression estimates, the resulting estimates for conditional failure to suppress a fire before cable damage occurs may vary by a factor of 20 or more.

The TMI–1 fire analysis did not include plant-specific COMPBRN analyses. However, screening estimates for fire severity and nonsuppression factors were obtained from past PRAs that did include COMPBRN analyses. Because of this, the TMI–1 fire sequences should reflect a high degree of uncertainty. However, Table 6–9 in the Plant Model Report appears to have no information on fire sequence uncertainty distributions.

Internal Fire Documentation. The TMI–1 internal fire analysis documentation, contained mainly in Section 3 and Appendix D of the Environmental and External Hazards Report, is grossly inadequate. The fire analysis methodology is essentially discussed in two paragraphs in Section 3.5 of that report. Also, the six dominant fire sequences are described in several sentences in Section 3.7. No diagrams of the fire areas and zones were included in the report. Also, almost no documentation is provided to support analyses and probabilities used in the screening tables. For example, the control room fire (Table 14) with a frequency of 3.0E–6/yr was screened out. This sequence involves a fire frequency of 4.9E–3/yr, a geometric factor of 0.01, and an operator error of 0.05. The geometric factor of 0.01 supposedly represents the probability of a fire starting in only one of many panels in the control room. In this case, remote shutdown apparently is not possible; however, an undefined operator error of 0.05 is also applied to this sequence. There is no documentation indicating what type of operator error is involved. Also, what happens if there is a fire in the other 99% of the control room panels? If remote shutdown must be used, the TMI–1 analysis assumed a 0.2 failure probability. In such a case, the sequence frequency would be:

$$(0.0049/\mathrm{yr})\,(0.2) = 9.8\mathrm{E}{-4}/\mathrm{yr}. \qquad (3)$$

The study does not indicate why fires in 99% of the control room panels are not significant.

Plant Visit to TMI–1. During a plant visit to TMI–1, conducted during the course of this review, it was found that a) TMI–1 has a well thought out and thoroughly documented fire plan, b) there are zero to very–low amounts of transient combustibles in areas containing safety–related equipment, and c) there are multiple means of detecting and suppressing fires.[a] GPUN personnel stated they are reanalyzing the fire sequences and expect to find them to be an order–of–magnitude smaller in their contribution to core damage frequency than was indicated in the PRA report.

Summary. The TMI–1 PRA fire study appears to be a comprehensive screening analysis. However, it appears that the six dominant sequences were not analyzed in detail. Plant–specific COMPBRN analyses were not used, and screening estimates for nonsuppression, geometric, and severity factors were estimated based on previous PRAs. Seismic–fire interactions were not included. The total core damage

a. Letter from H. J. Reilly, EG&G Idaho, to Dr. Arthur Buslik, NRC, "Report of TMI–1 Plant Visit, October 18–19,, 1988," November 8, 1988.

frequency from internal fire is quoted in the PRA as 1.0E–4/yr. However, the screened–out sequences would add up to an additional 5.0E–5/yr. Documentation is grossly inadequate, making it impossible to perform a detailed review of the methodology, data, and results. It was the feeling of the reviewers, based on a plant visit and comparisons with other PRAs, that the core damage frequencies caused by in–plant fires may be overestimated in the TMI–1 PRA, but this claim cannot be substantiated without more analysis.

Seismic Events

During the review, it was discovered that the quantification of the seismic events contained errors that invalidated the results contained in the PRA report. These errors were acknowledged by GPUN (see the discussion in Appendix C to this report). Independent analyses were conducted as part of this review, using seismic hazards curves from three different sources: the PRA, EPRI, and LLNL. These analyses are described in Appendix C. All three of the analyses produced core damage frequencies larger than the value published in the PRA report. Using the PRA hazards curves and component fragilities, a mean seismic CDF of 6.5E–5/yr was obtained, as opposed to the value 2.7E–6/yr in the PRA. With the EPRI hazards curves, and some modifications to equipment fragilities because of the different seismic spectrum, the mean seismic CDF would be 2.3E–5/yr; with the LLNL hazards curves, it would be 3.8E–4/yr. It is also observed that only a few of the component and structural fragilities were based on plant–specific analysis. However, this effect is not considered as important as the selection of the appropriate hazards curves. This situation may be clarified when GPUN completes its evaluations as part of the IPE program.

ESTIMATES OF EFFECTS OF RECOMMENDED CHANGES TO THE PRA

Introduction

It was not possible in this review to requantify the accident sequences from the TMI–1 PRA, because of the complexity of the analysis and the unavailability of the computer programs and inputs. Therefore, it was difficult to determine the impacts of changes in modeling or data on the overall results. However, it was possible to gain some insights by manipulating the data in the report.

There were several items of interest to the review that were "reestimated." Each is discussed briefly in this section; the detailed explanation of the basis for each item is elsewhere in this review report (for example, the impact of changes to loss of control building ventilation sequences is examined in this analysis, while the discussion of the validity of the assumptions is in the Assumptions section). The results of the reestimation are shown in Table 16.

Three kinds of estimates were made. First, the effects of changes in initiator frequencies were estimated directly from Tables 5–1 and 5–2 of the PRA Report, Vol. 2. These tables list the aggregates of the core damage frequencies attributable to each initiator and initiator category. Estimates using this method are believed to be precise.

Secondly, the effects of changes in parameters that affect only fractions of sequences for specific initiators were estimated using the top 100 sequences listed in Table 6–5 of the PRA Report, Vol. 3. These top 100 sequences compose about 75% of the total core damage frequency, so that an estimate using this method, while an approximation, probably accounts for most of the effect.

Lastly, the effects of changes in the analyses of station blackout, external floods, and seismic events were taken from the respective review sections in this report. The methodologies for those estimates can be seen by reading those sections.

Table 16. Summary of reestimation of core damage frequency

Change	Old Value	New Value
Control building ventilation failure eliminated as a core damage sequence	2.00E–4/yr	0
Factor of 6.6 reduction in HRA value for sump recirculation switchover, medium LOCA	1.46E–5/yr	2.2E–6/yr
Very small break LOCA frequency 4 times larger	1.74E–5/yr	6.96E–5/yr
Use of value 2E–3/yr for loss of instrument air initiator frequency	1.98E–5/yr	6.6E–6/yr
Requantification of loss of offsite power sequences	2.90E–5/yr	5E–5/yr
Total CDF for Internal Initiators	4.4E–4/yr	2.9E–4/yr
Requantification of seismic sequences	2.70E–6/yr	6.5E–5/yr
Requantification of external flooding sequences	7.50E–6/yr	5E–4/yr
Total CDF for External Initiators	1.1E–4/yr	6.6E–4/yr

Changes That Were Included in the Estimates

A major finding of the PRA was that control building ventilation failures were major contributors to the core damage frequency. This was based on the assumption that the electric power system would fail catastrophically when the temperature in the control building exceeds 104°F. Subsequent analysis by the utility indicates that loss of control building ventilation would not lead to failure of the electrical power system. A review of this information by members of the review team confirmed that loss of CBV would not make a significant contribution to overall CDF. Therefore, the reestimation used a value of zero for sequences with control building ventilation failure.

The PRA indicates that the sequence of highest frequency (other than control building ventilation failure) is a medium LOCA with failure of sump recirculation switchover. The human response value used to quantify this sequence was the same as that for the large LOCA. The Systems Analysis Report clearly defined a value for both trains of the recirculation for medium LOCAs distinct from large ones, but the PRA did not use this value. The estimate in Table 16 used a value reduced by a factor of 6.6 for the (SAA*SBB) headings of the ML sequence to account for this discrepancy.

The initiating event review indicated that the very small break frequency appeared to be a factor of four lower than estimates from other sources. The reestimation increased the initiator frequency for those sequences by that factor.

The loss of instrument air initiator frequency appeared to be overestimated according to the initiating event review. The value assumed in Table 16 is the 2.0E-3/yr value from that review.

Appendix B, which contains a requantification of CDF attributable to station blackout, indicates that this frequency should be 3E-5/yr rather than the PRA value of 6E-6/yr. The CDF for all losses of off-site power then becomes about 5E-5/yr rather than the PRA value of 2.9E-5/yr.

After reestimating the internal event sequences with the changes noted above, the CDF for internal events is reduced from 4.4E-4/yr to 2.9E-4/yr.

The review of External Flooding indicated that the best estimate frequency for river floods above the PMF is 5E-4/yr instead of 1E-5/yr.

Appendix C contains three analyses of the seismic frequencies for TMI-1. The first corrects the erroneous analysis in the TMI-1 PRA report. The second is an analysis using the seismic acceleration frequency data from studies by LLNL. The third is an analysis using the seismic acceleration frequency data from studies by EPRI. The three analyses produce different results for the CDF (attributed to seismic events), but all are higher than the value in the TMI-1 PRA report. The highest value (using LLNL data) is 3.8E-4/yr, which would make seismic events among the dominant sequences for TMI-1. Table 16 includes the value 6.5E-5/yr, which was obtained using the data in the PRA report.

After reestimating the external event sequences with the changes noted above, the CDF for external events increased from 1.1E-4/yr to 6.6E-4/yr, making external events the dominant sequences at TMI-1.

Changes Not Included in the Estimate

There were numerous other changes that were recommended in the various sections of this review report. They were not included in Table 16 for various reasons. The following is provided to explain these changes as they appear in Table 17:

The Assumptions section indicated that the assumption in the PRA, that shutdown operations need not be examined because they have no significant effect, was questioned. The PRA for this operational mode could have a significant effect on overall CDF at TMI-1.

The section on Fires indicates the analysis in the PRA was suitable only for screening purposes, and it seems likely, but not certain, that further analysis will show core damage from fires to be smaller in frequency.

The initiating event review indicated that there had been one incident in 12 years of operation in which the intake screens at Unit 2—which was the only one of the two units operating at the time—plugged completely, requiring 6 hours to clear. The discussion of this initiating event appears erroneous; the PRA divides the assumed frequency of 1/12 per year by a recovery factor related to recovery before turbine trip. The PRA also uses a seal-LOCA model that assumes

Table 17. Potential changes not included in Table 16

Potential Change	Probable Effect on CDF	Significance on CDF
Risks of shutdown operations	Increase	High
Sequences initiated by in-plant fires	Unknown	High
Loss of river water sequences	Increase	High
V-sequence frequency	Unknown	Low
Frequency of reactor vessel rupture due to PTS	Increase	Low
Miscellaneous component failure data	Unknown	Low
Added backup air compressor	Decrease	Low
Relay chatter during seismic events	Increase	Unknown
Seismic-initiated fires	Increase	Unknown
Effects of non-Class I equipment falling on Class I equipment during a seismic event	Increase	Unknown

that 9 hours is available after loss of river water pump suction before seal-LOCA occurs. The NUREG/CR-4550 seal-LOCA model is much more pessimistic when applied to TMI-1. Given a blockage of the intake screens with mean time to clear of 6 hours, the following factors govern the time available (using the times quoted in the PRA for the EFW available case):

Water available in pump house: 1.3–4 hours with 2 RW pumps operating, double that for 1 pump

Additional time gained by rotating MU pumps after loss of river water: "a few hours" according the PRA—actual time is unknown

Time to seal-LOCA after loss of seal cooling: 1.5–2.5 hours (70% chance)

Time to core damage after seal-LOCA (not part of time available): 1 hr.

The minimum time may be less than required. To ensure success, the operator must take actions to turn off 1 RW pump and rotate MU pumps after the water in the pumphouse is depleted, as well as diagnosing and initiating the screen-clearing operation. There is also a possibility—identified but not analyzed in the PRA—of hooking up fire service water in place of river water. These are all knowledge-based actions, with an operator-to-plant interface that is fair at best, and conditions of potential emergency. Without more detailed information and analysis, it is not possible to derive defensible values for the failure probabilities of the human actions.

GPUN provided some additional information informally. There have been an additional 5 years of operation of the TMI-1 intake screens without blockage. There are no procedures to maintain a minimum amount of water in the river water intake structure, and no procedure directing the operator to reduce the number of operating river water pumps if a complete loss of river water supply occurs. However, a fire service supply is available near the DHCCCW heat exchangers with connection points available for a temporary hookup. Also, the heat load is so low (32 gpm) when running only makeup for RCP seal injection flow, that GPUN believes the makeup pumps would run for a long time even without river water.

Unless it can be verified that the makeup pumps can run without river water, or that a recovery action is possible using the fire service water supply, the situation upon loss of river water supply—which is reasonably probable based upon its previous occurrence—may be much more serious than the PRA indicates.

In the analysis of V–sequence frequencies, the PRA combines what appears to be conservative assumptions with nonconservative data. These sequences are insignificant contributors to CDF, but are important to offsite risk in most PRAs.

The review (see Comparison with Generic Unresolved Safety Issues) found that frequency of core damage due to PTS was probably underestimated, but conceded that PTS is not a dominant contributor to overall CDF.

The Data section of this review report indicated that some of the component failure data values were significantly different than in other databases. But it was not expected that any individual change in a value would have much effect on the overall CDF.

During the plant visit, we noticed the addition of a backup air compressor. It is not clear how this will affect the PRA, except it should be beneficial.

During the plant visit, it was established that relay chatter was assumed to be recoverable, i.e., had no effect on the CDF due to seismic events. Forthcoming resolutions by NRC of generic issues involving seismic events may be expected to have an impact if relay chatter during seismic events is found to be an important failure mode of electrical power and control systems.

The effects of seismically–induced fires, and the effects of non Class I equipment falling on Class I equipment during a seismic event, appear to have been neglected in the PRA. The effects of their inclusion would not be simple to calculate.

REFERENCES

1. Pickard, Lowe and Garrick, Inc., *Three Mile Island Unit 1 PRA*, PLG–0525, prepared for GPU Nuclear Corporation, November 1987).

2. Letter from H. D. Hukill, Vice President & Director, TMI–1, to U.S. Nuclear Regulatory Commission, December 7, 1987, (available from Hukill file).

3. J. W. Hickman et al., *PRA Procedures Guide*, Vols. 1–2, NUREG/CR–2300, prepared under the auspices of the ANS and IEEE, January 1983.

4. A. S. McClymont and B. W. Poehlman. *ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients*, EPRI NP–2230, Electric Power Research Institute, January 1982.

5. *Nuclear Power Experience*, S. M. Stoller Corporation, Boulder, Colorado.

6. *Zion Probabilistic Safety Assessment*, Commonwealth Edison of Chicago, Fall 1981.

7. *Probabilistic Risk Assessment, Seabrook Station*, Public Service Company of New Hampshire, December 1983.

8. D. P. Mackowiak, C. D. Gentillon, and K. L. Smith, *Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments*, NUREG/CR–3862, U. S. Nuclear Regulatory Commission, May 1985.

9. H. Wyckoff, *Losses of Offsite Power at U. S. Nuclear Power Plants, All Years Through 1986*, NSAC–111, Nuclear Safety Analysis Center, Electric Power Research Institute, May 1987.

10. P. W. Baranowsky, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*, NUREG–1032, U. S. Nuclear Regulatory Commission, June 1988.

11. *Guidelines and Technical Bases for NUMARC Initiatives Addressing Station Blackout at Light Water Reactors*, NUMARC–8700, Nuclear Management and Resources Council, November 20, 1987.

12. Letter from H. D. Hukill of GPUN Nuclear Corporation to USNRC, Docket No. 50–289, May 5, 1988, (available from Hukill file).

13. Letter from H. D. Hukill of GPUN Nuclear Corporation to USNRC, Docket No. 50–289, August 5, 1988, (available from Hukill file).

14. Letter from Ronald W. Hernan, Senior Project Manager, to Mr. Henry D. Hukill, Vice President and Director – TMI–1, "Resolution of Various TMI–1 Appendix R Issues (TAC Nos. 64951 and 68331)," September 7, 1988, (available from Hernan file).

15. USNRC, *Loss of Residual Heat Removal System, Diablo Canyon, Unit 2, April 10, 1987*, NUREG–1269, June 1987.

16. Brookhaven National Laboratory, *Improved Reliability of Residual Heat Removal Capability in PWRs as Related to Resolution of Generic Issue 99*, NUREG/CR–5015, May 1988.

17. *Zion Nuclear Plant Residual Heat Removal PRA*, NSAC–84, July 1985.

18. A. Ang and N. M. Newmark, *A Probabilistic Seismic Safety Assessment of the Diablo Canyon Nuclear Power Plant*, 1977.

19. Power Authority of the State of New York, Consolidated Edison Company of New York, Inc., *Indian Point Probabilistic Safety Study*, 1982.

20. Fauske & Associates, Inc., *Evaluations of Containment Bypass and Failure to Isolate Sequences for the IDCOR Reference Plants*, FAI/86-29, July 1986.

21. M. T. Drouin, et al., *Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines*, NUREG/CR-4550, Vol. 1, Sandia National Laboratories, September 1987.

22. *Crystal River Unit 3 PRA*, Florida Power Corporation and Science Applications International Corporation, July 1987.

23. N. A. Hanan and D. R. Henley, *A Review of the Crystal River Unit 3 Probabilistic Risk Assessment*, NUREG/CR-5245, Argonne National Laboratory, January 1989.

24. *Safety and Performance Improvement Program*, BAW-1919, Rev. 5, Babcock & Wilcox Owners' Group, July 22, 1987.

25. *Safety Evaluation Report Related to the B&W Owners' Group Plant Reassessment Program*, NUREG-1231 and NUREG-1231 Supplement 1, U.S. Nuclear Regulatory Commission, March 1988.

26. Oak Ridge National Laboratory, *Preliminary Development of An Integrated Approach to the Evaluation of Pressurized Thermal Shock as Applied to the Oconee Unit 1 Nuclear Power Plant*, NUREG/CR-3770, May 1986.

27. *Shutdown Decay Heat Removal Analysis of a Babcock and Wilcox PWR*, NUREG/CR-4713, Sandia National Laboratories, March 1987.

28. *Analysis of Core Damage Frequency: Surry Unit 1 Internal Events Appendices*, NUREG/CR-4550, Vol. 3, Rev. 1, Part 2, (Draft), Sandia National Laboratories, December 1988 (Available from the NRC Public Document Room).

29. *Leak Rate Analysis of Westinghouse Reactor Coolant Pump*, NUREG/CR-4294, Rockwell International Corp., July 1985.

30. *Analysis of Core Damage Frequency from Internal Events: Expert Judgment Elicitation – Part 1: Expert Panel Results, Part 2: Project Staff Results*, NUREG/CR-4550, Vol. 2, Sandia National Laboratories, April 1989.

31. *IEEE Guide to the Collection and Presentation of Electrical, Electronic and Sensing Component Reliability Data for Nuclear Power Generation Stations*, IEEE STD-500, June 1977.

32. *Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Example*, NUREG/CR-4780, January 1988.

33. U.S. Nuclear Regulatory Commission, *Reactor Risk Reference Document*, NUREG-1150, Vols. 1-3, (Draft), February 1987.

34. A. A. Garcia, et al., *A Review of the Millstone 3 Probabilistic Safety Study*, NUREG/CR-4142, Lawrence Livermore National Laboratory, April 1986.

35. C. L. Atwood and J. A. Steverson, *Common Cause Fault Rates for Diesel Generators: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1978*, NUREG/CR-2099, EG&G Idaho, Inc., May 1982.

36. A. D. Swain and H. E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Sandia National Laboratories, 1983.

37. G. W. Hannaman, A. J. Spurgin and Y. D. Lukic, *Human Cognitive Reliability for PRA Analysis*, NUS–4531, Electric Power Research Institute, 1984.

38. R. E. Hall, J. Fragola and J. Wreathall, *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, NUREG/CR–3010, Brookhaven National Laboratory, 1983.

39. L. M. Potash et al., *Experience in Integrating the Operator Contributions in the PRA of Actual Operating Plants*, 1981 ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY.

40. R.C. Bertucio and J. A. Julius, *Analysis of Core Damage Frequency: Surry Unit 1 Internal Events*, NUREG/CR–4550, Vol. 3, Rev. 1, Part 1, Sandia National Laboratories, September, 1988.

41. Corps of Engineers, Department of the Army, North Atlantic Division, *Hydrologic Study – Tropical Storm Agnes*, December 1975.

42. United States Water Resources Council, *Guidelines for Determining Flood Flow Frequency*, Bulletin #17B, September 1981.

43. Interagency Advisory Committee on Water Data, Hydrology Subcommittee, *Feasibility of Assigning a Probability to the Probable Maximum Flood*, 1986.

44. C.Y. Kimura and R.J. Budnitz, *Evaluation of External Hazards to Nuclear Power Plants in the United States*, NUREG/CR–5042, Lawrence Livermore National Laboratory, December 1987.

45. *Fire Risk Scoping Study, Investigation of Nuclear Power Plant Fire Risk Including Previously Unaddressed Issues*, NUREG/CR–5088 (Draft), Sandia National Laboratories, March 1988 (Available from NRC Public Document Room).

46. M. Kazarians and G. Apostolakis, *Modeling Rare Events, The Frequencies of Fires in Nuclear Power Plants*, presented at the Workshop on Low–Probability/High–Consequence Risk Analysis, Society for Risk Analysis, Arlington, Virginia, June 15–17, 1982.

47. N.O. Siu, *COMPBRN – A Computer Code for Modeling Compartment Fires*, NUREG/CR–3239, University of California, May 1983.

APPENDIX A

REVIEW OF ASSUMPTIONS IN THE PRA REGARDING LOSS OF CONTROL BUILDING VENTILATION

APPENDIX A

REVIEW OF ASSUMPTIONS IN THE PRA REGARDING LOSS OF CONTROL BUILDING VENTILATION

It should be noted that, unlike most initiators, the frequency of the loss of control room ventilation initiator is not based on data (Table 3–8, Page 3–38, Volume 5), but is instead quantified based on an analysis of the system failure probability as contained in Volume 4, Book 1, Section 6. This review is concerned only with the evaluation of major assumptions made in the PRA regarding the initiator—loss of control building ventilation.

The major assumptions made in the PRA regarding this initiator and the accident sequence that it initiates are as follows:

- All key electrical equipment in the control room is assumed to always fail if the temperature exceeds 104°F.
- Loss of control room building ventilation is assumed to result in a core damage accident (see discussion below).
- If the outside ambient air temperature exceeds 84°F, the chillers associated with the control room building ventilation system are assumed to be required.
- Operator action to establish control building ventilation from a portable vent system is modeled. Equipment for this system was being purchased at the time of the PRA study.
- The operator actuated portable vent system is assumed to be incapable of limiting control building temperature below 104°F if the outside ambient air temperature is >95°F.
- Control tower air system failures are neglected.

The significance and validity of each of these assumptions will be explored individually, as follows:

- *104°F Limit*—The only basis that could be found for this assumption was on page 6–47, Volume 4, Book 1, where information shows that this is the design temperature limit of the equipment in the control building. It is also stated on page 6–48 that this assumption is believed to be conservative, but no evaluation could be found that provided either a qualitative or quantitative estimate of the degree of conservatism. The following statement is made on page 6–48:

  "The assumed temperature limit is important because it not only affects the time available for recovery, but also, if the limit was just a little higher (i.e., 130°F), many of the rooms might never reach the limit even without ventilation."

In view of the extraordinary dominance of the sequence associated with this initiator the omission of any estimate of the significance of this assumption is considered a major shortcoming in the study. Furthermore, it does not appear that the uncertainty or conservatism associated with this assumption is reflected in the very tight uncertainty bounds estimated for the core damage frequency.

An attempt was made to assess the validity, quantitative significance, and uncertainty associated with this assumption. Such efforts proved generally futile, however, for several reasons. First, no assessment of the control building heatup rate could be found in the TMI–1 PRA. Thus, the timing and sensitivity of the 104°F limit to building heatup rate could not be verified. Further, no other PRA or safety assessment could be found, for comparison, which evaluated this initiating event. The manufacturer of, and specifications for, the electrical equipment in the control building are not known. Thus, an independent evaluation of the operational temperature limits could not be determined, although engineers familiar with this general field confirmed that assuming failure at the design limit is likely to be a very conservative approach.

The TMI–1 PRA contains additional discussion of the interest related to the control building ventilation failure sequence. In particular, Pages 2–6 and 2–7 of the Executive Summary (Volume 1) make the following statement:

> "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 that the operator has more than enough time to perform the action successfully, then the frequency of the scenario will become insignificant. 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."

An attempt was made to evaluate the analysis of this sequence and also to estimate the impact of a more realistic assessment utilizing the September 1987 data. However, no analysis of the building heatup rate could be found, nor was any detail found regarding the time available and assumptions made regarding operator recovery actions. Furthermore, the September 1987 data is apparently not included in the PRA.

The reviewers concluded that the basis for the 104°F control building equipment failure assumption is inadequate and probably not realistic (overly conservative). This appears to be a major shortcoming in the study in view of the significance of the related accident sequence. A related shortcoming is the lack of sufficient information in the PRA to allow either an independent evaluation of the sequence or a quantitative estimate of the effect of the assumption. Furthermore, it appears inappropriate in a PRA study to assume a step failure distribution (i.e., never fails at temperatures <104°F and always fails at or above 104°F) for such an important initiator. It would be more realistic, and more consistent with the general PRA approach, to represent the failure as a temperature versus failure probability relationship. Such a relationship would have to be derived on the basis of existing data, or engineering judgement if data is unobtainable.

- *Loss of control building ventilation leads to core damage*—The PRA assumes that loss of control building ventilation will lead to equipment failures in the control building that result in core damage. Page 2–2 (Volume 1), presents the following conclusion to this problem:

"Failure of the ventilation system causes the internal room temperatures to increase and, within a period of hours, to exceed the design temperatures of 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 event 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. 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."

Further, Page 2–7 of Volume 1 presents the following:

"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."

In a related discussion, the PRA speculates (Page 2–7) that tests performed by Westinghouse on RCP seals, believed to be representative of the seals for the reactor coolant pumps at TMI–1, suggest that seal failures may be delayed from what was assumed in the PRA.[A–1] These delays are addressed on Page 2–8:

"These delays will significantly increase the likelihood of successful accomplishment of these (recovery of seal cooling and/or seal injection in scenarios after both were lost) and such actions that already exist in the PRA thus reducing the total core damage frequency."

Based on the previous discussion, it appears that the PRA assumes that the loss of control building ventilation leads to loss of the seal injection and seal injection cooling systems, due to loss of ac power to the pump motors in these systems. The loss of these systems causes a loss of pump seals, resulting in a LOCA (of unspecified size). Because the high–pressure injection system is also assumed lost due to loss of ac power to the pump motors, the pump seal LOCA results in unrecoverable loss of primary coolant inventory and eventual core damage.

This assumption of core damage (given failure of equipment in the control building) appears reasonable if pump seals fail and HPI is unavailable. The speculation that Westinghouse data on pump seal failures may argue for an extended recovery period and reduced core damage frequency, although not quantified in the PRA, does not appear particularly favorable in view of a recent report on pump seal failures.[A-2] This report presents a rather high probability of core uncovery from pump seal failures in a rather short time (four hours or less) given loss of seal injection and seal injection cooling. The forthcoming resolution of NRC Generic Issue 23 (Reactor Coolant Pump Seal Failure) should provide additional data and information relevant to this issue, and may require modifications at some plants, including TMI–1, which could alter the probability of the accident sequence considered here, as well as other sequences in the report.

- *Control building ventilation chillers assumed required if outside ambient exceeds 84°F*—The PRA states, on Page 6–10, that if the chilled water system fails, it is assumed that adequate ventilation is provided as the outside air temperature is less than 84°F. The basis for this assumption is not given in the PRA, but is based on GPUN correspondence.[A-3] This reference was not provided with the PRA and was therefore not reviewed. However, an apparently conflicting assumption appears on Page 6–49 of the PRA, which states:

  "If nuclear services closed cooling water is unavailable...the chilled water system...is unavailable. The system failure frequency then becomes strongly dependent on the outside air temperature. If the outside air temperature is greater than 95°F...then neither the normal ventilation system operating in the once-through mode nor the alternate ventilation system that may be established by the operators is assumed to be successful."

  The validity of the outside ambient air temperature assumption could not be evaluated on the basis of information provided in the PRA. However, the significance of the assumed outside temperature appears important based on the following statement on page 6–49:

  "Common cause failures of the two chilled water trains at a time when the outside air temperature is greater than 95°F is the major contributor to the initiating event (loss of control building ventilation) frequency."

  If the 85°F limit stated on Page 6–10 is the actual limit, then loss of control room ventilation frequency would be even higher.

- *Use of a Portable Vent System*—The PRA states on Page 6–10 that a portable vent system is modeled on the basis that equipment for the system was being purchased, and procedures were being revised, at the time of the PRA study. It is questionable if an accurate estimate of the unavailability of this system could have been made at the time of the PRA without this information. However, this quantification may not be overly significant in view of the preceding discussion, which indicates that failure of the main system when outside air temperatures are greater than 95°F (when the backup system would also not be effective) is the major contributor to loss of ventilation.

- *Operator actuated system ineffective if outside air temperature is >95°F*—This assumption appears on page 6–10, Volume 4, Book 1. The basis for it is referenced correspondence that has not been reviewed.[A-4]

- *Control air system failures are neglected*—This assumption appears on Page 6–43, Volume 4, Book 1. Further, on Page 6–12, it is stated that the control tower compressed air trains are needed for damper position and fan control for the control building ventilation system. However, page 6–11 states that the control tower air system consists of four compressors, two powered from each train; therefore, this omission is expected to have a very minor impact.

REFERENCES

A–1. Westinghouse Owners' Group, *Reactor Coolant Pump Seal Performance Following the Loss of All ac Power*, WCAP–10541, Revision 2, November 1986.

A–2. D. B. Rhodes, *Review of the Westinghouse Owners Group Report WCAP–10541, Revision 2, Reactor Coolant Pump Seal Performance Following a Loss of All ac Power*, NUREG/CR–4906P, January 1988, .

A–3. Letter from C. D. Adams of GPUN Nuclear Corporation to D. J. Wakefield of Pickard, Lowe and Garrick, Inc., April 29, 1986.

A–4. Letter from C. D. Adams of GPUN Nuclear Corporation to D. J. Wakefield of Pickard, Lowe and Garrick, Inc., May 9, 1986.

APPENDIX B

REQUANTIFICATION OF THE STATION BLACKOUT CORE DAMAGE FREQUENCY

APPENDIX B

REQUANTIFICATION OF THE STATION BLACKOUT CORE DAMAGE FREQUENCY

This appendix provides an independent calculation of the frequency of core damage from station blackout at TMI-1. The basic model is that of NUREG-1152.[B-1] A station blackout may occur either at the time of the loss of offsite power, or later if, for example, the diesel generators fail during operation while offsite power is unavailable. If the duration of the station blackout exceeds a certain time (called the "grace time" here), core damage occurs. Recovery of the diesel generators, and of loss of offsite power are modeled. One distinction between the model used here, and the model developed for NUREG-1152, is that the grace time is treated here as a random variable. Another distinction is that, in the model used for NUREG-1152, the grace time depended on the time after the loss of offsite power that the station blackout occurred, and this distinction is not made here.

The model considers contributions from five different ways of entering station blackout:

a. Both diesel generators are unavailable at the time of loss of offsite power, either because they fail to start, or because one is in maintenance and the other fails to start

b. One diesel is in maintenance, the other diesel starts but fails while running

c. One diesel fails to start, the other diesel starts but fails while running, leading ultimately to core damage

d. Both diesels start but fail (at the same time) during operation from a common cause

e. Both diesels start, then one fails during operation from an independent cause; later, the second diesel fails from either an independent or common cause.

The term "probability" is used here as the frequentist would use it. It corresponds to the term "frequency" used in the PRA. In this section, frequency refers to a rate per unit time (e.g., frequency of loss of offsite power). The probability distribution for the grace time is then a frequentist's probability distribution. However, if one were to assume that this probability distribution really represented a degree-of-belief distribution, the results for the mean value of the station-blackout-induced severe core damage frequency would not be affected.

The estimates obtained closely approximate the mean frequency of severe core damage (due to station blackout). Mean values are used for estimates of the various failure rates; the dominant terms in the result for the station blackout core damage frequency are linear in these parameters, because the terms involving common mode failures are the most important terms. There are contributions from non-linear terms, for example, both diesel generators failing to start from independent causes, and because the mean of the square of a variable over its degree-of-belief distribution is not the square of the mean, the estimates for the frequency of severe core damage due to station blackout are not exactly mean values.

Glossary of Symbols

λ_n — Rate of loss of the offsite power network (events per year).

$Q_n(t)$ — Probability that offsite power has not been recovered by time t after its loss. Thus $\lambda_n Q_n(t)$ is the frequency of losses of offsite power exceeding t hours.

q_f — The probability that a single diesel generator fails to start on demand.

$Q_f(t)$ — Probability of nonrecovery of a diesel generator by time t after its failure, for either the failure-to-start mode of failure or the failure-during-operation mode of failure, if these failures were from independent causes.

q_m — Probability of a single diesel generator being in maintenance at the time of demand.

$Q_m(t)$ — Probability a diesel generator in maintenance will not be recovered by time t after the maintenance is begun. The equations for the contribution of the maintenance unavailability to the station blackout core damage frequency are valid only for an exponential distribution for $Q_m(t)$. In this case, $Q_m(t)$ also equals the probability a diesel generator found to be in maintenance at the time $t = 0$, at which loss of offsite power occurs, will still be in maintenance at the time t after the loss of offsite power occurred.

q_c Probability both diesel generators fail to start from a common cause.

$Q_c(t)$ Probability a diesel generator that has failed from a common cause will not be recovered by time t after its failure; the same distribution is used for both the common cause failure–to–start and the common cause fails–during–operation modes of failure.

λ_f Failure rate (per unit time) for a diesel generator to fail during operation. The rate is assumed constant, and independent of the time since the diesel generator was started. The observed increased failure rate of a diesel generator during the first hour of operation is incorporated into the model by increasing the failure–to–start probability of the diesel generator.

λ_c Failure rate from a common cause event (or shock) that will disable all the running diesels.

τ Grace time, or coping time. If the duration of the station blackout exceeds the time (τ), core damage occurs. The value of τ depends on whether or not emergency feedwater is available, the timing and magnitude of a reactor coolant pump seal LOCA, and the timing of battery depletion. Therefore, a probability distribution is used for τ.

w_1 The end point in the calculations. Station blackouts occurring after this point of time (as measured from the time of initiation of the loss of offsite power event) are assumed to be recovered before core damage occurs. An inherent assumption in the model is that some source of ac power will be recovered within 24 hours. The value of w_1 is determined from $w_1 + \tau = 24$ hours.

Model Equations

Corresponding to each of the five ways of reaching station blackout, a quantity where I_j, j = a, b, c, d, or e, is defined. Then the contribution of case j to the station blackout core melt frequency is $\lambda_n I_j$.

The values of I_j for the five cases are given as follows:

a. Both diesel generators are unavailable at the time of the loss of offsite power, either because both diesel generators fail to start, or because one diesel generator fails to start and the other is in maintenance.

$$I_a = \{(q_f - q_c)^2\,[Q_f(\tau)]^2 + q_c Q_c(\tau)\}Q_n(\tau)$$
$$+ 2Q_n(\tau)q_f q_m Q_f(\tau)Q_m(\tau) \qquad \text{(B–1)}$$

b. One diesel generator is in maintenance, and the other fails during operation,

$$I_b = 2q_m Q_f\,(\tau)\int_0^{w_1}\lambda_f \exp(-\lambda_f w)Q_m(w+\tau)$$
$$Q_n(w+\tau)dw \qquad \text{(B–2)}$$

c. One diesel generator fails to start, the other fails during operation.

$$I_c = 2q_f Q_f\,(\tau)\int_0^{w_1}\lambda_f \exp(-\lambda_f w)Q_f(w+\tau)$$
$$Q_n(w+\tau)dw \qquad \text{(B–3)}$$

d. Both diesel generators start, but then fail during operation by common mode.

$$I_d = Q_c\,(\tau)\int_0^{w_1}\lambda_c \exp(-\lambda_c w)\cdot$$
$$\exp(-2\lambda_i w)Q_n(w+\tau)dw \qquad \text{(B–4)}$$

e. Both diesel generators start, then fail during operation at different times; the diesel generator that fails first by an independent failure, and the other diesel generator fails by either common cause or an independent failure. Little error results from assuming that the distribution of the time to recovery for the second failed diesel generator is that for a diesel generator failed from an independent cause, although, strictly speaking, it should be a mixture of the distributions for the independent failures and the common cause failures, weighted by their relative frequencies.

$$I_e = 2Q_f(\tau) \int_0^{w_1} \lambda_f \exp(-\lambda_f w) Q_n(w + \tau)$$

$$\int_0^{w} \lambda_f \exp(-\lambda_f x) \cdot$$

$$Q_f(w - x + \tau) dx dw \quad . \qquad \text{(B–5)}$$

Then the station blackout core melt frequency is:

$$P_{sb} = \lambda_n (I_a + I_b + I_c + I_d + I_e) \quad . \qquad \text{(B–6)}$$

Diesel Generator Failure, Repair and Maintenance

The diesel generator failure–to–start probabilities and the fails–during–operation failure rates are taken from the PRA (these values, and the manner in which they were derived, were reviewed during the review of the PRA, see the section on component failure data in the main review report). The common mode parameters (the beta factors) are also taken from the PRA. For the recovery distributions for a failed diesel generator, or the distribution for the maintenance time, exponential distributions are assumed. For the recovery distribution for a diesel generator failed by independent causes, the parameter in the exponential distribution is obtained by fixing the median repair time at the median value of 8 hours given in NUREG–1032 (see Ref. B–2, p. B–12). For recovery from a common cause failure, the value of the parameter is chosen so as to best reproduce the distribution of recoveries given in NUREG/CR–3226 (see Ref. B–3, p. 237). The same reference is used for recovery from maintenance. Table B–1 summarizes the diesel generator data.

Distribution of the Grace Time

The grace time, or time that the plant can be without ac electric power without suffering severe core damage, depends on the timing and magnitude of any reactor coolant pump (RCP) seal LOCA, on whether or not emergency feedwater is available, and on the battery depletion time. It is a random variable, because the timing and magnitude of the reactor coolant pump seal LOCA are random variables, and because failure of emergency feedwater is a random event.

If emergency feedwater (EFW) is not available, the grace time is about 1 hour, according to the PRA (see p. 4–43, Vol. 6, Book 1 of the PRA). The probability the EFW fails, given station blackout, is 0.056, according to Table 6–1, Vol. 3 of the PRA.

As for the grace time distribution if the RCP seal LOCA is controlling, the calculation proceeds as follows. According to the expert opinion elicitation done in support of NUREG–1150 (see Ref. B–4, pp. 5–6ff), there is a 53% chance of a RCP seal LOCA of 1000 gpm after 1.5 hours (Table B–2, reproduced from Ref. B–4, Table 5.4–2 gives the results of the expert elicitation process.) It is assumed that the "old" O–rings are in use.

With a 1000 gpm leak, it is estimated that core uncovery will occur in about an additional 2 hours. The basis for this estimate is as follows: According to a report by Fletcher, core uncovery will occur at TMI after a loss of 2.4E5 lbm of water from the primary system.[B–5] For a Westinghouse reactor (Zion), core uncovery will occur after a loss of 3.3E5 lbm of water. It is estimated that the time to core uncovery for a 4–loop Westinghouse reactor with a 1000 gpm RCP seal leak is about 3 hours if credit is given for operator action in depressurizing and cooling down the primary system (the leak rate decreases as the reactor pressure decreases). If it is assumed that the core uncovery time for a given size leak is proportional to the amount of water that must be lost before core uncovery, then, for TMI–1, the time to core uncovery is about 2 hours from the time of the start of the leak. If the leak begins at 1.5 hours after station blackout, then the grace time is about 3.5 hours.

There is an additional probability of 13% that the 1000 gpm leak begins at 2.5 hours according to the discretized distribution for leak rate versus time given by the NUREG–1150 expert elicitation process (see Table B–2). Here the time to core uncovery would be the time (2.5 hours) until the leak starts plus the 2 hours until core uncovery given the leak, or 4.5 hours. Leak rates other than 1000 gpm are of sufficiently low probability or magnitude that they do not contribute significantly to the station blackout core damage frequency. Moreover, the probability of a 1000 gpm leak initiating after 2.5 hours is sufficiently low as to have a negligible contribution to the station blackout core damage frequency.

Table B–1. Failure, maintenance, and repair parameters used in the station blackout requantification

A. Failure data for the diesel generators

q_f = 0.02

q_c = 0.00095

λ_f = 2.5E–3/hr

λ_c = 1.02E–4/hr

Note: The above value of q_f includes a correction to account for the increased failure–to–run rate of the diesel generators during the first hour; a constant value of λ_f is used. The PRA used q_f = 0.0158 per demand, and an increased value of λ_f during the first hour (λ_f = 6.58E–3/hr).

The diesel generator repair time distribution is assumed exponential, but the exponential distribution used is fitted to the median repair time of 8 hours given in NUREG–1032 instead of the mean repair time. The distribution obtained is $Q_f(t) = \exp(-\propto t)$, where $\propto$ = 11.5 hours.

The distribution for repair of a diesel generator failed by common cause is also assumed to be exponential, and is fitted to the distribution given in NUREG/3226, on p. 237. A mean 10–hour repair time is obtained for a diesel generator failed by common cause.

B. Maintenance data

Maintenance unavailability of a diesel generator: 0.0341

For recovery from maintenance, an exponential distribution is assumed:

$$Q_m(t) + \exp(-\propto t), \text{ with } \propto = .05. \qquad (B\text{–}7)$$

This value of $\propto$ fits reasonably well the recovery from maintenance distribution given in NUREG/CR–3226, p. 237, for the pertinent values of t (less than 8 hours or so).

Table B–2. Aggregated RCP seal LOCA probabilities for a Westinghouse four loop plant[a]

Leak Rate (gpm)	Old O–Rings Time (h)					New O–Rings Time (h)				
	1.5	2.5	3.5	4.5	5.5	1.5	3.6	3.5	4.5	5.5
84	0.302	0.286	0.271	0.271(255)	0.271(0.239)[b]	0.810	0.809	0.809	0.807	0.805
244/245[c]	0.148	0.038	0.053	0.051(.067)	0.049(.081)	0.014	0.016	0.017	0.0198	0.020
313	—	—	—	—	—	0.010	0.010	0.010	0.010	0.010
433	0.011	0.012	0.028	9.9E–3	9.3E–3	6.0E–4	6.0E–4	6.0E–4	6.0E–4	6.0E–4
480	1.3E–3	1.3E–3	1.3E–3	1.3E–3	1.3E–3	—	—	—	—	—
543	—	—	—	—	—	2.6E–3	2.6E–3	2.6E–3	2.6E–3	2.6E–3
688/698/728	1.2E–3	1.2E–3	1.1E–3	1.1E–3	0.146	0.146	0.146	0.146	0.146	0.146
796	—	—	—	—	—	2.7E–3	2.7E–3	2.7E–3	2.7E–3	2.7E–3
1000/1026	0.530	0.659	0.659	0.665	0.666	8.3E–3	8.3E–3	8.3E–3	8.3E–3	8.3E–3
1230	1.6E–6	1.6E–3	1.6E–3	1.6E–3	—	—	—	—	—	—
1920	4.2E–3	4.2E–3	4.2E–3	4.2E–3	4.2E–3	4.2E–3	4.2E–3	4.2E–3	4.2E–3	4.2E–3

a. Reproduced from Table 5.4–2 of NUREG/CR–9550, Vol. 2.

b. Parentheses denote calculations which change if no depressurization is assumed. All other probabilities are for depressurized conditions.

c. Similar leak rates have been lumped together.

These values are the probabilities of being at a particular leak rate at a particular time.

The battery depletion time is taken as 6 hours, based on the estimate given in the PRA, Section 4.3, Vol. 6, p. 4–43. According to Ref. B–3, p. 35, severe core damage will occur in a B&W plant about 1 hour after battery depletion. However, no credit is taken here for averting severe core damage by recovering ac power in the time between battery depletion and the onset of severe core damage. As noted on p. 4–32, Vol. 6 of the PRA, battery depletion guarantees core damage. The diesel generators are no longer recoverable because they require dc power. Moreover, the 230 kV substation breakers require dc, even for local operation; hence offsite power may not be recoverable. The grace time is six hours as determined by the battery depletion time if it is not limited to a smaller value by loss of emergency feedwater or reactor coolant pump seal LOCA.

The grace time distribution is as follows:

Grace Time (hrs)	Probability	Result
1	.056	(EFW fails)
3.5	(1–.056)(.53) = .50	(EFW succeeds, 1000 gpm leak at 1.5 hrs)
4.5	(1–.056)(.13) = .12	(EFW succeeds, 1000 gpm leak at 2.5 hrs)
6	.32	(Battery depletion)

Frequency of Losses of Offsite Power Exceeding a Given Duration

The model used for predicting the frequencies of losses of offsite power of a given duration is essentially that described in NUREG–1032, Appendix A, with the parameters for the TMI site supplied by John Flack of the NRC staff in a private communication.[B–2] According to the analysis done in support of the station blackout rule, the site characteristics are as follows (with reference to the model in NUREG–1032):

Switchyard category:	I =	3 (worst category)
Grid stability category:	G =	2
Recovery category:	R =	2 (no enhanced recovery)
Extremely severe weather freq:		0.0016/yr
Severe weather freq:		0.004/yr

NUREG–1032 uses Weibull distributions for the non-recovery curves for loss of offsite power; however, in the actual numerical work performed in support of the station blackout rule, exponentials or linear combinations of exponentials were used. These equations, when specialized to the TMI site using the above categorizations are as follows:

$$i(t) = 0.069(0.7008\exp(-2.002t) + .3063\exp(-0.5072t))$$

$$g(t) = 0.03(0.6886\exp(-1.971t) + .349\exp(-.2903t))$$

$$s(t) = 0.[illegible]4\exp(-0.1983t)$$

$$ss = .0016$$

with the annual frequency of losses of offsite power exceeding a duration t given by

$$F(t) = i(t) + g(t) + s(t) + ss.$$

The terms i(t), g(t), s(t), and ss, respectively correspond to the switchyard, grid, severe weather, and extremely severe weather contributions to the loss of offsite power frequency.

Figure B–1 gives the frequency of losses of offsite power exceeding a duration t, as calculated from the above expressions.

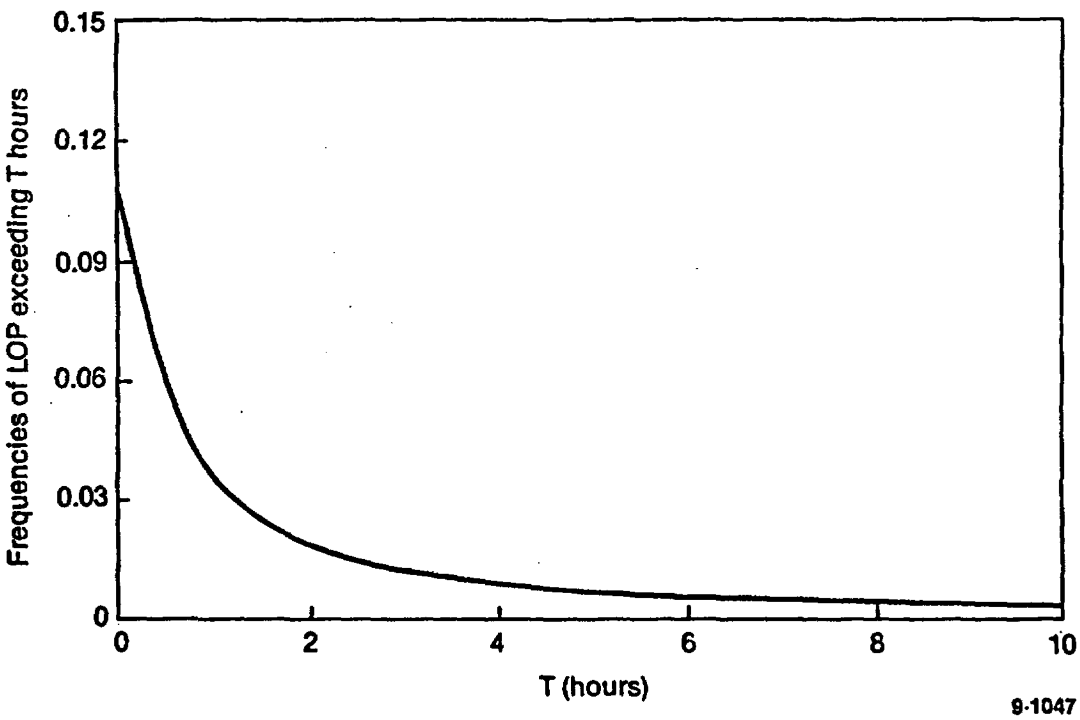

Figure B–1. Annual frequencies of loss of offsite power (LOP) exceeding a time T. (Review Estimates)

Results for the Station Blackout Severe Core Damage Frequency

A station blackout severe core damage frequency of 3E–5/yr is obtained from the above data and equations. The station blackout core damage frequency is calculated conditional on each value of the grace time, and then the weighted sum is taken, with the weights being the probabilities of each grace time. The intermediate results of the severe core damage frequency conditional on each value of the grace time are as follows:

Grace Time (hrs)	Conditional Core Damage Frequency (per year)
1	1.2E–4
3.5	3.3E–5
4.5	2.3E–5
6	1.4E–5

Here conditional core damage frequency is the station blackout severe core damage frequency conditional on the given grace time.

It is interesting to compare the results to those obtained in the PRA. In particular, Section 4.3.5 of volume 6 of the PRA was not understood. This section is entitled "Electric Power Recovery Model." The equation for $\phi_{\text{core melt}}$ in this section was especially confusing. The loss of offsite power frequency, as given in the PRA, was 0.071/yr (see Table 3–8 of Vol. 5 of the PRA). The above model gives 0.106/yr.

The severe core damage frequency due to the loss of offsite power initiator was given as 2.9E–5/yr in Table 6–4, Vol. 3 of the PRA. However, the greatest contribution to this frequency was apparently from nonstation blackout loss of offsite power sequences. Of the top 100 sequences on pgs. 6–46, 6–47, Vol. 3 of the PRA, the core damage frequency from all loss of offsite power sequences was 1.45E–5/yr, while the core damage frequency from the single station blackout sequence (in the top 100 sequences) was 2.8E–6/yr, composing about 19% of the total of all loss of offsite power sequences in the top 100 sequences.

If the sequences below the top 100 contributed negligibly to the station blackout severe core damage frequency, then station blackout would contribute about 3E–6/yr to the severe core damage frequency in the PRA. If the ratio of the contribution of station blackout to the contribution of all loss of offsite power sequences was the same as for the top 100 sequences (that is, 19%), then station blackout would contribute about 6E–6/yr to the severe core damage frequency in the PRA.

The discrepancy, between the estimate in this requantification of 3E–5/yr for the contribution of station blackout to the core damage frequency, and the PRA estimate of about 6E–6/yr, is caused in part by different assumptions on the behavior of the reactor coolant pump seals upon loss of cooling (and seal injection). We estimate a 53% chance of a RCP seal LOCA of 1000 gpm (250 gpm per RCP pump), while the PRA assumes that the leak will be limited to 20 gpm per pump for the first 10 hours of a station blackout (see p. 4–42, Vol. 6 of the PRA). Because of the difficulty in following the PRA analysis of station blackout, it is not known to what extent other differences in assumptions are important.

Taking the 1.2E–5/yr contribution of non–station–blackout loss of offsite power sequences from the PRA top 100 sequences, and multiplying it by the ratio of the estimate of the loss of offsite power initiating event frequency to the PRA estimate, i.e., 0.106/0.071, would result in an estimate of 1.8E–5/yr for the contribution of the nonstation blackout loss of offsite power sequences to the core damage frequency. Adding this figure to the 3E–5/yr estimate of the core damage frequency from station blackout sequences, will result in about 5E–5/yr as an estimate of the core damage frequency from the loss of offsite power initiator. A substantial portion of this value is attributable to the RCP seal LOCA problem. If the seal LOCA problem did not exist, the core damage frequency would be about 3E–5/yr from loss of offsite power.

REFERENCES

B–1. G. Kelly, R. Barrett, and A. Buslik, *Millstone 3 Risk Evaluation Report*, NUREG–1152, June 1986.

B–2. P. W. Baranowsky, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*, NUREG–1032, June 1988.

B–3. A. M. Kolaczkowski and A. C. Payne, Jr., *Station Blackout Accident Analyses*, NUREG/CR–3226, May 1983.

B–4. T. A. Wheeler, S. C. Hora, W. R. Cramond, *Analysis of Core Damage Frequency From Internal Events: Expert Judgement Elicitation*, NUREG/CR–4550, Vol. 2, April 1989.

B–5. C. D. Fletcher, *A Revised Summary of PWR Loss of Offsite Power Calculations*, EGG–CAAD–5553, EG&G Idaho, Inc., September 1981.

APPENDIX C

SEISMIC ANALYSIS

APPENDIX C

SEISMIC ANALYSIS

This appendix estimates the core damage frequency from the seismic initiator and compares it to the estimates given in the PRA. Estimates of the seismic–induced core damage frequency are made with the fragility parameters given in the PRA, and with the seismic hazard curves given in the PRA. The uncertainties due to the uncertainties in the hazard curves are presented.

In addition, estimates with the LLNL hazard curves and EPRI hazard curves are provided.[C-1,C-2] Because the response spectrum estimates and the soil amplification factors are different for the LLNL hazard curves, the fragilities must be modified when the LLNL curves are used.

In this section, the term "probability" is used as the frequentist uses it. This corresponds to the term "frequency" used in the PRA. Here, frequency refers to a time rate, as in the expression "core damage frequency." Probability, as used in the PRA, corresponds to the term degree–of–belief in this section.

Seismic Core Damage Frequencies with the Utility Hazard Curves and Component Fragilities

General Remarks. The seismic core damage frequency is estimated using the utility hazard curves and component fragilities. It will be seen that the seismic–induced core damage frequency estimated here is much higher than that estimated in the PRA. A mean frequency of 6.5E–5/yr is estimated, whereas the PRA estimated 2.7E–6/yr for the seismic–induced core damage frequency; a differential factor of about 24. This difference exists despite the fact that the same hazard curves and component fragility parameters (the median ground acceleration capacities and the logarithmic standard deviations of the capacities) are used here. One reason for this discrepancy is that apparently an error was made in the PRA in the evaluation of the seismic–induced core damage frequency. This error consisted in the neglect of some of the support states, as noted in a letter from GPU to the NRC.[C-3]

The assignment of the dominant sequences to plant damage states also appeared to be in error. In the PRA, the seismically initiated plant damage states 5E and 5F contributed 90% to the seismically–induced core damage frequency. However, plant damage states 5E and 5F (see Table 5–1 of Volume 3 of the PRA) corresponded to late core damage, where the Borated Water Storage Tank (BWST) water accumulated in the reactor building sump before reactor vessel meltthrough. Moreover, these plant damage states were states in which the containment is not intact at the time of core melt initiation. In our analysis, the seismic severe core damage sequences of importance are station blackout sequences, loss of dc sequences, and loss of Nuclear Service River Water sequences. In these sequences, reactor vessel meltthrough occurs without water accumulating in the containment sump. BWST injection never occurs, reactor vessel meltthrough is at high pressure, the containment functions (heat removal and fission product removal) are inoperable, and the containment is intact at the time of core melt. This is plant damage state 3C of Table 5–1, Vol. 3 of the PRA.

Of the sequences contributing most often to plant damage state 5E in the PRA (See table on page A–100, Vol. 3 of the PRA) the top 8 sequences came from the 0.6g seismic initiator. These sequences all involved loss of dc power and failure of the BWST; several of them also involved failure of reactor trip. It is puzzling how such sequences could have been assigned to a plant damage state in which the BWST water is supposed to find its way to the containment sump before reactor vessel meltthrough.

Component Failure Probabilities, for a Given Peak Ground Acceleration

The mean failure probability for a component or structure, for a given horizontal peak ground acceleration a, is given by

$$p(a) = \phi[\ln (a/A_{med})/\beta_c] \qquad (C\text{–}1)$$

where $\phi(z)$ is the distribution function for a normally distributed variable with mean zero and unit variance,

$$\phi(z) = [1/\sqrt{(2\pi)}] \int_{-\infty}^{z} \exp(-t^2/2)dt \quad . \qquad (C\text{–}2)$$

The quantity A_{med} is the median ground acceleration capacity (MGAC) of the component or structure, and β_c is the standard deviation of the logarithm of the ground acceleration capacity, given by

$$\sqrt{(\beta_r^2 + \beta_u^2)} \qquad \text{(C-3)}$$

where

β_r = the logarithmic standard deviation associated with the randomness in the acceleration capacity, and

β_u = the logarithmic standard deviation associated with the uncertainty in the acceleration capacity.

The component failure probabilities, conditional on the peak ground acceleration (pga), are calculated at the four values of the pga (0.15g, 0.25g, 0.4g, and 0.6g) used in the PRA, and compared to those given in the PRA, for the components judged to be important. These components are as follows:

1. Ceramic insulators
2. 4160 V switchgear
3. 480 V switchgear
4. 480 V MCC
5. Battery charger
6. Fuel oil day tank
7. 4160V/480V transformers
8. Diesel generators
9. dc power battery
10. NS river water pumps
11. NSS tank
12. NS heat exchanger.

No significant differences are found. Note that, because the same median ground acceleration capacities and β's are used, this is a check on the computations only.

Conditional Probabilities of Seismic Sequences, given the Peak Ground Acceleration. We select the sequences we consider most likely to be important after inspecting the component failure probabilities conditional on the pga, and after inspecting the list of Boolean expressions given in Table 2-7 of Vol. 7 of the PRA. Although it is possible that an important sequence was missed, the result for the severe core damage frequency is a factor of 24 greater than in the PRA, even though the same component fragilities and hazard curves are used. The sequences considered are:

1. Loss of offsite power, followed by loss of onsite power. The loss of offsite power is event 1 of Table 2-7, Vol. 7, Book 1 of the PRA. The loss of onsite power is event 9 of the same table. Denote this sequence by

   $$E(1) \cdot E(9) \qquad \text{(C-4)}$$

   That is, E(j) denotes event number j in the table referred to above. This notation is used in the discussion of the other sequences. Event E(9) is caused by either loss of the 4160V switchgear, the 480V switchgear, the 480V MCC, the fuel oil day tanks, the 4160V/480V transformers, or the diesel generators.

2. Loss of dc power in conjunction with loss of offsite power. This sequence is $E(1) \cdot E(5)$. The loss of dc power either occurs immediately from failure of the batteries (leading to immediate station blackout) or later from failure of the battery chargers (leading to station blackout later after the batteries discharge, since the diesel generators require dc control power to continue running.) The net result is loss of dc and ac, leading to severe core damage.

3. Loss of nuclear services river water. This is event E(2). Event E(2) is caused by loss of the nuclear service river water pumps, loss of the NSS tank, or loss of the nuclear service heat exchangers.

The calculations of the conditional probabilities of the events E(2), E(5) and E(9), given the pga, involve calculating the probability of a Boolean sum of events. This is done by formulas like the following, where the C_i represent component failure events,

$$\mathrm{pr}\{C_1 + C_2 + C_3 \mid a\} = 1 - (1 - \mathrm{pr}\{C_1 \mid a\})$$

$$(1 - \mathrm{pr}\{C_2 \mid a\})(1 - \mathrm{pr}\{C_3 \mid a\}) \quad . \qquad \text{(C-5)}$$

This type of formula accounts for the overlap between the component failures at high pga's. It assumes, however, that the component failure events are conditionally independent, in the sense that

$$\mathrm{pr}\{C_i \cdot C_j \mid a\} = \mathrm{pr}\{C_i \mid a\} \cdot \mathrm{pr}\{C_j \mid a\} \quad . \qquad \text{(C-6)}$$

If this is not the case, then the formula is conservative.

The results obtained for the conditional probabilities of events E(1), E(2), E(5), and E(9), given the pga, may be compared to those given in Table 2–7, Vol. 7 of the PRA. The only substantial differences occur in event E(2), at 0.6g, and in event E(5) at 0.4g. The conditional probability of event E(2), the loss of nuclear services river water, given a pga of 0.6g, is 0.74, according to these calculations, while it was 0.94 in the PRA. The conditional probability of E(5), given a pga of 0.4g, is 0.426, according to these calculations, while it was 0.185 in the PRA. It is easy to see, without calculation, that the value for the conditional probability of E(5), given a pga of 0.4g, was incorrect in the PRA. This event referred to failure of dc caused by either failure of the battery chargers or the batteries. However, the battery chargers, according to Table 2–5 of Vol. 7 of the PRA, have a 32.4% chance of failing at 0.4g; therefore the probability of E(5) must be at least as great, at this pga, and must be greater than the 18.5% given in the PRA. The error in the probability of E(2), given a pga of 0.6g, is probably not important, since at such a large pga there is a high probability of core damage from other failures. The error in E(5) could possibly have some effect, but not nearly enough to account for the differences in the estimates of seismically–induced severe core damage between our results and the results given in the PRA.

Once the probabilities of the events E(i) are calculated, conditional on the pga, the following quantities are calculated:

$$\Pr\{S1 \mid a\} = \mathrm{pr}\{E(1) \mid a\} \cdot \mathrm{pr}\{E(9) \mid a\}$$

$$\Pr\{S2 \mid a\} = \mathrm{pr}\{E(1) \mid a\} \cdot \mathrm{pr}\{E(5) \mid a\}$$

$$\Pr\{S3 \mid a\} = \mathrm{pr}\{E(2) \mid a\} \qquad \text{(C-7)}$$

Here S1 represents the station blackout sequence, S2 the loss of dc sequence (either immediately by loss of the batteries or later because of loss of the battery chargers), and S3 represents the loss of nuclear service river water. The core damage event is given by the Boolean sum of these 3 sequences, since the contributions of all other sequences to the seismically–induced core damage frequency are being neglected. Overlap between the sequences is accounted for as follows:

$$\mathrm{pr}\{S1 + S2 \mid a\} = \mathrm{pr}\{E(1) \mid a\} \cdot (\mathrm{pr}\{E(5) \mid a\} + \mathrm{pr}\{E(9) \mid a\} - \mathrm{pr}\{E(5) \mid a\} \cdot \mathrm{pr}\{E(9) \mid a\})$$

$$\mathrm{pr}\{S1 + S2 + S3 \mid a\} = \mathrm{pr}\{S1 + S2 \mid a\} + \mathrm{pr}\{S3 \mid a\} - \mathrm{pr}\{S1 + S2 \mid a\}\mathrm{pr}\{S3 \mid a\} \quad \text{(C-8)}$$

The quantity $\mathrm{pr}\{S1 + S2 + S3 \mid a\}$ is the conditional probability of core damage given a pga of a. When considered as a function of a, it is sometimes called the plant fragility curve. The mean plant fragility curve is displayed in Figure C–1. One sees that there is about a 50% chance of core damage, given a pga of 0.36g. Since the Safe Shutdown Earthquake (SSE) corresponds to 0.12g for the pga, there is a 50% chance of core damage at about 3 times the SSE pga. Typically the 50% point on the plant fragility curve is between twice the SSE and four times the SSE, so the results for TMI are not unusual.

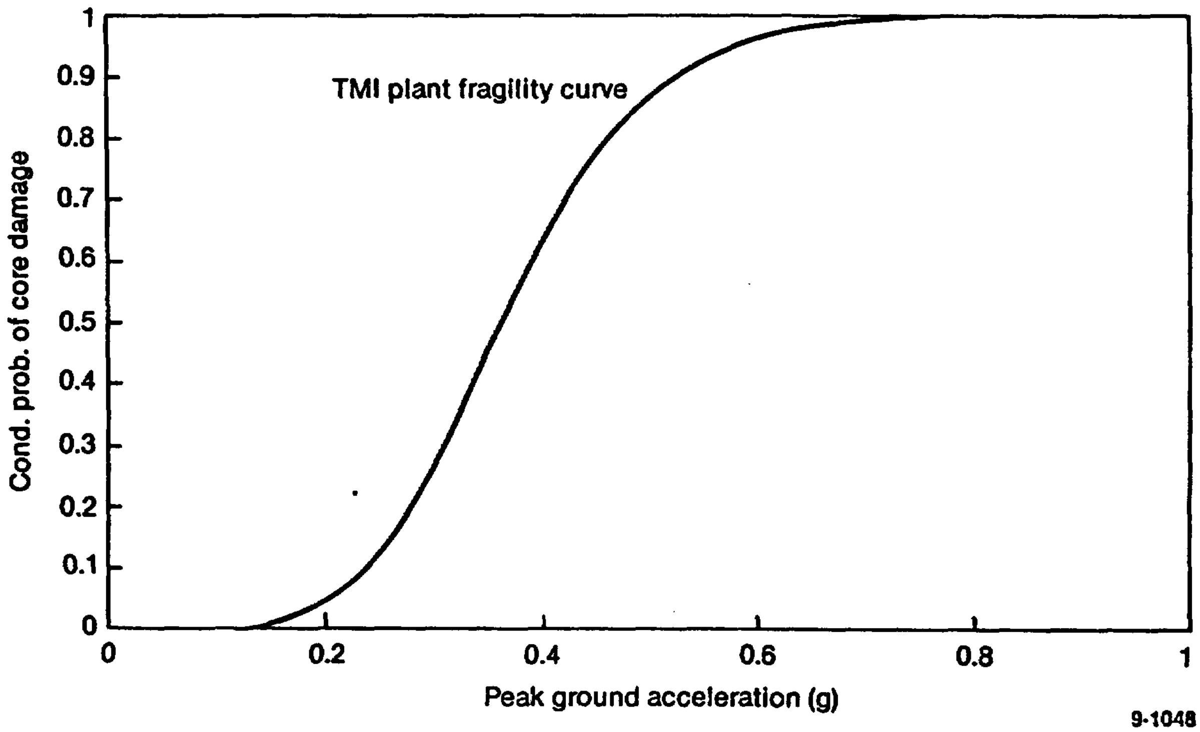

Figure C-1. TMI plant fragility curve.

Combining the Conditional Sequence Probabilities and the Hazard Curve. If, based on the mean hazard curve, g(a)da is defined as the probability that the pga lies in the interval da about a, then the mean frequency of core damage from the sequences S1, S2, and S3 is

$$f_{seismic} = \int pr\{S1 + S2 + S3 \mid a\}g(a)da \quad . \qquad \text{(C-9)}$$

This integral is approximated by a sum, in the same way as was done in the PRA. A small error was made in the PRA, which is not corrected in our review. The four ranges in the pga are:

0.1g<a<0.2g

0.2g<a<0.3g

0.3g<a<0.5g

0.5g<a

The typical values of a used, in each of these ranges, for evaluating the conditional probabilities of failures, are, respectively, 0.15g, 0.25g, 0.4g, and 0.6g.

The PRA should have used the integral of g(a) from 0.5g to infinity for the last range. The value of the mean acceleration frequency for the range 0.5g<a should be 6.8E-6/yr, while Table 2-1, Vol. 7 of the PRA gives 5.6E-6/yr. The error has quite a small effect on the review results. (A correction for this error would be, to a good approximation, an increase in the seismic-induced core damage frequency by the difference of these two mean acceleration frequencies, or 1.2E-6/yr; the reason for this is that the probability of seismically-induced core damage is close to unity, given a pga of 0.6g, using the component fragilities in the PRA for TMI.)

The results obtained in this review are:

$$pr\{S1\} = \int pr\{S1 \mid a\}g(a)da = 2.3E\text{-}5/y \text{(station blackout)}$$

$$pr\{S2\} = \int pr\{S2 \mid a\}g(a)da = 3.2E{-}5/yr$$

(loss of dc)

$$pr\{S3\} = \int pr\{S3 \mid a\}g(a)da = 3.1E{-}5/yr$$ (loss of NS river water)

and the seismic induced core damage frequency, pr{S1+S2+S3}, is 6.5E–5/yr. (It is to be recalled that, because of overlap, pr{S1+S2+S3|a} is not equal to the sum of the pr{Sj|a}, j = 1,2,3).

The value obtained for the mean seismically–induced core damage frequency is some 24 times greater than the value of 2.7E–6/yr given in the PRA, despite the fact that the same component fragility parameters and hazard curves are used.

Uncertainty due to the Hazard Curves using the Utility Hazard Curves. The PRA (see Table 4, Appendix A of Vol. 7) gives a family of hazard curves, each with a different degree–of–belief weight assigned. Each member of the family is really an aggregate of a set of hazard curves. By considering the variation of the seismic–induced core damage frequency over this ensemble of hazard curves, one can generate a degree–of–belief, or uncertainty distribution, for the seismic–induced core damage frequency. Of course, this uncertainty distribution includes only the uncertainty due to the uncertainty in the hazard function, and not that due to the uncertainty in the median ground acceleration capacities of the components and structures. In addition, although this uncertainty distribution is appropriate for the authors of the PRA, other analysts may decide that the hazard curves of other experts should be included in the assessment of the uncertainty. Nevertheless, it is of interest to determine the uncertainty in the seismic core melt frequency caused by the uncertainty in the hazard curves, using the uncertainty distribution for the hazard given in the PRA. Each hazard curve generates a density function; the density function g(a) is the negative derivative of the hazard curve, since the hazard curve H(a) gives the annual probability that the pga exceeds a. If $g_i(a)$ is the density function for the ith hazard curve, and if w_i is the degree–of–belief weight assigned to it, then the seismic core melt frequency calculated from

$$f_i = \int pr\{cd \mid a\}g_i(a)da \tag{C-10}$$

has degree–of–belief weight w_i. In this way one finds the following table of seismic–induced core–melt frequencies and associated weights:

Curve No.	Weight	CDF	Cumumative Weight
10	0.047	2.66E–04	1
9	0.074	1.16E–04	0.953
7	0.147	1.10E–04	0.879
2	0.033	5.44E–05	0.732
3	0.138	5.22E–05	0.699
6	0.052	4.46E–05	0.561
5	0.182	4.35E–05	0.509
4	0.141	3.71E–05	0.327
8	0.086	2.48E–05	0.186
1	0.1	2.34E–05	0.1

In this table, the curve number corresponds to the curve number of the aggregate hazard curve in Table 4, Appendix A, Vol. 7 of the PRA. The weight is the corresponding weight from this table. The column heading CDF represents the seismic–induced core damage frequency; the curves are ordered such that the CDF's are in descending order of magnitude. From the above table one sees that the 95.3 percentile on the uncertainty distribution corresponds to a seismic CDF of 1.16E–4/yr. The median value of the seismic cdf is about 4.3E–5/yr, and the mean value is about 6.5E–5/yr.

Qualitative Discussion of the Uncertainties in the Fragilities. In the PRA, the fragility parameters for many of the components were based on generic data. This introduced greater uncertainty. Also, the fragility parameters obtained from generic data were treated conservatively. This is appropriate for an initial screening analysis, but for components which are identified as important contributors to the seismic core damage frequency, a plant–specific analysis should be done. In particular, the battery chargers, with a relatively low median ground acceleration capacity of 0.48g, contributed significantly to the seismic core damage frequency, and a plant–specific analysis would be appropriate. If the battery chargers were so strong that they would never fail, the mean seismic core damage frequency would change from 6.5E–5/yr to 4.8E–5/yr. If the fragility parameters of the battery chargers and the ceramic insulators are kept the same, and all other components strengthened to the point that they would never fail, then the mean seismic core damage frequency would be 2.9E–5/yr.

Of the components entering into the important seismic sequences, only the nuclear service river water pumps and the fuel oil day tank were treated by plant-specific calculations in the PRA.

Loss of coolant accidents from seismically–induced pipe breaks were not important contributors to core damage in this PRA, as in most utility–sponsored PRAs. However, PRAs performed using the Seismic Safety Margins Research Program (SSMRP) methodology have estimated much higher conditional probabilities of small LOCAs at a given level of peak ground acceleration. For example, at Zion, according to Ref. C–4, Table 7.3, there is a 26% chance of a small LOCA due to a pipe break, at a pga of 0.37g. We note further that the SSE pga for Zion is 0.17g, while it is 0.12g at Three Mile Island.

The lack of inclusion, even in a generic way, of design and construction errors in the assessment of the fragilities, was another source of uncertainty. The most important uncertainty in the fragilities is judged to be the use of generic data.

Uncertainties in the Accident Sequence Delineation. Relay chatter was assumed to be completely recoverable. This assumption should be investigated further. If this assumption were removed, greater detail in the accident sequence delineation would be required.

The accident sequences considered were those judged to be most important. The error associated with lack of completeness is believed to be small.

Insights. The fuel oil day tank was treated by a plant specific analysis, and contributed significantly to the seismic severe core damage frequency. If the fuel oil day tank were so strong it would never fail, but all other fragilities remained the same, the mean seismic core damage frequency would change from 6.5E–5/yr to 6.1E–5/yr. If the fragility parameters for the ceramic insulators and the fuel oil day tank were kept the same, but all other components strengthened to the point where they would never fail, the seismic severe core damage frequency would be 1.2E–5/yr. According to the PRA (see p. 5–45, Vol. 7, Book 2, of the PRA), the fuel oil day tank had no seismic design and contained no anchorage between the concrete saddles and the tank.

If the fragility parameters of the nuclear service river water pumps were kept the same, but all other components strengthened to the point where they would never fail, then the mean seismic core damage frequency would be 1.9E–5/yr.

Seismic Core Damage Frequencies with the LLNL Hazard Curves

General Remarks. Since the completion of the TMI PRA, results of the Eastern Seismicity Characterization Program at LLNL[C–1] and a parallel program conducted by EPRI[C–2] have become available. These results include site–specific probabilistic hazard estimates and site–specific uniform hazard spectra. The hazard estimates and spectral shapes of the LLNL study, the EPRI study, and the TMI PRA, all differ from each other. We will therefore estimate the sensitivity of the seismically–induced core damage frequency to the LLNL hazard curves and spectral shapes, and later to the EPRI hazard curves. The results of the hazard studies influence the fragilities in two ways: through a soil amplification factor, and through a spectral shape factor.

Soil Amplification Factor. Except for the diesel generator (DG) building, the borated water storage tank (BWST), the condensate storage tank (CST), and the underground fuel oil day tank, all TMI structures are founded on bedrock. The DG building, BWST, and CST are on compacted backfill which is approximately 30' thick over bedrock. In the TMI PRA analysis, the seismic hazard was defined with respect to bedrock and a soil amplification factor was included in the fragility analysis to account for the acceleration experienced at the top of the bedrock. In the LLNL program, hazard estimates are provided for both the bedrock condition and the surface condition. Therefore, the first issue is to examine whether the soil amplification factor used in the TMI analysis was consistent with the information developed by LLNL. LLNL, in Ref. C–1, provided approximate estimates of the following ratios of PGA values between shallow and rock conditions for fixed values of the hazard (annual exceedance probability):

	Ratio Shallow/Rock PGA			
Probability of Exceedance (per year)	10^{-3}	10^{-4}	10^{-5}	Avg.
	1.50	1.47	1.44	1.47

The amplification factor used in the TMI analysis was 1.2. Implications of this difference, along with other differences, are discussed below.

Spectral Shape Issues. The uniform hazard spectra (UHS) developed in the LLNL and EPRI programs exhibit significantly different characteristics than the median spectral shapes used in the TMI analysis. The LLNL spectra are significantly lower than the TMI median spectra below approximately 10 Hz, and higher at high frequencies. Spectral accelerations are amplified even at frequencies of 50 Hz or greater in the LLNL results, while PGA values are approached at 20 Hz in the TMI spectra. One should be cautioned that there are a number of issues yet to be resolved in using uniform hazard spectra in the probabilistic risk analysis. Further investigations are needed to properly characterize the damage potential of a ground motion which is rich in high frequencies but less rich in low frequencies. Issues associated with uncertainty estimates require further examination. The following table lists the ratio of amplification factor (value of spectral acceleration at given frequency to PGA) used in the TMI median spectrum to the amplification factor of the median LLNL rock spectrum for a 10^{-4} return period:

Frequency,Hz	$\text{Ratio} = \dfrac{\text{TMI Amplification Factor}}{10^{-4}\ \text{LLNL UHS Amplification Factor}}$
1.0	3.0
2.0	2.36
2.5	2.55
3.33	2.1
5.0	1.7
10.0	1.0
20.0	0.6

If specific fragility calculations for component and structures, or information on natural frequencies of TMI structures, were available, then one could make better judgments about the impact of different spectral shapes on the fragility estimates. This information was requested but has not been received.

In the absence of the needed information, to gain qualitative insights, it can be assumed that the stiff nuclear structures founded on the bedrock will not have natural frequencies below 5 Hz and frequencies will be in the range of 5–10 Hz. Examining the above table, in the frequency range of 5–10 Hz, the TMI spectrum shape overpredicts the response for a given PGA by approximately 0% to 70%. For a sensitivity analysis, an arbitrary value of 1.5 is selected. It should be noted that in the TMI analysis, the spectral shape factor (or structural response factor in component fragility evaluations) used in calculations was 1.0 since the median spectrum was used in the response analysis. This factor should be changed in the sensitivity analysis as discussed above when the plant–specific fragility estimates are used.

Ideally, one should also evaluate uncertainty parameters (β_u and β_r) associated with the spectrum shape factor; however, it is very difficult in a short amount of time to sort out the partitioning of uncertainties in the hazard estimates and uniform hazard spectra estimates provided by the LLNL. Therefore, in this order of magnitude sensitivity analysis, the TMI β_u and β_r values are retained.

Reestimation of Some Fragilities. Three specific fragilities were reexamined in this effort. Two components are surface mounted (the DG building and the BWST), and the other component (the Nuclear Service River Water Pump) is one for which a plant–specific fragility was developed as part of the PRA, and which was found to be risk–significant in the PRA.

The approach used was to derive qualitatively– and judgmentally–determined median factors of safety for soil amplification, spectral shape, and peak ground velocity values, and requantify fragility values for the above components. No requantification of uncertainty values is made. It must be emphasized that detailed or specific calculations were not available.

Of the above three components, only the Nuclear Service River Water Pump is found to be an important contributor. The fragility parameters for the fuel oil day tank, for which a plant–specific analysis was performed for the PRA, should also be revised. However, the calculations performed for the PRA were not available.

For the nuclear service river water pump, the structural response factor is revised to 1.5 from 1.0, leading to an increase in the MGAC to 1.02g from 0.68g. Note that a detailed evaluation of this component has not been made with regard to the other failure modes and the adequacy of the parameter values used in the analysis.

There is the potential for the MGAC to be decreased significantly for certain components. One reason for this is the soil amplification factor discussed earlier. Another reason is that, for component natural frequencies greater than about 10 Hz, the spectral amplification factor (ratio of the spectral acceleration at a given frequency to the PGA) will be larger than assumed in the PRA, further reducing the MGAC. For example, diesel generators generally have natural frequencies in the neighborhood of 20 Hz, as may be seen from Table 5.2 of NUREG/CR-3428.[C-4] Further support for this value is supplied by the Long-Term Seismic Program Diablo Canyon PRA,[C-5] where the diesel generator natural frequency is estimated to be about 17 Hz. For a frequency of about 20 Hz, the spectral amplification factor obtained from the LLNL program is about 1.6 times that assumed in the PRA. Since the diesel generator building is on soil, there is the additional reduction coming from the soil amplification factor. The two factors together would yield a reduction of the MGAC by a factor of about (1.6)(1.47/1.2), or a factor of about 2. Since at present the MGAC for the diesel generators is about 0.75, this would result in a revised MGAC of about 0.38, if straightforward modifications to the median safety factors are made. Further investigations are needed to properly characterize the damage potential of high frequency ground motion. The precise impact of such high frequency motion on component fragilities is not clear. In any event, because the fragility parameters in the PRA are not plant specific, it does not appear appropriate to make this correction. It would be more desirable to do a plant specific fragility analysis for the diesel generators, with all factors affecting the diesel generator seismic capacity considered in a plant specific way.

The important implications for the stiff components of nuclear power plants of the spectral amplification factor obtained from the LLNL program is noted in the LLNL report (see p. 47, Vol. 6, of Ref. C-1).

LLNL Hazard Curves. The LLNL mean hazard curve (see Ref. C-1, Vol. 2, p. 211) is given by the table:

PGA	H
5.00E-02	1.37E-02
7.55E-02	7.20E-03
1.26E-01	2.88E-03
2.00E-01	1.11E-03
2.50E-01	6.83E-04
4.00E-01	2.28E-04
5.61E-01	9.82E-05
6.12E-01	7.85E-05
7.65E-01	4.37E-05
1.00E+00	2.11E-05

Here the column labelled PGA is the perk ground acceleration in g's; the column labelled H gives the mean hazard curve, or mean annual probability of exceedance of PGA. The LLNL mean hazard curve is considerably higher than the mean hazard curve in the PRA. For example, at 0.4g the mean exceedance frequency is 1.8E-5/yr, from the data in Volume 7, Appendix A, Table 4 of the PRA, while it is 2.28E-4/yr from the LLNL mean hazard curve, more than an order of magnitude different.

Results with the LLNL Hazard Curves. Two calculations were performed with the LLNL hazard curves. First, the seismic core damage frequency is calculated with the same fragility parameters as in the PRA. Secondly, the seismic core damage frequency is calculated with the increased MGAC for the NS river water pumps derived above. We estimated above that the MGAC for the NS river water pumps should be 1.02g, instead of 0.68g, when the LLNL hazard curves and spectral shapes are used. Because there are other important components contributing to the seismic core damage frequency, there is not much effect from this change. With the same fragility parameters for the NS river water pumps as in the PRA, the mean seismic core damage frequency is calculated as 4.3E-4/yr, while with the modified fragility parameters for the NS river water pumps it is 3.8E-4/yr. For comparison, the seismic core damage frequency with the utility hazard curves was calculated as 6.5E-5/yr, so that the LLNL results are a factor of about 7 higher.

Seismic Core Damage Frequencies with the EPRI Curves

The mean hazard curve for the EPRI study for the TMI site is given by the following table:

PGA	H
0.510E-02	0.640E-02
0.510E-01	0.510E-03
0.102E+00	0.170E-03
0.255E+00	0.260E-04
0.510E+00	0.380E-05
0.714E+00	0.120E-05

The column labelled PGA gives the peak ground acceleration in g's. The column labelled H gives the corresponding values of the mean hazard function, or annual probability of exceedance of the corresponding value of PGA. This hazard curve lies below the mean hazard curve of the utility. For example, at 0.5g the utility hazard curve has the value 6.8E-6/yr, while the above table gives 3.8E-6/yr.

For the EPRI hazard curves, all that was done was to calculate the mean seismic core damage frequency using the mean EPRI hazard curve and the structure/component fragilities given in the PRA. The seismic core damage frequency obtained is 1.74E–5/yr. The uniform hazard spectra generated in the EPRI program are similar to the LLNL uniform hazard spectra but indicate a smaller spectral amplification factor for all frequencies. The estimate of 1.74E–5/yr for the seismic core damage frequency does not include any changes in spectral response factors from those used in the TMI PRA. If, as in the case of the LLNL hazard, only the MGAC of the nuclear service river water pumps is changed, not much change in the seismic core damage frequency would be expected.

Summary

The estimate of the mean seismic core damage frequency is 6.5E–5/yr when the PRA hazard curves and component/structure fragility parameters are used. This is a factor of 24 greater than the value of 2.7E–6/yr given in the PRA. One reason for this is that the PRA omitted the contribution of some plant damage states, as is noted in the letter from GPU to the NRC.[C–3] There may be other reasons. The assignment to plant damage states in the PRA also appears incorrect.

Only a few of the component and structure fragility parameters are based on plant–specific fragility analyses. It would be highly desirable to use plant–specific fragilities.

The 95th percentile core damage frequency is 1.2E–4/yr, when only the uncertainty in the hazard is considered and the utility hazard curves are used. When the LLNL hazard curves are used, a mean seismic core damage frequency of 3.8E–4/yr is obtained with the NS river water pump fragilities modified to account for the response spectrum shape obtained in the LLNL study. This value of 3.8E–4/yr falls outside the 95th percentile bound obtained when the PRA hazard curves are used. When the EPRI hazard curves are used, a value of 1.74E–5/yr is obtained for the mean seismic core damage frequency. This value is below the 10th percentile value of 2.3E–5/yr obtained from the utility hazard curves.

REFERENCES

C–1. D.L. Bernreuter, J.B. Savy, R.W. Mensing, and J.C. Chen, *Seismic Hazard Characterization of 69 Nuclear Plant Sites East of the Rocky Mountains*, NUREG/CR–5250, January 1989.

C–2. R. K. McGuire et al., *Probabilistic Seismic Hazard Evaluations in the Central and Eastern United States: Results for 57 Sites*, Project P101–53, Final Report, Electric Power Research Institute, Appendix E to EPRI NP–6395–D, April 1989.

C–3. Letter from H. D. Hukill to U. S. Nuclear Regulatory Commission, GPU letter no. C311–89–2020, GPU Nuclear Corporation, March 17, 1989.

C–4. M. P. Bohn et al., *Application of the SSMRP Methodology to the Seismic Risk at the Zion Nuclear Power Plant*, NUREG/CR–3428, January 1984.

C–5. *Long–Term Seismic Program Diablo Canyon PRA*, Pacific Gas & Electric Co., March 1988.

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

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

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

NUREG/CR-5457
EGG-2572

2. TITLE AND SUBTITLE

A Review of the Three Mile Island-1 Probabilistic Risk Assessment

3. DATE REPORT PUBLISHED

MONTH	YEAR
November	1989

4. FIN OR GRANT NUMBER

A6892

5. AUTHOR(S)

H.J. Reilly, D.L. Schurman, H.J. Welland, R.C. Bertucio, S.A. Eide, P.R. Davis, S.E. Mays, A.J. Buslik, N.C. Chokshi

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

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

Idaho National Engineering Laboratory
EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, ID 83415

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

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

The Level 1 Probabilistic Risk Assessment that was prepared by Pickard, Lowe and Garrick for GPU Nuclear, and forwarded to NRC, was reviewed. The review included both plant internal events and three kinds of external events: plant fires, seismic events and river flooding. At the close of the review, the authors estimated the frequencies the core damage sequences would have if the recommended corrections were made to the data and assumptions. It was concluded that the recommended corrections would have a major effect on the estimated risk profile of TMI–1, including major increases in some sequence frequencies and major decreases in others.

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

Probabilistic Risk Assessment (PRA)
Three Mile Island-1

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

NRC FORM 335 (2-89)

*U.S.GOVERNMENT PRINTING OFFICE:1989-262-436:00353