NUREG/CR-6042
SAND93-0971

Perspectives on Reactor Safety

Prepared by
F. E. Haskin/UNM
A. L. Camp/SNL

Chemical and Nuclear Engineering Department
University of New Mexico

Sandia National Laboratory
Operated by
Sandia Corporation

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 20555-0001

2. The Superintendent of Documents, U.S. Government Printing Office, Mail Stop SSOP, Washington, DC 20402-9328

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 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, international agreement reports, grant publications, 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 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 Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

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, for 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-6042
SAND93-0971

Perspectives on Reactor Safety

Manuscript Completed: February 1994
Date Published: March 1994

Prepared by
F. E. Haskin, University of New Mexico
A. L. Camp, Sandia National Laboratories

Chemical and Nuclear Engineering Department
209 Farris Engineering Center
University of New Mexico
Albuquerque, NM 87131

Under Contract To: Sandia National Laboratories
Albuquerque, NM 87185

Prepared for
Division of Safety Issue Resolution
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC FIN L1914

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) maintains a technical training center at Chattanooga, Tennessee to provide appropriate training to both new and experienced NRC employees. This document describes a one-week course in reactor safety concepts. The course consists of five modules: (1) historical perspective; (2) accident sequences; (3) accident progression in the reactor vessel; (4) containment characteristics and design bases; and (5) source terms and offsite consequences. The course text is accompanied by slides and videos during the actual presentation of the course.

TABLE OF CONTENTS

FOREWORD

The USNRC maintains a technical training center (TTC) at Chattanooga, Tennessee. This TTC is responsible for training and, in part, qualification programs for new employees and, at times, for retraining. Inasmuch as the agency hires about 150 new technical staff per year (due to turnover from retirement or other losses) there is a need to train these new employees for their NRC role. The entering staff have varied backgrounds: fresh from college or university; from Naval Reactors programs; from private industry. In all cases there are some training needs. However, the NRC must cope, in its training programs, with the nationwide deemphasis in nuclear power in the universities. Thus, we see in the incoming interns educational background in other areas, such as chemical or electrical engineering, or else degrees in mathematics or physics or chemistry. This shift in emphasis has placed an added burden on the TTC. In particular, it is seen that the most fundamental concepts in reactor safety, are not readily available to the college student as formal courses. Further, many of the present employees have not had the benefit of formal training in the bases for many of the regulations dealing with fundamental safety concepts. In this sense, fundamental concepts include: the design basis loss of coolant accident; the core melt assumptions which are embedded into the siting policy (Part 100); core melt progression and fission product release; fission product inventories and biological effects; atmospheric diffusion and transport; offsite effects; and, historical aspects of important rules such as station blackout.

This one-week course was developed to fill the gap in understanding of reactor safety concepts. It started with an expression of need from the Director of AEOD to the Director of Research, in the fall of 1990. The Research office engaged Sandia National Laboratories to develop much of the work contained herein. Sandia in turn engaged Professor Eric Haskin of the University of New Mexico who worked with Dr. Allen Camp at Sandia as the principal developers. Over the last two years the course material has been developed, refined, discussed, and is now ready for trial use. It consists of five modules: 1) historical perspective; 2) accident sequence; 3) accident progression in the reactor vessel; 4) containment characteristics and design bases; and 5) source terms and offsite factors. Presentation slides have been developed, but are not included in this text, although copies will be available for the course attendees. Several videos will be shown on topics of the developing accident sequences, with scale model examples from the severe accident research program at Sandia. A video on the Three Mile Island event will be shown. Hand calculations on various accident phenomena (such as core heat up time) will be emphasized. Although most TTC training courses culminate with a written examination, this Reactor Safety course does not have exams.

Comments or criticisms on the enclosed training material are welcome and solicited. We hope to improve and refine the material and plan to issue a revision in 1995, on the basis of your comments and experience with the first few course deliveries. We also plan to make this document available abroad to interested countries and, as is usual at TTC, expect a few foreign attendees at this course.

Please direct your comments to the undersigned,

Denwood Ross,
Deputy Director
AEOD

ACKNOWLEDGEMENTS

This course covers an extremely wide range of topics. Developing this material required input from numerous people at the NRC and elsewhere. In particular, we would like to thank Dr. Denwood Ross, whose breadth and depth of knowledge concerning the history of reactor safety was invaluable. Additional information and program guidance was provided by Mark Cunningham and Lee Abramson of the NRC PRA branch. Other key NRC reviewers included Ken Raglin, Len Reidinger, Larry Bell, Eric Beckjord, Warren Minners, Jocelyn Mitchell, and Tom McKenna.

At Sandia, information and insights were provided by Walt von Riesemann, Dana Powers, Susan Dingman, and Fred Harper. Steve Hodge at Oak Ridge National Laboratory also provided an excellent review of the material. Finally, we wish to acknowledge the support of Darla Tyree, Emily Preston, and Ellen Walroth in the preparation of this document.

English to Metric
Conversion Factors

English	Metric
1 Foot	.3048 meters
1 Mile	1.6093 kilometers
1 $ft.^2$	.0929 m^2
1 gallon	3.785×10^{-3} m^3
1 $ft.^3$	.02832 m^3
1 lbm	.4536 kg.
1 lbf	4.44822 Newtons
1 psi	6895 pascals
1 Btu	1055 Joules
1 Btu/hr.	.2931 watts
1 Btu/hr-ft^2	3.155 watts/m^2

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF TABLES

Table

LIST OF ILLUSTRATIONS

Figure

1.0 HISTORICAL PERSPECTIVE

1.0.1 Introduction

Of all modern technologies, the highest potential for catastrophe in the public's mind is probably associated with nuclear power. The awesome destructive power of nuclear weapons provides reason for some to fear all things that utilize nuclear energy or emit radiation. The accidents at Three Mile Island (TMI) and Chernobyl strongly reinforced intuitive public concerns about nuclear power. In the U.S., the potential hazards of nuclear power were recognized very early, and some features to prevent, contain, and otherwise protect the public from reactor accidents were applied from the outset.

U.S. safety strategies evolved with successive generations of larger capacity plants, and many additional safety features were introduced. It is true that U.S. plants are inherently safer than plants like Chernobyl. It is also true that single accidents in other industries have killed and injured far more people than Chernobyl. However, such arguments are not likely to alter the public perceptions of the hazards of nuclear power. More importantly, no argument can change the actual hazard -- the core inventories of radionuclides. Whether one's objective is to make nuclear power plants safer or to change public perceptions of their safety, in the long run, the attitude recommended for the nuclear industry by the President's Commission on TMI-2 seems most likely to succeed:

> *"Nuclear power is by its very nature potentially dangerous, and ... one must continually question whether the safeguards already in place are sufficient to prevent major accidents."*[1]

This course presents both historical and technical information required to support such an attitude.

Figure 1.0-1 depicts the timing of major events and activities relevant to commercial power reactor safety from the 1940s to the present. A brief history of developments significant to the U.S. regulatory process is presented in this module to provide a framework for the course materials that follow. Trends and events are discussed in roughly the chronological order in which they became significant. Historical perspective is also provided, where appropriate, in subsequent modules. Several references discuss additional relevant history.[2,3,4,5,6,7,8,9]

1.0.2 Learning Objectives for Module 1

At the end of this module, the student should be able to:

1. Describe the principal elements of the defense-in-depth strategy.

2. Describe the legal basis of NRC's regulatory process including the content and impact of:

   a. The Atomic Energy Acts of 1946 and 1954
   b. Price-Anderson Act
   c. The National Environmental Policy Act of 1969
   d. The Energy Reorganization Act of 1974

3. Describe the content of some key elements of NRC's regulations and regulatory process, including:

   a. General Design Criteria (10 CFR 50 Appendix A,)
   b. Emergency Core Cooling System Acceptance Criteria (10 CFR 50.46 and Appendix K)
   c. Backfit Rule (10 CFR 50.109)
   d. Siting Criteria (10 CFR 100)

4. Describe the changes in the following areas resulting from the TMI-2 accident:

   a. NRC Structure
   b. Nuclear Industry Structure
   c. Plants
   d. Operator Training
   e. Emergency Response
   f. Severe Accident Research

5. Explain the basis and content of some key elements of NRC's policies and practices with respect to severe accidents, including:

   a. Severe Accident Policy Statement
   b. Safety Goal Policy Statement
   c. Individual Plant Examination Process

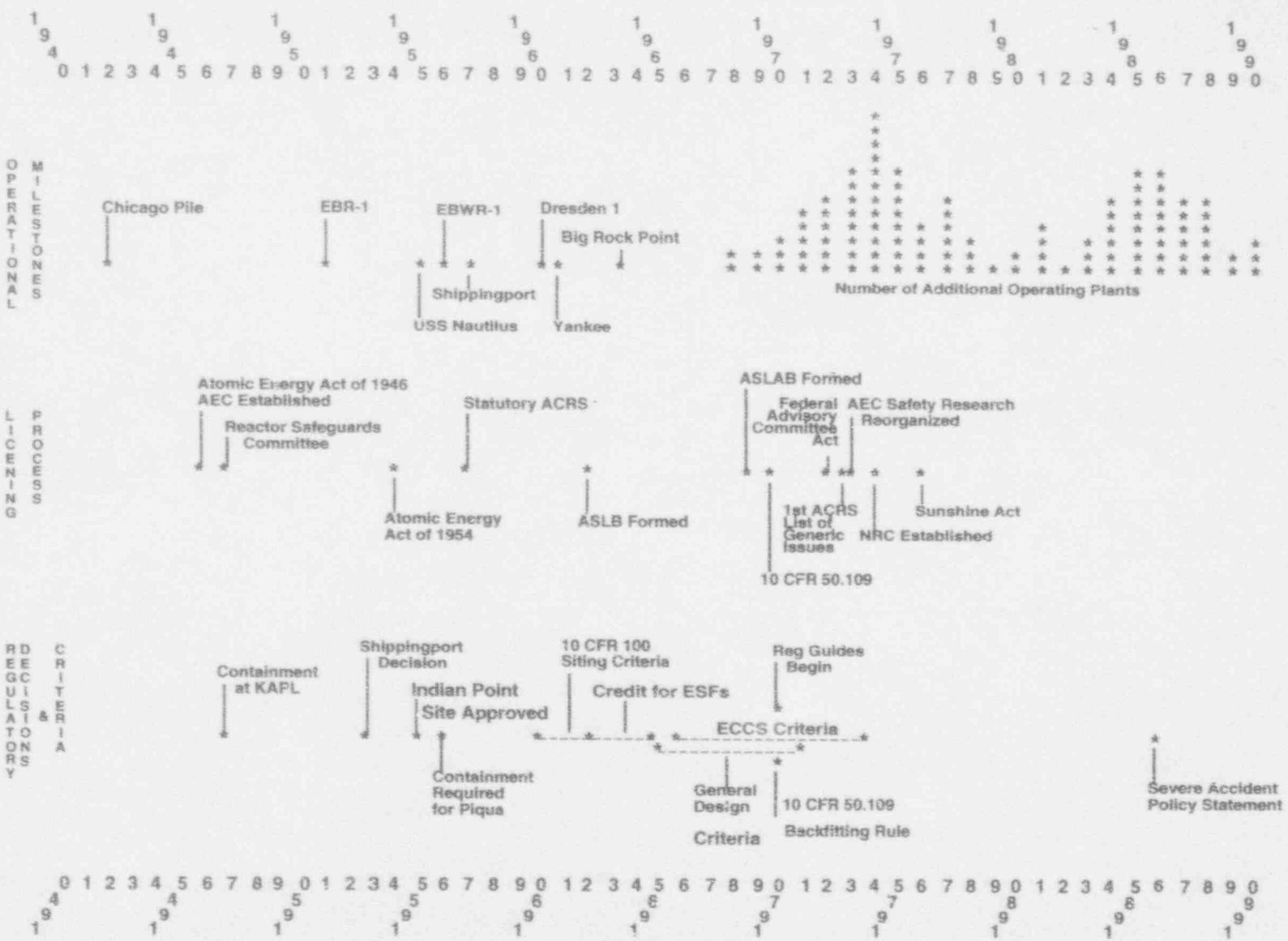


Figure 1.0-1 Timing of major events and activities relevant to commercial power reactor safety from 1940's to present (1 of 2)

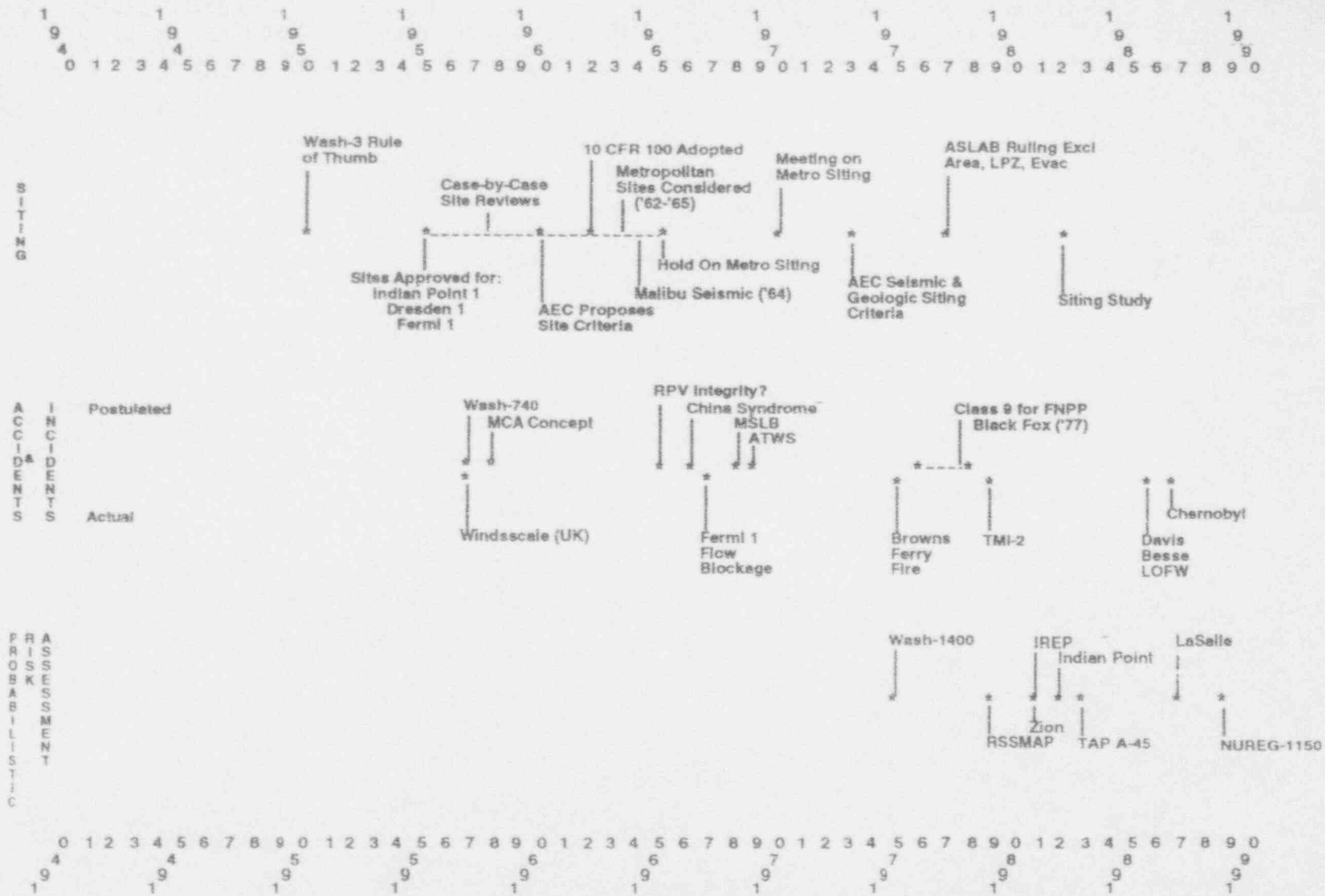


Figure 1.0-1 Timing of major events and activities relevant to commercial power reactor safety from 1940's to present (2 of 2)

References for Section 1.0

1. Mitchell Rogovin and George T. Frampton, Jr., Nuclear Regulatory Commission Special Inquiry Group, *Three Mile Island, A Report to the Commissioners and to the Public*, Rogovin, Stern & Huge law firm report (January 1980); summarized in *Nucl. Safety* **21**, 389 (1980).

2. Richard G. Hewlett and Francis Duncan, *Atomic Shield, 1947/1952, Volume II, A History of the United States Atomic Energy Commission*, The Pennsylvania State University Press, University Park, PA (1960).

3. C. P. Russel, *Reactor Safeguards*, MacMillan, New York (1962).

4. Richard G. Hewlett and Francis Duncan, *Nuclear Navy 1946-1962*, University of Chicago Press, Chicago, IL (1974).

5. George T. Mazuzan and Roger R. Trask, *An Outline History of Nuclear Regulation and Licensing 1946-1979*, Historical Office, Office of the Secretary, Nuclear Regulatory Commission (April 1979).

6. J. Samuel Walker, *A Short History of Nuclear Regulation 1946-1990*, Historical Office, Office of the Secretary, Nuclear Regulatory Commission (June 1991).

7. David Okrent, *Nuclear Reactor Safety: On the History of the Regulatory Process*, The University of Wisconsin Press, Madison, WI (1981).

8. Alice L. Buck, *A History of the Atomic Energy Commission*, DOE/ES-0003/1, U.S. Department of Energy, Assistant Secretary, Management and Administration, Office of the Executive Secretariat, History Division, Washington, DC (July 1983).

9. George T. Mazuzan and Samuel Walker, *Controlling The Atom: The Beginnings of Nuclear Regulation 1946-1962*, University of California Press (1984).

1.1 1946-1953, Emergence of Safety Strategies

1.1.1 The Atomic Energy Act of 1946

Following the use of the atomic bomb to end World War II, peaceful uses of nuclear energy were rapidly proposed. However, a much higher priority was to maintain control of and advance the weapons-related aspects of the new technology. Consequently, the Atomic Energy Act of 1946, while providing a statutory basis for developing peaceful uses of nuclear energy, stressed the need for secrecy, raw materials, and the production of new weapons. The act did not allow for private commercial applications of nuclear energy. Instead, it created a virtual federal government monopoly of the new technology and stressed the minimum regulation necessary under this monopolistic framework. To manage the nation's atomic energy programs, the act established the five-member Atomic Energy Commission (AEC). The Joint Committee on Atomic Energy (JCAE) was created by the act to provide congressional oversight of the AEC.

1.1.2 Siting

In 1947 the AEC established a Reactor Safeguards Committee (predecessor to the current Advisory Committee on Reactor Safeguards, ACRS) to determine whether the reactors being planned could be built without endangering public safety. In the first few years after World War II, several low power (less than 50 MWt) engineering test reactors were built in the United States to develop peaceful uses of atomic energy. For most of these reactors, the Reactor Safeguards Committee continued the practice established during the Manhattan project of siting reactors on large government reservations far from populated areas.

A 1950 report, WASH-3,[1] describes this isolated siting practice. For each reactor, a serious accident was postulated. The accident involved gross overheating or melting of the fuel, rupture of the reactor coolant system, and an uncontrolled release of radionuclides from the relatively conventional building that housed the reactor. Allowing for meteorological effects on the transport and dispersion of radionuclides, the Reactor Safeguards Committee recommended that residents be excluded within a specified distance R of the reactor. The exclusion distance R depended on the reactor thermal power, P(kWt), according to the following rule of thumb:

$$R = 0.01\sqrt{P\ (kWt)}$$

where R is measured in miles, or

$$R = 0.016\sqrt{P\ (kWt)}$$

where R is measured in kilometers.

Outside the exclusion area, it was stipulated that the calculated radiation exposure should be less than 300 rem (which is roughly the threshold for a lethal dose), or evacuation should be possible. For a 50 Mwt plant, the rule of thumb gives an exclusion distance of 1.73 miles (2.77 km). For a 3000 Mwt plant like many currently used to produce electricity, the rule of thumb would give an exclusion distance of 17.3 miles (27.8 km).

1.1.3 Containment

A significant early exception to government reservation siting was approved in 1952 for the sodium-cooled Submarine Intermediate Reactor Mark A, which was to be located at Knolls Atomic Power Laboratory (KAPL) only 19 miles (30.6 km) from Schenectady, NY. In response to Reactor Safeguards Committee concerns, the entire reactor facility was enclosed in a gas-tight steel sphere that was designed to withstand "a disruptive core explosion from nuclear energy release, followed by sodium-water and air reactions"[2] and to contain radionuclides that might otherwise be released in a reactor accident[3]. The AEC accepted this containment strategy; however, containment was not considered a perfect substitute for isolation by distance. The reactor was still built in a sparsely populated area.

In December 1953, the AEC invited private industry to submit proposals for the first "civilian" nuclear power plant. This plant, the Shippingport Atomic Power Station, which was also called the pressurized water reactor (PWR), was owned by the government, but was designed and constructed by Westinghouse and operated by Duquesne Light Company under the stringent guidance of the Division of Naval Reactors of the AEC. The PWR would not have met the 1950 rule of thumb criterion. The Shippingport, Pennsylvania site was about 420 acres (1.7 km^2) in area and about 20 miles (32 km) from Pittsburgh. Although remote, the site was in a region with more population than was characteristic of isolated government reservation sites. Therefore a containment building was provided for Shippingport.

1.1.4 Accident Prevention and Safety Systems

Nuclear-powered submarines were developed in parallel with commercial nuclear power plants in the early 1950s. The U.S.S. Nautilus, the first nuclear-powered submarine, commenced sea trials in 1955. Shippingport began to produce electrical power in 1957. Since the submarine crew had no avenue of escape while the ship was at sea and major ports were generally large population centers, remote siting could not be relied upon to acceptably limit the consequences of an accident. Nor could containment be reasonably engineered for a submarine.

As a result, the Navy relied on an accident prevention strategy. Stringent procedures were developed for operator training, quality control, and system/component testing. Systems and components were built with considerable design margin to withstand substantially higher than likely temperatures and pressures. Potential equipment malfunctions and failures were postulated anyway, and redundant systems were included in the design so that each safety function could be performed by more than one component or system. Prevention and safety-system strategies analogous to those used for submarine reactors evolved in the 1950s and early 1960s for commercial nuclear reactors on a case-by-case basis.

1.1.5 Defense In Depth

Figure 1.1-1 lists the key elements of an overall safety strategy that began to emerge in the early 1950s and has become known as defense in depth. One key element is <u>accident prevention</u>. Quality control and assurance are emphasized; plant systems and structures are conservatively designed, procured, and installed; and operators are trained to reduce the likelihood initiating a serious accident. In spite of these accident-prevention measures, equipment failures and operator errors that could result in serious accidents are postulated, and redundant <u>safety systems</u> are installed to prevent the release of radionuclides from the fuel. Notwithstanding these safety systems, radionuclide releases from the reactor coolant system are postulated, and a <u>containment</u> building is provided to prevent these radionuclides from escaping the plant. Plants are now being required to develop <u>accident management</u> programs (Module 2), which should reduce the likelihood of uncontrolled radionuclide releases during accidents. Further, in <u>siting</u> the reactor, exclusion areas and low population zones (Section 1.2.4) are provided so that potential leakage from the containment can be tolerated without endangering nearby residents. Finally, emergency plans (Sections 1.4.8 and Module 5) are developed that include provisions for sheltering and evacuation to further reduce potential doses to the public. Defense in depth can also be described in terms of the multiple barriers or layers of protection against radionuclide releases as indicated in Table 1.1-1.

The preceding description of defense in depth does not address questions such as: What accident initiators to postulate; what reactor containment system radionuclide releases to postulate; how much credit should be given for removing radionuclides using containment sprays, fan coolers, or suppression pools; how strong the containment should be; or what containment leakage to postulate. Of necessity, answers to these questions evolved and continue to evolve as plants are licensed, safety issues are addressed, operating experience is obtained, accidents occur, and safety research is conducted.

As the history discussed in the following subsections demonstrates, balance evolved in the defense-in-depth strategy. No single element (*e.g.*, accident prevention) or barrier (*e.g.*, containment) is emphasized to the exclusion of others. Much of this course describes the current balance and how it was achieved.

TABLE 1.1-1
DEFENSE IN DEPTH
MULTILAYER PROTECTION FROM FISSION PRODUCTS

Barrier or Layer	Function
1. Ceramic fuel pellets	Only a fraction of the gaseous and volatile fission products is released from the pellets.
2. Metal cladding	The cladding tubes contain the fission products released from the pellets. During the life of the fuel, less than 0.5 percent of the tubes may develop pinhole sized leaks through which some fission products escape.
3. Reactor vessel and piping	The 8- to 10-inch (20- to 25-cm) thick steel vessel and 3- to 4-inch (7.6- to 10.2-cm) thick steel piping contain the reactor cooling water. A portion of the circulating water is continuously passed through filters to keep the radioactivity low.
4. Containment	The nuclear steam supply system is enclosed in a containment building strong enough to withstand the rupture of any pipe in the reactor coolant system.
5. Exclusion area	A designated area around each plant separates the plant from the public. Entrance is restricted.
6. Low population zone, evacuation plan	Residents in the low population zone are protected by emergency evacuation plans.
7. Population center distance	Plants are located at a distance from population centers.

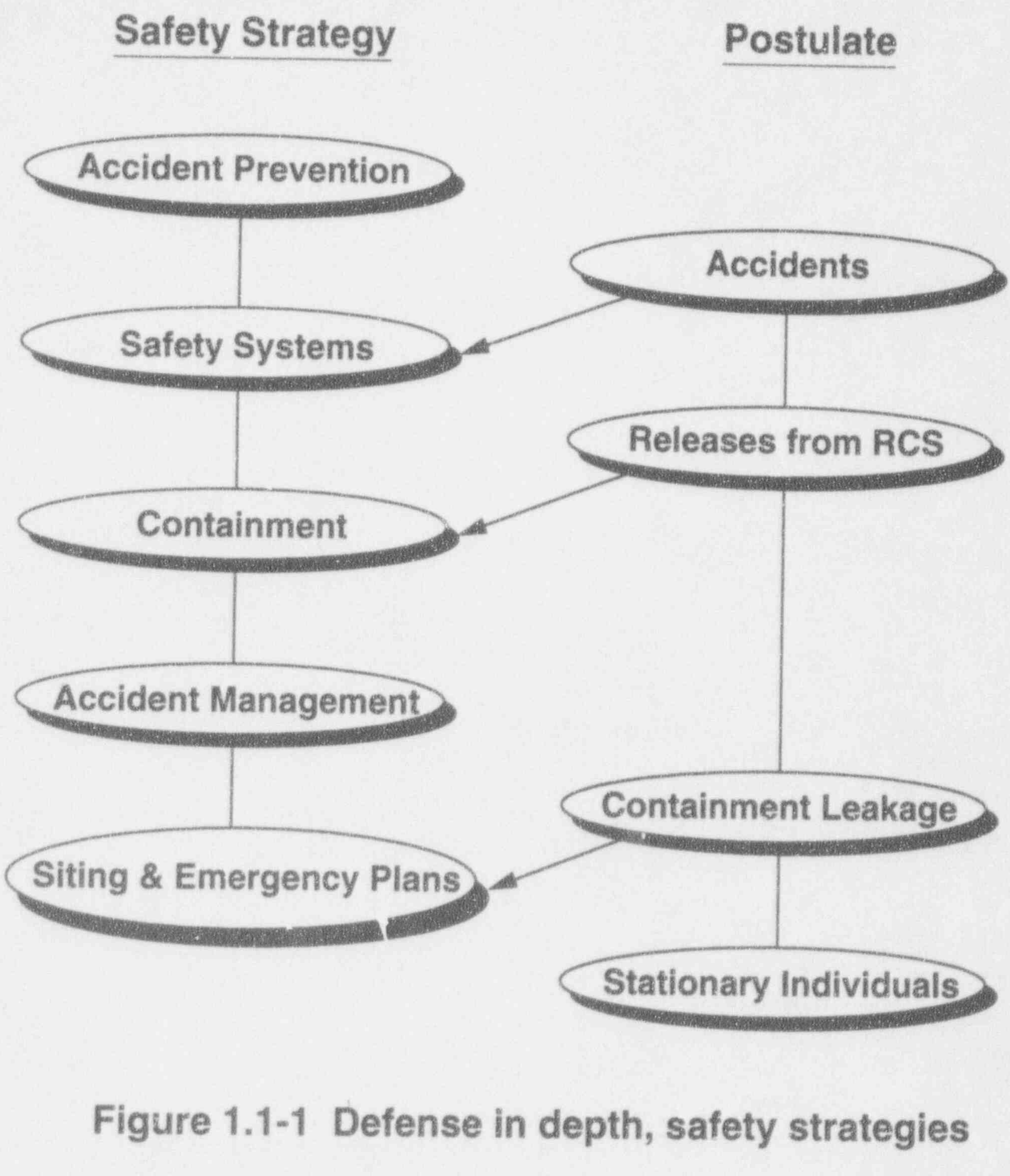


Figure 1.1-1 Defense in depth, safety strategies

References for Section 1.1

1. *Summary Report of Reactor Safeguards Committee*, U.S. Atomic Energy Commission report WASH-3 (1950).

2. C. P. Russel, *Reactor Safeguards*, MacMillan, New York (1962) p19.

3. Richard G. Hewlett and Francis Duncan, *Nuclear Navy 1946-1962*, University of Chicago Press, Chicago, Il. (1974) p176.

1.2 1954-1965 Early Commercial Reactors, Emphasis on Containment

1.2.1 Atomic Energy Act of 1954

In the early 1950's, there was no immediate need for nuclear power plants in the U.S. The impetus for developing U.S. nuclear power plants came from the fear of falling behind other nations, particularly the Soviet Union. In the midst of the cold war, U.S. government officials argued that countries in need of electrical power would gravitate toward the Soviet Union if it won the nuclear power race. In addition, with the development of the hydrogen bomb by both the U.S. and the Soviet Union, strong desire was expressed by the President and congressional leaders for counterbalancing peaceful uses of nuclear energy. But the development of such peaceful uses was thwarted by the limitations on access to technical information imposed by the Atomic Energy Act of 1946. After considerable debate concerning the merits of public versus private power, the 1946 act was amended by the Atomic Energy Act of 1954. Much of this act survives today under the Nuclear Regulatory Commission.

Among other things, the 1954 act provided for

> *a program to encourage widespread participation in the development and utilization of atomic energy for peaceful purposes to the maximum extent consistent with the common defense and security and with the health and safety of the public.*

The act largely satisfied industry needs for information, and it allowed private patents for inventions related to non-military applications of nuclear energy. It provided for the federal licensing of medical, research and development, and commercial facilities using nuclear materials. The rights of state or local government to license or regulate the safety (but not economics) of such facilities were preempted. U.S. antitrust laws were applied to licensees.

The act gave the AEC the responsibility for adequately protecting the public health, safety, life, and property. Section 182(a) of the Act requires the Commission to ensure that

> *the utilization or production of special nuclear material will ... provide adequate protection to the health and safety of the public.*

The Congress left it to the AEC to determine what constituted "*adequate protection.*" In its rules and decisions, the Commission refers to this standard as either the "*adequate protection*" standard or the "*no undue risk*" standard. The interchangeable use of these two terms has been accepted in legal decisions [1]

Under the 1954 Act, in addition to continuing its nuclear weapons programs, the AEC was given the responsibility for both encouraging and licensing commercial nuclear power. The Act outlined a two-step procedure for granting licenses. If the AEC found the safety analysis submitted by a utility for a proposed reactor to be acceptable, it would issue a construction permit. After construction was completed and the AEC determined that the facility met the provisions of the act and the rules and regulations of the commission, an operating license could be issued. The act allowed a public hearing "*upon the request of any person whose interest may be affected by the proceeding.*"

The AEC's regulatory staff, created soon after the passage of the 1954 Atomic Energy Act, confronted the task of writing regulations and devising licensing procedures rigorous enough to assure safety but flexible enough to allow for new findings and rapid changes in atomic technology. Within a short time the staff drafted rules and definitions on radiation protection standards, distribution and safeguarding of fissionable materials, and reactor operators' qualifications.

The AEC also established regulations implementing the two-step licensing process. Under the initial licensing regulations, reviews of applications for construction permits were evaluated by the regulatory staff, which next (or concurrently) sent the application to the Advisory Committee on Reactor Safeguards (ACRS) for independent review. The regulatory staff and Advisory Committee on Reactor Safeguards reviewed the information that applicants supplied on the suitability of the proposed site, construction specifications, plan of operations, and safety features. The AEC did not require finalized technical data on the safety of a facility at the construction permit stage. A construction permit could be granted if there was "reasonable assurance" that the plant could be constructed and operated at the proposed site "without undue risk to the health and safety of the public." Permitting construction to proceed without first resolving all potential safety problems was deemed acceptable in light of the existing state of the technology and the commitment to rapid development of nuclear power.

The recommendations of the staff and the Advisory Committee on Reactor Safeguards went to the commissioners, who made the final decision on whether to approve a construction permit or operating license. (Later, the Commission delegated consideration of regulatory staff and Advisory Committee on Reactor Safeguards judgments to the Atomic Safety and Licensing Boards while retaining final jurisdiction in licensing cases if it chose to review a board ruling.) The commission did not publicly document its findings regarding safety, nor did it make publicly available the reports it received from the Advisory Committee on Reactor Safeguards. Also, public notice of commission action on an application represented a *fait accompli*.

1.2.2 Early Siting Precedents

In 1955 and 1956, the AEC received and approved applications for construction permits for three large, privately owned power reactors. Each was to be in the general vicinity of a large city: Commonwealth Edison proposed the Dresden 1 BWR about 35 miles (56 km) southwest of Chicago, Illinois; Consolidated Edison proposed the Indian Point 1 PWR 24 miles (39 km) north of New York City; and Detroit Edison proposed the Enrico Fermi fast reactor 25 miles (40 km) south of Detroit. Containment buildings were proposed for all three reactors.

The advent of containment was clearly a decisive step in moving large reactors away from highly remote sites to populated areas. The large exclusion distance required by the rule of thumb criterion would have allowed few sites in the United States to qualify for large, uncontained nuclear power plants. The unavailability and/or cost of large blocks of unoccupied land near electrical load centers made isolated siting economically impractical. Furthermore, containment provided a barrier to the release of radionuclides that was highly desirable for public safety and for public acceptance of nuclear power.

In response to questions posed in 1956 by a U.S. senator, then AEC Chairman Libby stated:

> *It is expected that power reactors such as that now under construction at Shippingport, Pennsylvania, will rely more upon the philosophy of containment than isolation as a means of protecting the public against the consequence of an improbable accident, but in each case there will be a reasonable distance*

between the reactor and major centers of population.[2]

In 1958, a proposal was made to build a small (48 Mwt) organic-cooled commercial reactor without a containment near the town of Piqua, Ohio. This proposal was rejected and a containment building was required for the Piqua plant.[3] In fact, all the commercial nuclear power plants approved for construction in the U.S. have had containments.

No formal design criteria or site criteria existed in 1955, and rather little preliminary design information was available in 1955-1956 when the Dresden 1, Indian Point 1, and Enrico Fermi applications for construction permits were reviewed. Clearly, there was no plant operating experience at the time. In addition there was little consideration of alternative sites or demographic factors. In this light, it is interesting that the early siting decisions, particularly approval of the 585 Mwt Indian Point reactor, set major precedents on power reactor siting. No large power reactor has been built in the United States at a site having a greater surrounding population density than Indian Point.

1.2.3 Power Reactor Development Company Construction Permit Application

The January 1956 application for a construction permit to build the Enrico Fermi plant proved particularly contentious. The application was filed by the Power Reactor Development Company (PRDC), a consortium of utilities led by Detroit Edison. The fast breeder reactor that PRDC planned was far more technologically advanced than the light water reactors planned for Dresden 1 and Indian Point 1. The ACRS review of the PRDC application concluded that "*there is insufficient information available at this time to give assurance that the PRDC reactor can be operated at this site without public hazard.*" The ACRS expressed uncertainty that questions regarding the reactor's safety could be resolved within PRDC's proposed schedule for obtaining an operating license. The ACRS urged the AEC to expand its experimental programs on fast breeders to seek more complete data on the issues the PRDC application raised.

Public controversy regarding the PRDC application arose as the result of congressional testimony. In June 1956, AEC Chairman Lewis L. Strauss testified in support of a supplemental appropriation for the civilian nuclear power program before the House Appropriations Committee. The committee chairman was a strong public power advocate. He chided Strauss about private industry's lack of progress in atomic development and suggested that PRDC had "*no intention of building this reactor at any time in the determinable future.*"[4] Strauss, eager to refute this assertion, replied: "*They [PRDC] have already spent eight million dollars of their own money to date on this project. I told you they were breaking ground on August 8. I have been invited to attend the ceremony; I intend to do so.*"[4] This reply indicated that the AEC chairman was planning to attend the ground breaking ceremony for a reactor whose construction permit had not yet been granted.

During the hearings the next day, AEC Commissioner Thomas Murray, in arguing for additional research and development funds, disclosed the concerns of the ACRS regarding the PRDC application. Murray was so concerned about the ACRS safety concerns that he then went to see the chairman of the Joint Committee on Atomic Energy and described the contents of the ACRS report.

The Joint Committee, claiming the AEC had failed to keep them "*fully and currently informed*" as required by the 1954 Atomic Energy Act, promptly requested a copy of the ACRS document. The AEC reluctantly offered to provide a copy if the Joint Committee would keep it "*administratively confidential.*" The committee refused to accept the document under these conditions. (A few months later, the Commissioners discovered that the AEC had provided a copy of the document to PRDC. The Commissioners then decided they had no choice but to release the document publicly, an embarrassing change of stance.)

On August 2, 1956, based on more optimistic review of the PRDC application by the AEC staff, the commissioners decided to issue PRDC a construction permit by a vote of three to one (Murray was the dissenter). The AEC decision drew an angry response from the Joint Committee and led to the first intervention in nuclear power plant licensing.

1.2.4 The Price-Anderson Act and WASH-740

Angered by the AEC decision to grant the PRDC construction permit, Senator Clarance Anderson, Chairman of the Joint Committee on Atomic Energy, introduced legislation which (1) established the ACRS as a statutory body, (2) required it to review all applications for construction permits and operating licenses, (3) required the ACRS to make a public report on each review, and (4) required public hearings on all such applications.

These measures were passed as amendments to the Price-Anderson act in August 1957. The primary purpose of this act was to establish liability limits and no-fault provisions for insurance on nuclear reactor accidents. Such indemnity legislation was deemed essential by AEC, the emerging nuclear industry, and the Joint Committee on Atomic Energy who recognized that the probability of a severe reactor accident could not be reduced to zero. The original act, which has periodically ammended, had the government underwrite $500 million of insurance beyond the $60 million available from private companies. The AEC initially opposed setting a specific upper limit, but Anderson wanted to avoid a "*blank check*" for industry.[4] 10 CFR 140 describes the financial protection required for licensees.[5]

An important technical input to establishing the indemnity provisions of the Price-Anderson act was the report WASH-740 entitled, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants," which was prepared by Brookhaven National Laboratory and published by the AEC.[6] Using what would prove to be extremely pessimistic assumptions including a core meltdown with the release of fifty percent of the core fission products to the atmosphere, the worst case consequences of a 500 MWt reactor accident were estimated to be 3,400 early fatalities, 43,000 acute injuries, and 7 billion (1957) dollars.

There was a consensus among those involved in the WASH-740 study that the likelihood of a meltdown accident was low, but quantitative probability estimates could not be supported given the lack of operating plant experience. Similarly, the likelihood of containment failure (or bypass) given a meltdown accident was not quantified (or quantifiable, at the time). However, until 1966, the containment building was treated as an independent barrier, which should remain intact even if the core melted, thereby preventing any large release of radionuclides to the atmosphere. It was recognized that failure of the containment building and melting of the core could occur--for example, as a consequence of gross rupture of the reactor pressure vessel--but such events were not considered credible. Containment failure was not expected to occur just because the core melted.

1.2.5 The First Intervention

In the days after the AEC decision to grant the PRDC construction permit, private meetings were held between members of the Joint Committee and labor union representatives. Labor unions had opposed many of the changes in the Atomic Energy Act of 1954, citing fear of industry monopolization by private utilities.

On August 31, 1956, the AEC received three identical intervention petitions from American Federation of Labor--Congress of Industrial Organizations (AFL-CIO) unions. These were the first intervention petitions ever received by the AEC. They requested suspension of the PRDC construction permit while a hearing was held on the reactor's safety, PRDC's financial qualifications, and the legality of the AEC's conduct in issuing the construction permit. The AEC did not suspend the PRDC construction permit; however, the request for hearings was granted. The hearings began on January 8, 1957 and ran for more than two years.

On May 26, 1959 the hearings ended with an AEC ruling that the construction permit would stand. The unions appealed this decision, and almost a year later the US Court of Appeals in a two to one opinion upheld the unions by declaring the PRDC construction permit illegal. In a particularly controversial section, the two judge majority took it upon themselves to review the proposed site of the PRDC reactor. Apparently swayed by testimony of unmitigated nuclear accidents like that described in WASH-740 the majority opinion stated: "We think it clear from Congressional concern for safety that Congress intended no reactor should, without compelling reasons, be located where it will expose so large a population to the possibility of a nuclear disaster."[7]

The PRDC obtained a stay of the court-of-appeals order while the AEC appealed to the US Supreme Court. On June 12, 1961, the Court announced a seven-to-two vote in favor of the government's position. The decision supported the two-step licensing process holding that the AEC was within its authority to issue the construction permit because a separate positive finding of "adequate protection to the heath and safety of the public" would be required before granting an operating license. It was the PRDC case that established that "adequate protection" and "no undue risk" were synonymous. Regarding the AEC's authority to license reactors near a large city "*without compelling reasons*," the majority decision noted that the issue had been raised by the court of appeals, not by the intervenors and concluded that "the position is without merit."[7]

Although the AEC won the PRDC case, its early bungling of the ACRS report, the manner in which it handled the case, and the continuance of the construction permit during the five years of contention fostered the image of an agency more concerned with promoting the development of commercial nuclear power than with regulating its safety.

1.2.6 Reactor Site Criteria, 10 CFR 100

In the late 1950s several smaller reactors, all with containments and all at rural sites, were approved. However, during the same period, a few small power reactors (60 MWt) were proposed for sites within or adjacent to small cities. These were rejected or forced to move to somewhat less populated sites. To avoid wasting future efforts on reactor proposals for sites that would be evaluated unfavorably, the AEC commissioners encouraged the development of written site criteria.

On May 23, 1959, the AEC published in the Federal Register notice of a proposed rule making concerning site criteria.[3] The notice introduced several concepts that strongly influenced the licensing process for commercial reactors, particularly when site criteria were formally issued as 10 CFR 100 in April 1962.

The *maximum credible accident* was a concept introduced in the draft to strike a balance between two extremes. If the worst conceivable accident was postulated (*e.g.*, an uncontained meltdown as in WASH 740), only sites isolated from populated areas by hundreds of miles would offer sufficient protection. As noted earlier, this would have effectively precluded the commercialization of nuclear power. On the other hand, if engineered safety features (ESFs) to protect against all possible accidents were included in the facility design, then it could be argued that every site would be satisfactory. Of course, in the latter case no potentially serious accidents could be overlooked and the ESFs would have to be fail proof. Such omnipotence was not defensible. This led to the idea of designing for what was subjectively assessed to be the maximum credible accident.

When 10 CFR 100 was issued (April 1962), the term maximum credible accident was dropped, but the notion was retained in 100.11 (a) and an associated footnote:

> *As an aid in evaluating a proposed site, an applicant should assume a fission product release from the core, the expected demonstrable leak rate from the containment and the meteorological conditions pertinent to his site ...**

The fission product release assumed for these calculations should be based upon a major accident, hypothesized for purposes of site analysis or postulated from considerations of possible accidental events, that would result in potential hazards not exceeded by those from any accident considered credible. Such accidents have generally been assumed to result in substantial meltdown of the core with subsequent release of appreciable quantities of fission products.

This maximum credible accident has, at various times, also been referred to as the design basis accident (DBA), the design-basis loss of coolant accident (LOCA), and the siting-basis LOCA. Given the rather prescriptive assumptions that evolved for demonstrating compliance with 10 CFR 100, the term design-basis LOCA is adopted here. This hypothetical accident is invariably initiated by the reactor-coolant system pipe break that would yield the highest containment pressure.

To demonstrate compliance with 10 CFR 100, 100% of the noble gas fission products, 50% of the volatile (halogen) fission products, and 1% of the particulates are assumed to be immediately released to the containment atmosphere following the pipe break.[8,9,10] Such releases are only possible if a large fraction of the core melts. Containment, which is designed to withstand the peak pressure associated with reactor coolant system blowdown, is assumed to remain intact but to leak radionuclides to the environment at the design leakage rate (the containment leakage rate to be incorporated in the plant technical specifications).

Only very limited metal-water reactions and associated hydrogen production are accounted for in the computational assumptions that evolved for demonstrating compliance with 10 CFR 100. The reason for this is not clear. The potential importance of metal water reactions during core melt accidents was recognized as early as 1957 (in WASH-740); however, the fact that stainless steel, which was used for cladding until the mid-1960s, is considerably less reactive than Zircaloy probably influenced the design-basis LOCA assumptions that evolved in the late 1950s and early 1960s. Design-basis LOCA assumptions and calculations are discussed further in Section 2. The evolution of hydrogen and the burn that occured at Three Mile Island Unit 2 are discussed in Sections 2.4 and 3.4.

For purposes of site evaluation, 10 CFR 100 requires that doses at two area boundaries be considered. The *exclusion area* is

> *that area surrounding the reactor in which the licensee has the authority to determine all activities, including exclusion or removal of personnel and property from the area.*[11]

The exclusion area does not have to be owned by the licensee, merely controlled. The *low population zone* is

> *the area immediately surrounding the exclusion area, which contains residents, the total number and density of which are such that there is a reasonable probability that appropriate protective measures could be taken in their behalf in the event of a serious accident.*[12]

10 CFR 100 stipulates that neither an individual located at any point on the outer boundary of the exclusion area for two hours immediately following onset of the postulated fission product release nor an individual located at any point on the outer boundary of the low population zone for the duration of the accident should receive a total radiation dose in excess of 25 rem to the whole body or 300 rem to the thyroid.[13] Thus, the design-basis LOCA, whose consequences were not to be exceeded by any other credible accident, became the focus of siting evaluations. 10 CFR 100 also stipulates that the

> *population center distance*, which is "*the distance from the reactor to the nearest boundary of a densely populated center containing more than 25,000 residents, should be "at least one and one-third times the distance from the reactor to the outer boundary of the low population zone.*[14]

This requirement developed as a result of various considerations. In late 1960, the Advisory Committee on Reactor Safeguards proposed a rather specific criterion--no lethal doses at the population center for the worst conceivable accident (an uncontained meltdown as considered in WASH 740). This philosophy was reflected in the statement of considerations which accompanied the interim version of the site criteria released in March 1961:

> *Even if a more serious accident (not normally considered credible) should occur, the number of people killed should not be catastrophic.*[3]

However, when the AEC published 10 CFR 100 in April 1962, the new statement of considerations discussed the use of a minimum acceptable distance to the nearest population center as a way to limit the cumulative population dose (i.e., the sum of the individual dose received by each person) and to provide for protection against excessive radiation exposure to people in large centers, where effective protective measures might not be feasible. Thus, 10 CFR 100 does not address accidents more serious than the maximum credible LOCA.

1.2.7 Credit for Engineered Safety Features

Although the 10 CFR 100 reactor site criteria notes the

> *current policy of the Commission of keeping stationary power and test reactors away from densely populated centers,*" it goes on to say, "*It should be equally understood, however, that applicants are free and indeed encouraged to demonstrate to the*

Commission the applicability and significance of considerations other than those set forth in the guides.

The nuclear industry responded to 10 CFR 100 in two ways: (1) by seeking credit for engineered safety features (ESFs, which were called engineered safeguards at the time) and (2) by direct attacks on metropolitan siting restrictions.

Credit for ESFs was sought to allow siting of reactors at locations where, without such features, protection of the public would not be adequate (10 CFR 100 guidelines would be exceeded). Applicants attempted to get maximum credit for reductions in containment pressure and radionuclide concentrations by ESFs during postulated LOCAs. The ESFs for which credit was routinely given were containment, the pressure suppression pool, containment building sprays, containment heat removal systems, and containment air-cleaning systems.

In approving the San Onofre 1 construction permit application in 1963, credit was even given for emergency core cooling systems (ECCS) so that only 6% of the core was assumed to melt, thereby reducing the containment fission product inventory to 6% of that which would otherwise have been postulated for siting.

In November 1964, in response to an AEC request, the Advisory Committee on Reactor Safeguards documented its rationale for accepting certain ESFs as substitutes for distance in meeting 10 CFR Part 100.[15] The position of the Advisory Committee on Reactor Safeguards was that credit was appropriate for all of the above listed ESFs except emergency core cooling system. Emergency core cooling system was deemed essential for accident prevention, but radionuclide releases postulated for siting were to be consistent with emergency core cooling system failure:

Core spray and safety injection systems ... might not function for several reasons in the event of an accident ... Therefore, reliance cannot be placed on systems such as these as the sole engineered safeguards in the plant. Nevertheless, prevention of core melting after an unlikely loss of primary coolant would greatly reduce the exposure of the public. Thus, the inclusion of a reactor core fission product heat removal system as an engineered safeguard is usually essential.

The San Onofre 1, Connecticut Yankee, Oyster Creek, Nine Mile Point, and Dresden 2 plants were approved for construction from 1963 to 1965 using ESFs to permit relaxing previous requirements on the size of the exclusion area and low population zone. In 1962 an application was submitted for a construction permit for the Ravenswood plant essentially in the heart of New York City.[3] The AEC staff rejected this application; however, metropolitan siting was still seriously considered as late as 1970.[3]

References for Section 1.2

1. Union of Concerned Scientists v. U.S. NRC, 824 Federal Reporter, 2d series, 108 (DC Cir 1987)

2. Willard F. Libby, then Acting Chairman of the Atomic Energy Commission, letter to Senator Bourke Hickenlooper (March 14, 1956), reproduced in Okrent.

3. David Okrent, *Nuclear Reactor Safety*: On the *History of the Regulatory Process,* The University of Wisconsin Press, Madison WI (1981).

4. J. Samuel Walker, *A Short History of Nuclear Regulation 1946-1990,* NUREG/BR-1075, January 1993.

5. Title 10, Code of Federal Regulations, Part 140, January 1, 1991.

6. *Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants*, U.S. Atomic Energy Commission report WASH-740 (March 1957).

7. J. Samuel Walker, *Controlling the Atom: The Beginnings of Nuclear Regulation, 1946-1962*, University of California Press, 1992.

8. J. J. DiNunno, R. E. Baker, F. D. Anderson, and R. L. Waterfield, *Calculation of Distance Factors for Power and Test Reactor Sites*, TID-14844, Division of Licensing and Regulation, AEC, Washington, D. C. (March 23, 1962). Note: TID-14844 was supplanted by the following two regulatory guides.

9. U.S. Atomic Energy Commission Regulatory Guides 1.3, *Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Boiling Water Reactors*, Revision 2 (June 1974).

10. U.S. Atomic Energy Commission Regulatory Guides 1.4, *Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Pressurized Water Reactors*, Revision 2 (June 1974).

11. Title 10, Code of Federal Regulation, Part 100.3 (a) (April 1962).

12. Title 10, Code of Federal Regulations, Part 100.3 (b) (April 1962).

13. Title 10, Code of Federal Regulation, Part 100.11 (1)&(2) (April 1962).

14. Title 10, Code of Federal Regulations, Part 100.3 (d) and 10 CFR 100.11 (a) (3) (April 1962).

15. Herbert Kouts, ACRS Chairman, letter to Glenn T. Seaborg, Chairman, U.S. AEC, subject "Report on Engineered Safeguards," November 18, 1964.

1.3 1966-1974 Emphasis on Prevention, Public Debate

In 1966, two issues called into question the assumption of containment as an independent barrier. These were the issue of reactor pressure vessel integrity and the so-called China syndrome. The net effect of these issues was to shift the focus of regulatory actions toward a strategy of accident prevention and away from reliance on containment.

1.3.1 Reactor Pressure Vessel Integrity

The design and manufacture of early nuclear reactor vessels in the United States conformed to the basic requirements of Section I and/or Section VII of the American Society of Mechanical Engineers Boiler and Pressure Vessel Code. These procedures were also supplemented by nuclear code cases and the Navy Code.[1] Recognizing the unique nature of nuclear reactors, the American Society of Mechanical Engineers in 1955 established a special committee to consider reactor pressure vessels.[2] In March of 1964, the American Society of Mechanical Engineers Section III, "Rules for Construction of Nuclear Vessels" were issued to specify and provide a uniform approach to the design of nuclear pressure vessels. The new rules placed more emphasis on the careful analysis of design details leading to more refined design practices.[1]

As the temperature of reactor vessel material is raised, the toughness increases, slowly at first but near the reference temperature for nil ductility transition, RT_{NDT}, toughness begins to increase much more rapidly. This implies that reactor vessels are quite tough at normal operating temperatures. Starting about 1950 information on the effects of neutron radiation on the engineering properties of structural materials began to appear in the literature. Neutron irradiation was found to cause structural materials to embrittle. This can be characterized by a shift in RT_{NDT} that occurs over decades of plant operation, as depicted in Figure 1.3-1.

In 1959, an American Society for Testing and Materials task group made recommendations on test procedures for evaluating radiation effects on materials, which led to recommended practices for surveillance tests on structural materials in nuclear reactors.[3] As part of their safety analysis review, the AEC ensured that each plant conducted a reactor vessel irradiation surveillance program per American Society for Testing and Materials standards to evaluate the shift in RT_{NDT} over the plant life, especially in the beltline region opposite the core midplane where the reactor vessel sees the largest neutron flux.

Because of the stringent design and surveillance practices applied to reactor pressure vessels in U.S., failure of the reactor pressure vessel has traditionally been considered incredible. Containments for U.S. nuclear power plants are not designed to withstand the loads associated with gross rupture of the reactor pressure vessel.

In 1964 a failure occurred near the nil ductility transition temperature of a large heat exchanger under test by the Foster Wheeler Corporation. As a result of this failure and concerns raised in 1964-1965 by British researchers, the Advisory Committee on Reactor Safeguards issued a November 24, 1965 letter.[4] While acknowledging the low probability of reactor pressure vessel failure, the Advisory Committee on Reactor Safeguards expressed concern for the

> *increase in number, size, power level, and proximity of nuclear power reactors to large population centers,*

and recommended (1) the development of improved design and inspection methods for reactor pressure vessels and (2) the development of means "*to ameliorate the consequences of a major pressure vessel rupture.*" The latter recommendation prompted strong disagreement from both industry and AEC representatives. Nevertheless, more heavily populated sites such as Indian Point and Zion were required to design their reactor vessel cavities to withstand a longitudinal pressure vessel split. Ultimately, pressure on the part of both the Advisory Committee on Reactor Safeguards and AEC staff prompted the development of improved industry standards for the design, fabrication, and inspection of pressure vessels. In addition, major research efforts examining a variety of issues related to reactor pressure vessel integrity were conducted. In 1974, research conducted by the Advisory Committee on Reactor Safeguards concluded that the probability of a reactor vessel failure is less than 10^{-5} per vessel-year and that the most likely failures would be within the capability of engineered safety features.[5]

The issue of reactor pressure vessel integrity has remained active since 1974. In particular, the 1979 accident at Three Mile Island Unit 2 (Sections 1.4.3 and 2.3) was responsible for moving the concern of *pressurized thermal shock* (PTS) to a high level of visibility. A pressurized thermal shock event is a PWR transient that can cause severe overcooling accompanied by vessel pressurization to a high level. The thermal stresses caused by rapid cooling of the reactor vessel inside surface combine with the pressure stresses to increase the potential for fracture if an initiating flaw is present in low toughness material. Detailed discussion on pressurized thermal shock is beyond the scope of this class; however, historical information is available elsewhere.[1,6] The regulatory approach that has evolved is aimed at ensuring that the probability of reactor pressure vessel failure is exceedingly low. The current rule governing pressure vessel protection against pressurized thermal shock is contained in 10 CFR 50.61.[7]

1.3.2 The China Syndrome

In preparation for a 1965 extension of Price-Anderson legislation on liability limits and insurance for nuclear reactors, Brookhaven National Laboratory (BNL) reexamined the WASH-740 worst case accident scenario. Brookhaven National Laboratory analyzed a loss of coolant accident in a 3,200 MWt reactor. No credit was given for ESFs. Brookhaven National Laboratory estimated that, several hours following initial primary system blowdown, decay heat from fission products would cause the core to melt through the bottom head of the reactor pressure vessel and potentially through the concrete containment basemat and into the earth until a solid mass with sufficient conductivity to dissipate decay heat was formed.[8] It was estimated that solidification might occur before basemat meltthrough and would certainly occur before the melt had penetrated more than 100 feet (30 m) into the ground; however, considering this potentially significant downward penetration, the term *China syndrome* was introduced.

If the molten fuel were to penetrate the containment basemat, radionuclides could escape through the soil to the atmosphere. Such soil-filtered releases would probably not cause lethal radiation doses to persons outside the exclusion area. Nevertheless, the China syndrome was significant because it demonstrated a strong correlation between a core meltdown and a possible loss of containment integrity. Phenomena that were not considered in the Brookhaven National Laboratory study were later recognized as potential causes of more serious above ground containment failure modes. Such phenomena had not been considered in reviewing applications for commercial plants despite the fact that the hypothetical *design-basis LOCA*, which was used to demonstrate compliance with 10 CFR 100 siting criteria (Section 1.2.4), postulated reactor containment system fission product releases corresponding to a full-scale core meltdown.

The impact of core melt on containment integrity was raised by the Advisory Committee on Reactor Safeguards in the summer of 1966 for the Dresden 3 BWR and Indian Point 2 PWR applications. Both Westinghouse and General Electric were asked to consider the possibility of providing ESFs that would maintain containment integrity in the presence of large-scale core melt.[9] General Electric argued that maintaining containment integrity in the face of core meltdown was not feasible for their BWR. They contended that the emergency core cooling system was adequate to prevent core melt in the event of a LOCA. Westinghouse felt that a core catcher below the reactor vessel could be used to maintain PWR containment integrity. Based on information provided by Westinghouse and General Electric, the Advisory Committee on Reactor Safeguards concluded that it would be very difficult, given the existing state of knowledge, to design such safeguards to assure containment integrity given core meltdown. Instead, the Advisory Committee on Reactor Safeguards reports of August 16, 1966, on Dresden 3 and Indian Point 2 recommended major improvements in both primary system integrity to reduce the probability of a LOCA and emergency core cooling to reduce the probability of meltdown given a LOCA.[9]

Thus, the China syndrome led to a shift in emphasis from containment to prevention. As time passed, accident initiators other than the traditional large pipe break were identified as potentially leading to core melt. In particular, scenarios involving anticipated transients without scram, station blackout, other transients, and containment bypass would be evaluated, and regulated to reduce the probability of core meltdown. However, over the next decade, the emphasis was on the traditional design-basis LOCA and the adequacy of emergency core cooling.

The increased emphasis on prevention complicated the regulatory process. As long as containment was considered an independent barrier, the main issue in the regulatory process was whether the dose limitations of 10 CFR 100 would be met for the maximum credible accident. Disagreements focused on what was credible or on the amount of credit appropriate for ESFs. The new emphasis on prevention gave rise to a much larger set of debatable issues. The regulatory process began to address all potential causes of core meltdown including failures in mechanical, electrical, and control systems.

The Brookhaven reexamination of WASH-740, which gave rise to the China Syndrome and to the shift in emphasis from containment to prevention, was never completed or published. An internal AEC summary of the project written in 1969 stated that an important factor in the decision not to produce a complete revision of WASH-740 along the lines proposed by the Brookhaven staff was the public relations considerations. In fact, it was the failure to release a final report of the Brookhaven study that became a public relations concern, because opponents of nuclear power argued convincingly that the AEC was covering up the real risk of reactor accidents.[10]

1.3.3 The AEC Core Cooling Task Force (CCTF)

In September 1966, Advisory Committee on Reactor Safeguards members expressed their concerns regarding the China syndrome in a meeting with the AEC commissioners. To avoid a letter from the Advisory Committee on Reactor Safeguards, which would have recommended the development and implementation of safety features to protect against LOCAs in which emergency core cooling system did not work, the AEC commissioners established a task force to study and report on questions arising from the China syndrome.[9] The eleven-man task force, which was known as the AEC Core Cooling Task Force (CCTF), was chaired by William Ergen of Oak Ridge National Laboratory and had six members from industry and five from AEC supported laboratories. The Core-Cooling Task Force was asked to consider:

1. the degree to which core cooling systems could be augmented to prevent core meltdown;
2. the potential history of large molten masses of fuel;
3. the possible interactions of molten fuel with materials or atmospheres in containments; and
4. the design and development problems associated with systems whose objective is to cope with large molten masses of fuel.[9]

When faced with what little was then known about core meltdown accidents and associated phenomena, it was clear to the Core-Cooling Task Force that designing to assure containment integrity after core meltdown would require extensive, protracted, costly research. Such research was far beyond the scope of the Core-Cooling Task Force. Consequently, the Core-Cooling Task Force focused on item 1, preventing core meltdown.*

The Core-Cooling Task Force report entitled "Report of the Advisory Task Force on Power Reactor Emergency Cooling," which became available in late 1967,[9] concluded that augmented emergency core cooling system was feasible and beneficial. The report was used for policy decisions by the AEC during the ensuing years, when the AEC emphasized improvements in quality control and emergency core cooling systems. However, no significant efforts to address core meltdown accidents arose from the Core-Cooling Task Force report. The Core-Cooling Task Force correctly pointed out that small LOCAs might have safety significance [Beckjord memorandum*], a fact that would be re-asserted in the 1975 Reactor Safety Study (Section 1.4.2) and confirmed by the 1979 accident at Three Mile Island Unit 2 (Sections 1.4.3 and 2.4). In contrast, the task force conclusion that current (1967) technology was sufficient to enable prediction, with reasonable assurance, of the key phenomena associated with the design basis LOCA, as well as provide quantitative understanding an accident, would prove to be incorrect (Section 1.3.6).

1.3.4 General Design Criteria

The AEC review of all commercial reactors from Shippingport to Dresden 2 in 1965 was on a case-by-case basis. The list of potential hazards expanded as new questions were encountered during individual plant reviews. Tornadoes were first considered for a plant in Arkansas, hurricanes for a plant in Florida, and seismic events for plants in California. Such natural phenomena were then considered in the review of other plants. Unusual operating experiences also resulted in new design requirements. For example, tornadoes once disabled all five off-site power lines feeding the Dresden 1 plant, which had no on-site emergency AC power. Subsequently, first one small on-site diesel, then a larger diesel, then redundant diesels to drive containment related safeguards became the standard. In 1966, redundant on-site power was required to power the emergency core cooling system, requiring still larger diesels.

* Eric S. Beckjord, U.S. Nuclear Regulatory Commission Memorandum, (February 28, 1992).

Until 1965, there were no written criteria against which the various designs could be compared, and there was essentially no review of the detailed design approach, which actually determines the level of safety achieved. As the number of new plant applications grew, there was strong motivation on the part of both industry and the AEC to streamline the licensing review process. In the spring of 1965, in response to anticipated recommendations of an outside review panel, the AEC staff began drafting what would become the General Design Criteria, Appendix A of 10 CFR 50.

On November 22, 1965, the AEC issued a press release announcing the proposed criteria and requesting public comment.[11] During the comment period the discussions of Reactor Pressure Vessel failure, the China syndrome, and the Core-Cooling Task Force were active. In this light it is interesting to note three significant changes in the revised draft of the general design criteria, which was issued for comment 19 months later (July 10, 1967).[12] First, the revised draft no longer required the containment be designed to withstand a full meltdown as the original draft had. The revised containment design basis did contain the vague phrase

> *including considerable margin for effects from metal-water or other chemical reactions that could occur as a consequence of failure of emergency core cooling systems.*

Except for these words, the revised draft made no reference to core melt accidents. Second, the revised draft called for

> *at least two emergency core cooling systems preferably of different design principles, each with a capability for accomplishing abundant emergency core cooling.*

Third, requirements to design against single-failures, which had appeared in the November 1965 version in slightly different words, were prominent in the revised draft:

> *A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electrical systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly) results in a loss of the capability of the system to perform its safety function.**

> *Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development.*

The proposed criteria of July 10, 1967, provided "*interim guidance*" to the regulatory staff and the nuclear industry for several years. On February 20, 1971, the AEC published a revised set of general design criteria, which became Appendix A of 10 CFR 50.[13] The 1971 criteria, reflected the LWR plants that had been reviewed in the previous few years. Two emergency core cooling systems, each capable of providing abundant cooling were no longer required. The emergency core cooling system criterion now said, *A system to provide abundant emergency core cooling shall be provided,*

and the single failure criterion was applied to the emergency core cooling system. None of the criteria related to core melt accidents. The vague phrase of the July 10, 1965, containment design criteria was modified to require consideration of

chemical reactions that may result from degradation, but not total failure, of the emergency core cooling.

The introduction to the 1971 criteria listed several safety considerations for which general design criteria had not yet been (and have not yet been) developed. The list included redundancy issues; common mode failures; systematic, non-random failures; and passive failures.

The general design criteria do not provide quantitative bases for establishing the adequacy of any particular design. The detailed design and its acceptability were deliberately left to the "engineering judgment" of the designer and the regulator, respectively. The development of more detailed regulatory guidance began in the 1967-1968 time frame when the regulatory staff started generating internal documents that specified acceptable detailed design approaches to specific problems. In 1970 the AEC began publishing such regulatory guides. The first published regulatory guide dealt with the concern that emergency core cooling system should not fail as a result of a loss of containment integrity.[14] It required that sources of emergency core cooling system water be at sufficiently high pressure (provide sufficient net positive suction head, NPSH) to avoid pump cavitation. As shown in Figure 1.3-2, the number of regulatory guides issued or revised each year grew rapidly and remained high throughout the 1970s.* By 1978, more than 100 different regulatory guides had been issued.[9] In addition, numerous branch technical positions, and standard review plans were issued. None of these had the force of law like the general design criteria; however, utilities usually found it easier to follow a design approach prejudged as acceptable by the regulatory staff than to defend an alternative approach.

The actual general design criteria address 64 broad issues in 6 major categories:

I. Overall Requirements
II. Protection by Multiple Fission Product Barriers
III. Protection and Reactivity Control Systems
IV. Fluid Systems
V. Reactor Containment
VI. Fuel and Reactivity Control

Although all of the individual criteria can not be discussed here, the five criteria forming the overall requirements are worthy of further discussion. These criteria are particularly important and impact many aspects of reactor safety.

*Data provided by G. S. Hicher, U.S. Nuclear Regulatory Commission (March 10, 1992).

1.3.4.1 Criterion 1-Quality Standards and Records

Quality assurance is an important part of maintaining an adequate level of safety at nuclear power plants. A good quality assurance program can ensure that a plant is properly designed, that it is built as designed, that proper materials are used in construction, that the design is not inappropriately changed at a later date, and that appropriate maintenance and operational practices are followed.

Criterion 1 states that:

Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions being performed. ... A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the plant.

The criterion for quality assurance was first proposed in the July 1967 draft of Appendix A. The lack of AEC requirements and criteria for quality assurance was a key issue raised by the Atomic Safety and Licensing Board in the operating license hearings for the Zion plant in 1968. The board ruled that until the licensee presented a program to assure quality and until the AEC developed criteria by which to evaluate such a program, the hearings would be halted. Following the board's ruling and prior to the final issuance of Appendix A, the Atomic Energy Commission proposed a new regulation, Appendix B to 10 CFR Part 50. This new regulation more clearly spelled out requirements for the licensees to develop programs to assure the quality of nuclear power plant design, construction, and operation.

Appendix B contained 18 items that must be part of a quality assurance program for safety-related systems and components. Experience from military, the National Aeronautics and Space Administration, and commercial nuclear projects, as well as the Atomic Energy Commission's own nuclear reactor experience was used in developing the 18 items. Appendix B clearly places the burden of responsibility for quality assurance on the licensee. Visible quality assurance documentation is required for all activities affecting the quality of safety-related systems. Appendix B was published for comment in April 1969 and implemented in June 1970.

Following establishment of Appendices[1] A and B, the Atomic Energy Commission and the industry began issuing guidance that provided acceptable ways of meeting the intent and requirements of the specific regulations. In October 1971, The American National Standards Institute issued N45.2, "Quality Assurance Program Requirements for Nuclear Power Plants."[15] This standard was subsequently endorsed by the Atomic Energy Commission in Safety Guide 28 (now Regulatory Guide 1.28) in June 1972. Since that time there have been numerous additional guides and other documents on the subject of quality assurance. The Standard Review Plan includes guidance concerning how the NRC staff should review and evaluate proposed quality assurance programs.

1.3.4.2 Criterion 2-Design Bases for Protection Against Natural Phenomena

Criterion 2 recognizes that not all accidents are expected to begin as a result of failures within the plant boundaries. Additionally, natural phenomena may represent a threat to plant safety. Criterion 2 states:

Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to *perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.*

Module 2 describes in more detail the threats from natural phenomena and approaches for dealing with them.

1.3.4.3 Criterion 3-Fire Protection

Fires are a potential hazard at most large industrial facilities, including nuclear power plants. Fires can occur in electrical equipment or a variety of combustible materials that may be present at a plant. Small fires are fairly common occurrences, and to assure that nuclear power plants can adequately deal with fires, Criterion 3 was developed which states:

Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. ...

The criterion further specifies the need for using noncombustible materials whenever possible and for providing fire detection and firefighting systems.

Despite the development of Criterion 3, fires continued to occur at nuclear power plants. On March 22, 1975 the Brown's Ferry Nuclear Power Plant experienced a major fire, resulting in the loss of numerous safety systems. The Brown's Ferry fire is discussed at length in Module 2 of this course. Following the fire, the Special Review Group that investigated the fire recommended that NRC should develop additional specific guidance for implementation of Criterion 3. In response to this recommendation, the NRC developed Branch Technical Position 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants."[16] This information was later published as Regulatory Guide 1.120, Fire Protection Guidelines for Nuclear Power Plants.[17]

In 1980 the NRC formally proposed Appendix R to 10CFR50 to state the minimum acceptable level of fire protection for power plants operating prior to January 1, 1979.[18] Appendix R contains four general requirements to (1) establish a fire protection program, (2) perform a fire hazards analysis, (3) to incorporate fire prevention features, and (4) to provide alternative or dedicated shutdown capability. Furthermore, a number of specific requirements were included, dealing with:

- Water supplies for fire suppression
- Isolation valves in the fire suppression system
- Manual fire suppression
- Testing
- Automatic fire detection
- Safe shutdown capability
- Fire brigade
- Training
- Emergency lighting
- Administrative controls
- Alternative shutdown capability
- Fire barriers
- Oil collection

Compliance with Appendix R has led to significant improvements in fire safety at nuclear power plants; however, fires continue to occur and remain an important safety issue.

1.3.4.4 Criterion 4-Environmental and Dynamic Effects Design Bases

Reactor accidents may lead to harsh environmental conditions that may challenge the operation of components and systems or threaten the integrity of structures. Examples of environmental conditions that can occur include:

1. High-temperature steam
2. High pressure
3. Radiation
4. Missiles
5. Pipe whip

For safety systems to function during an accident, they must be designed to withstand the expected environments. Therefore, Criterion 4 states:

> *Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. ...*

Qualification testing is normally used to show that equipment can survive the postulated design-basis accident environments. The beyond-design-basis accidents discussed in Chapter 2 can produce environments exceeding the qualification limits.

The design of restraints to preclude pipe whipping has been a complex and controversial process. Criterion 4 allows the licensee an exemption for pipe whipping under certain conditions:

> *... dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.*

Assurance that nuclear power plants meet Criterion 4 is an ongoing process. Testing and documentation required by Criterion 1 are an essential part of the process. However, in certain cases testing may not accurately replicate the environments that will actually be seen during an accident. A classic case involves motor-operated valves. In 1985 an incident at the Davis-Besse plant involved failure of key valves in the auxiliary feedwater system.[19] The valves had been successfully tested on numerous occasions. However, during the actual incident, the valves were exposed to high differential pressures that were not present during testing, and the torque switches were not set to account for the differential pressure. Continuing vigilance on the part of inspectors and regulators to assure that Criterion 4 is met is an important part of the reactor safety philosophy.

1.3.4.5 Criterion 5-Sharing of Structures, Systems, and Components

Criterion 5 is intended to address features of a multi-unit site that could allow problems to propagate from one unit to another. The criterion states:

> *Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident at one unit,*

an orderly shutdown and cooldown of the remaining units.

Prior to the development of Criterion 5, multi-unit sites frequently made use of shared systems and structures. Service water systems, control rooms and other features were often shared. While each unit included enough redundancy to respond to an accident without consideration of the other units, it was possible for an event at one location to affect multiple units at the same time. Plants in multi-unit sites developed after the issuance of the General Design Criteria generally follow the philosophy of complete separation of units with separate components and structures for all important systems.

Although complete separation of units allows the licensee to easily meet Criterion 5, there are some important benefits lost in this approach. PRAs indicate that the ability to properly cross-tie safety systems from one unit to another can significantly reduce the risk of certain types of accidents. For example, cross-tieing diesel generators can reduce the risk of station blackout. Some plants have the ability to cross-tie emergency cooling and heat removal systems. The key is to make sure that the cross-ties are properly designed and implemented so they do not cause undue multi-unit problems. However, the philosophy that all cross-ties are bad and complete separation is good is an unfortunate one that, in some cases, has had a negative impact on safety.

1.3.5 The National Environmental Policy Act (NEPA)

In December 1969, Congress passed the National Environmental Policy Act (NEPA), which was signed by President Nixon on January 1, 1970. NEPA required federal agencies to consider the environmental impact of their activities. In many ways the Act was vague and confusing, and it gave federal agencies broad discretion in deciding how to carry out its mandate. The AEC acted promptly to comply with NEPA, but its procedures for doing so brought protests from environmentalists. The AEC took a narrow view of its responsibilities under NEPA. A proposed regulation issued by the AEC in December 1970, added non-radiological issues to the AEC's regulatory jurisdiction, but stated AEC's intent to rely on environmental assessments performed by other federal and state agencies rather than perform its own. The AEC agreed to consider environmental issues in licensing board hearings only if raised by a party to the proceeding. AEC also postponed a review of NEPA issues in licensing cases until March 1971.

The AEC took a limited view of its responsibilities under NEPA for several reasons. First was the conviction that the routine operation of nuclear power plants was not a serious threat to the environment, and indeed, was beneficial compared to burning fossil fuel. Second, the major products of nuclear power generation that affected the environment, radiation releases and thermal discharges, were already covered by existing legislation. Finally, implementation of NEPA might divert the AEC's limited human resources from tasks that were more central to its mission. The regulatory staff was inundated by a flood of reactor applications and did not relish the idea of having to spend large amounts of time on environmental reviews. The AEC feared that considering a wider range of environmental issues would cause unwarranted further delays in licensing plants.

Environmentalists charged that the AEC had failed to fulfill the purposes of NEPA and took the agency to federal court over the application of the AEC's regulations to the Calvert Cliffs nuclear units, which were then under construction on the Chesapeake Bay in rural Maryland. The July 23, 1971 ruling of the

United States Court of Appeals for the District of Columbia was a stunning defeat for the AEC.[20] The court sternly rebuked the AEC saying

> *We believe that the Commission's crabbed interpretation of National Environmental Policy Act makes a mockery of the Act.*

Recognizing the need to improve the public image of the AEC, the commissioners decided not to appeal the Calvert Cliffs court ruling. In effect, the NRC agreed to consider environmental impacts of proposed projects and to develop environmental expertise required to do so. In explaining this decision to industrial groups, James R. Schlesinger, newly appointed AEC Chairman, indicated that although AEC's policy of promoting and protecting the industry had been justified to help nuclear power get started, the industry was "*rapidly approaching mature growth*," and "*should not expect the AEC to fight the industry's political, social, and commercial battles.*" Rather, he added, the agency's role was "*primarily to perform as a referee serving the public interest.*"[21] This represented a new direction in the AEC's approach to its regulatory duties.

In response to requirements of the NEPA, the Atomic Energy Commission on December 1, 1971, published 10 CFR Part 51, Licensing and Environmental Policy and Procedures for Environmental Protection.[22] Originally, Part 51 identified nine classes of accidents. Events ranging from trivial events (Class 1) to major accidents considered in the design basis evaluation required for the safety analysis report (Class 8) were assigned to Classes 1 through 8. Accidents more severe than those postulated in Class 8, which could lead to core meltdown and radionuclide releases exceeding the dose guidelines of 10 CFR Part 100, were designated Class 9. Although this classification scheme is no longer contained in 10 CFR, the term Class 9 is still commonly used to distinguish severe accidents, which involve core damage (Section 2.2), from accidents for which the plant is designed (Sections 2.1).

1.3.6 Emergency Core Cooling System Rulemaking

In May 1971, the AEC released unexpected results of a Pressurized Water Reactor (PWR) emergency core cooling system test conducted at the Idaho National Engineering Laboratory (INEL), which indicated the possibility that the emergency core cooling system could fail to provide water to the core. The tests involved a 9-inch diameter pressure vessel with one set of inlet and outlet pipes. A break in an emergency core cooling system inlet pipe was simulated, and an attempt was made to inject water into the pressure vessel to cool the electrically heated rods simulating the core. The water was unable to enter against the residual steam pressure as steam and water were being expelled through the break. This test result prompted the AEC to adopt a set of Interim Acceptance Criteria,[23] that went into effect until further research on emergency core cooling system could be done. These criteria required additional maintenance and monitoring as well as changes in the emergency core cooling system of some operating reactors.

At the time, generic issues such as the adequacy of emergency core cooling were being contested at individual licensing hearings greatly delaying the licensing process. In an attempt to streamline the licensing process, the AEC decided to conduct rulemaking hearings on such generic issues. The hearings were adjudicatory in nature, affording the participants the opportunity to testify and to cross-examine other witnesses. Two rulemaking hearings were held in 1972. The first, on radioactive plant effluents, lasted 17 days and was rather easily resolved based on conservative assumptions. The second, on the Interim Acceptance Criteria for emergency core cooling system, began in January 1972 and took 125 days over 23 months. Scientists and engineers representing government, industry, and intervenor organizations were heard and, with their lawyers, cross-examined one another. Procedural matters often dominated. The hearing record is more than 22,000 pages. From this record and the recommendations of the Hearing Board, the AEC issued "final criteria" on January 4, 1974.[24]

In 1973, before the "final criteria" were issued, a second series of experiments were completed. These tests were called 1½ semiscale because a loop simulating the unbroken loops of a reactor was added to the 1/2 (broken) loop. This time water was injected through the unbroken loop, as would occur in the emergency core cooling system of actual power reactors, which have two, three, or four loops. The simulated core was successfully cooled in all tests while the steam escaped through the broken loop as predicted by computer models.

Section 50.46 and Appendix K of 10 CFR 50 defined the final outcome of the rulemaking by specifying that,[1] following postulated LOCAs, emergency core cooling system must assure:

- Peak cladding temperature cannot exceed 2200°F (1204°C),
- Oxidation cannot exceed 17% of the cladding thickness,
- Hydrogen generation from hot cladding-steam interaction cannot exceed 1% of its potential,
- The core geometry must be retained in a coolable condition
- Long-term cooling must be provided.

At the time the "final criteria" were developed, computer codes had limited capabilities for simulating the complex phenomena associated with large LOCAs. To ensure that calculations would be conservative, the rule also provided calculational restraints, some of which are:

- a multiplier of 1.2 on the decay heat rate
- prohibition on a return to nucleate boiling during blowdown, and
- conservative assumptions on emergency core cooling system delivery to the lower plenum.

During the period from 1971 through 1974, the AEC and its successor the NRC reviewed the emergency core cooling system designs of every operating plant. When necessary, retrofitting and upgrading of the emergency core cooling systems were required or the operating power level was reduced to assure compliance with the final criteria. Indian Point 1 was shut down in October 1974 because of an inadequate emergency core cooling system. All new plants and plants under construction were required to meet the final criteria.

The twenty years that followed the semiscale test brought several independent assessments of the emergency core cooling system criteria. NRC sponsored additional experiments to investigate both individual phenomena and system performance, and the development of advanced computer codes that could provide improved simulations of LOCAs. The experimental and computational efforts provided the technical basis for a revised rule for the acceptance of emergency core cooling systems, which were approved by the NRC in September 1988.[25] The revised rule retains the acceptance criteria based on peak cladding temperature, cladding oxidation, and hydrogen generation; however, it allows the use of best-estimate computer codes for evaluating those parameters. If best-estimate methods are used, the revised rule requires that the uncertainty of the calculations be quantified to a high level of probability and that the uncertainty be included when comparing calculated results with the acceptance limits provided in 10 CFR 50. This allows much more realistic estimates of plant safety margins.

1.3.7 The Energy Reorganization Act of 1974

The AEC's efforts under Chairman Schlesinger to narrow the divisions between nuclear proponents and critics and to recover the AEC's regulatory credibility produced, at best, mixed results. The AEC suffered from the general disillusionment with the "establishment" that prevailed by the late 1960's largely as a result of the Vietnam war. Major differences between the AEC and environmentalists remained regarding emergency core cooling system effectiveness, thermal pollution, and hazards of low-level radiation.

Another issue that undermined confidence in the AEC in the early 1970s was its approach to high-level radioactive waste disposal. In 1970, in response to increasing expressions of concern about the lack of a policy for high-level waste disposal, the AEC announced that it would develop a permanent repository for nuclear wastes in an abandoned salt mine near Lyons, Kansas. It aired its plans without conducting thorough geologic and hydrologic investigations. The suitability of the site was soon challenged by the state geologist of Kansas and other scientists. The uncertainties about the site generated a bitter dispute between the AEC on the one side and members of Congress and state officials from Kansas on the other. It ended in 1972 in great embarrassment for the AEC. The reservations of those who opposed the Lyons location proved to be well-founded, and numerous well holes were found to have penetrated the salt bed.

In addition to debates over emergency core cooling system and high-level waste disposal, questions over reactor design and safety, quality assurance, the probability of a major reactor accident, and other issues fueled the controversy over nuclear power. The number of contested hearings for plant licenses steadily grew. The AEC came under increasing attacks for its dual responsibilities for developing and regulating the technology. The question of creating separate agencies to promote and to regulate the civilian uses of nuclear energy had arisen within a short time after passage of the 1954 Atomic Energy Act, but in the early stages of nuclear development it had seemed premature and unwarranted. It gained greater support in later years as both the nuclear industry and antinuclear sentiment grew. One of President Nixon's responses to the Arab oil embargo and the energy crisis of 1973-4 was to ask Congress to create a new agency that could focus on, and presumably speed up, the licensing of nuclear plants. After much debate, in 1974 Congress passed the Energy Reorganization Act, which divided the AEC into the Energy Research and Development Administration (ERDA), predecessor to the current Department of Energy, and the Nuclear Regulatory Commission.

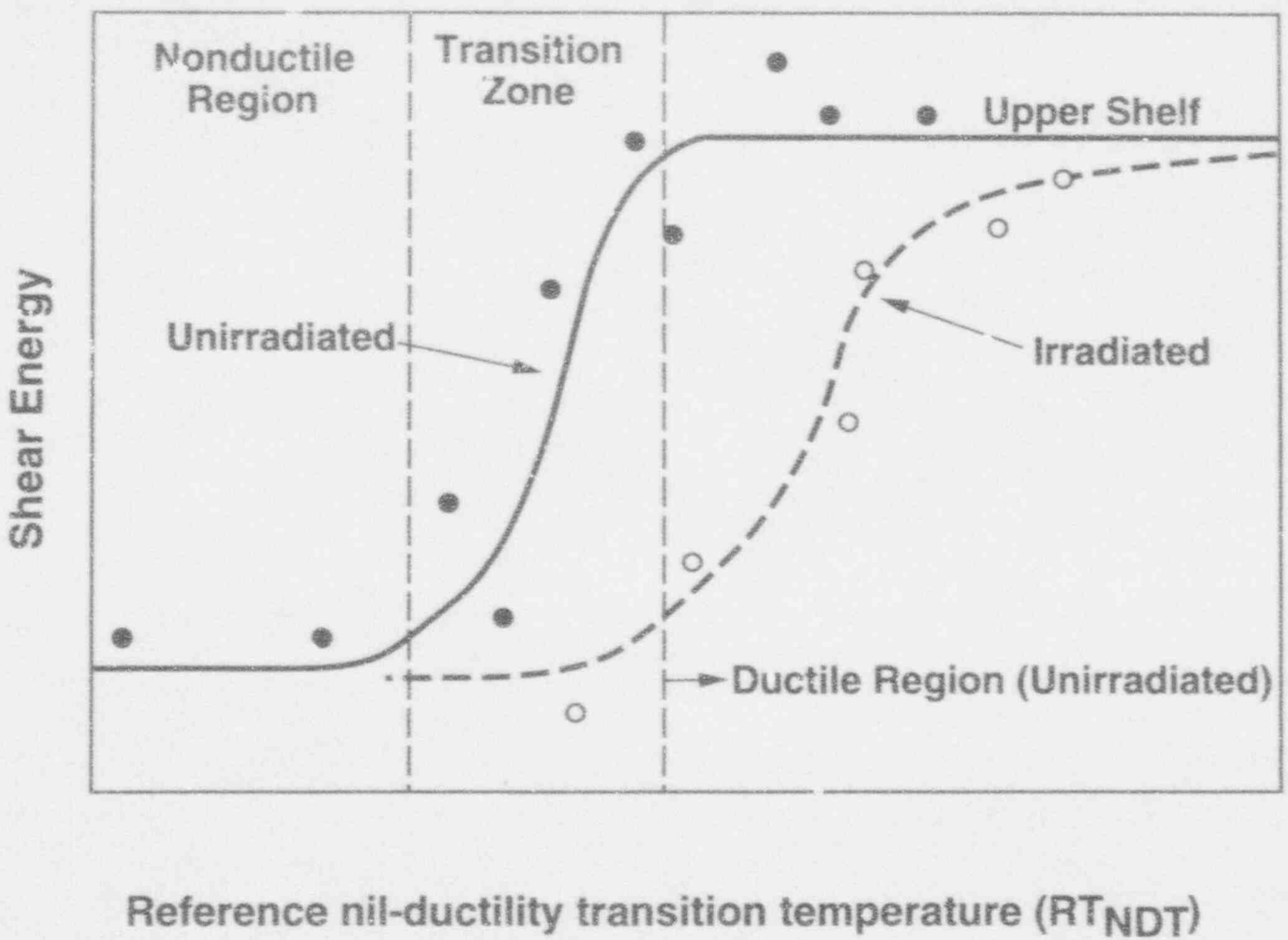


Figure 1.3-1 Shift in nil-ductility transition temperature

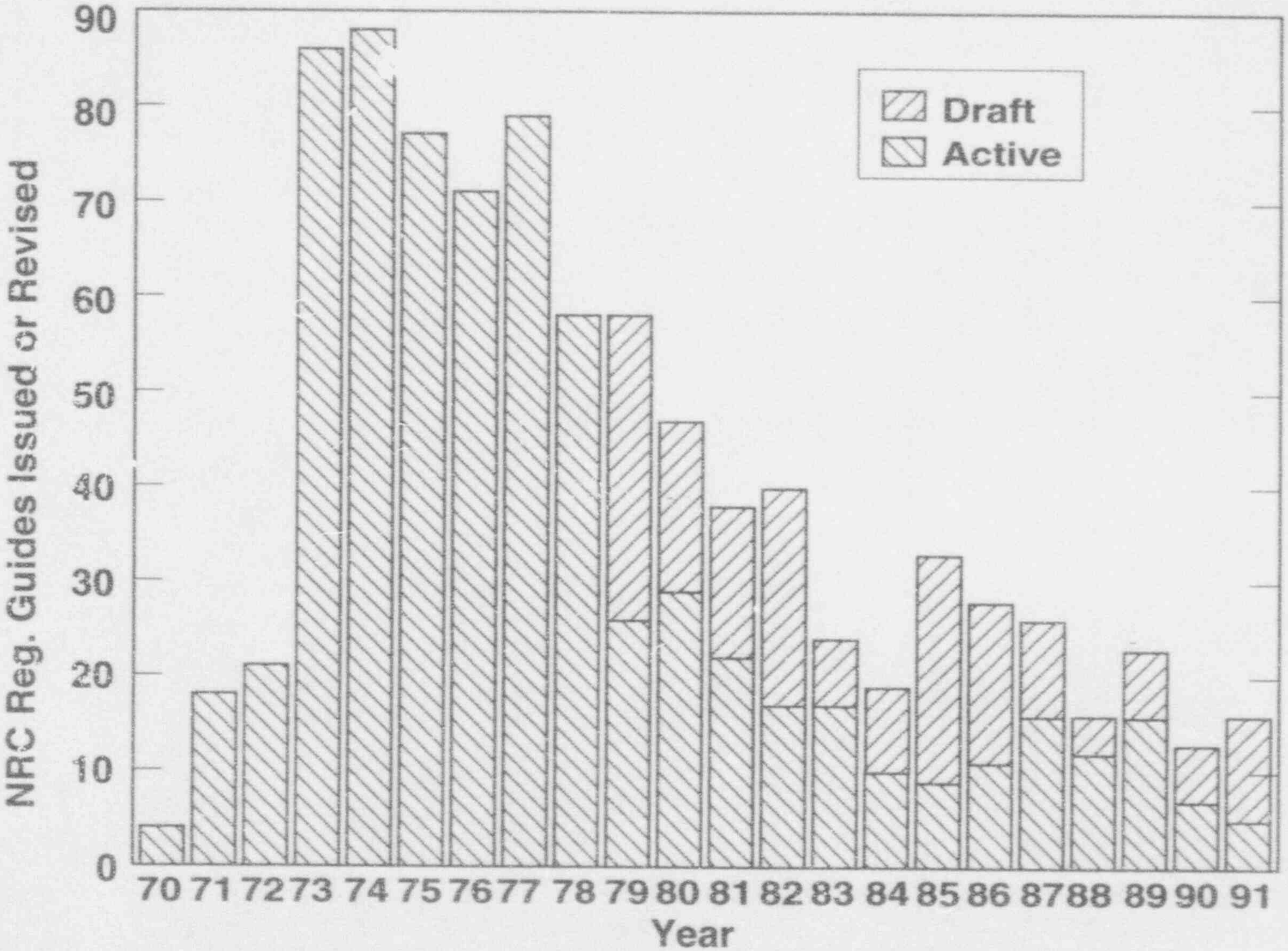


Figure 1.3-2 Number of regulatory guides issued per year

References for Section 1.3

1. Theodore A. Meyer, *The Evolution of Reactor Vessel PTS--A Catalyst to the Advancement of Technology*, Mechanical Engineering (June 1984), p37.

2. George T. Mazuzan and Samuel Walker, *Controlling The Atom: The Beginning of Nuclear Regulation 1946-1962*, University of California Press (1984), p217.

3. American Society for Testing and Materials (ASTM) Standards E-23, E-184, E-185, and E-208, Philadelphia, PA.

4. Advisory Committee on Reactor Safeguards (ACRS) letter on Reactor Pressure Vessels (November 24, 1965), reproduced in *Nuclear Reactor Safety: On the History of the Regulatory Process* by David Okrent, (1981) pp88-89.

5. Advisory Committee on Reactor Safeguards, *Report on the Integrity of Reactor Vessels for Light-Water Power Reactors*, WASH-1285 (January 1974).

6. U.S. Nuclear Regulatory Commission, Statement of Considerations for Proposed Revision to 10 CFR 50.61, *Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events*, (May 6, 1991).

7. Title 10, Code of Federal Regulations 50, criterion 61, *Fracture Toughness Req rements for Protection against pressurized Thermal Shock events.* (Jan 1, 1991)

8. ACRS subcommittee meeting minutes (June 3, 1966), reproduced in *Nuclear Reactor Safety: On the History of the Regulatory Process* by David Okrent,(1981), pp 99-101.

9. David Okrent, *Nuclear Reactor Safety: On the History of the Regulatory Process*, The University of Wisconsin Press, Madison, WI (1981), pp112-121.

10. May, John, *The Greenpeace Book of the Nuclear Age: The Hidden History, The Human Cost*, Greenpeace Communications Ltd., London, 1989.

11. Proposed General Design Criteria for Construction Permits for Nuclear Power Plants, U.S. Atomic Energy Committee, *Federal Register* (November 22, 1965).

12. Proposed General Design Criteria for Nuclear Power Plants, U.S. Atomic Energy Committee, *Federal Register* (July 10, 1967).

13. Design Criteria for Nuclear Power Plants, Title 10 Code of Federal Regulations Part 50, U.S. Atomic Energy Committee, *Federal Register* (February 19, 1971).

14. "Net Positive Suction Head for Emergency Core Cooling Containment Heat Removal System Pumps (Safety Guide 1.1)" U.S. Nuclear Regulatory Commission, Regulatory Guide 1.1., November 1970.

15. American National Standards Institute (ANSI N45.2), *Quality Assurance Program Requirements for Nuclear Power Plants*.

16. Branch Technical Position, Auxiliary Power Conversion Systems Branch, 9.5-1, *Guidelines for Fire Protection for Nuclear Power Plants*

17. Regulatory Guide 1.120, *Fire Protection Guidelines for Nuclear Power Plants*, draft for comment, (June 1976).

18. Title 10, Code of Federal Regulation 50, Appendix R, *Fire Protection Program for Nuclear Power Plants Operating Prior to January 1, 1979.*

19. Judge J. Skelly Wright, Calvert Cliffs decision, US Court of Appeals for the District of Columbia (July 23, 1971), noted in *An Outline History of Nuclear Regulation and Licensing 1946-1979* by Mazuzan and Trask, (April,1979), p68.

20. James R. Schlesinger, speech delivered to industry groups in Bal Harbour, Florida (October 20, 1971), cited in *A Short History of the Regulatory Process 1946-1990* by J. Samuel Walker, (June 1991), p34.

21. *Licensing and Regulatory Policy and Procedures for Environmental Protection*, Title 10 Code of Federal Regulations Part 51, U.S. Atomic Energy Commission, *Federal Register* (December 1, 1971).

22. George T. Mazuzan and Roger R. Trask, *An Outline History of Nuclear Regulation and Licensing 1946-1979*, Historical Office, Office of the Secretary, Nuclear Regulatory Commission (April, 1979), p71.

23. *Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled Nuclear Power Reactors*, Title 10 Code of Federal Regulations Part 51.46, U.S. Atomic Energy Commission, *Federal Register* (January 4, 1974).

24. *Emergency Core Cooling Systems; Revisions to Acceptance Criteria, Federal Register 53* (180), pp35996-36005 (September 16, 1988).

1.4 1975-Present, Emphasis on Severe Accidents and Risk

The NRC began operating as a separate agency in January 1975. It performed the same licensing and rule-making functions that the AEC's regulatory staff had discharged for two decades. However, under the Energy Reorganization Act, the NRC's statutory mandate was clearly focused on ensuring the safety of nuclear power. Unlike the AEC's regulatory staff, the NRC was the final arbiter of regulatory issues; its judgment on safety questions was less susceptible to being compromised by developmental priorities.

The NRC devoted a great deal of attention during its first few months to organizational tasks. At the same time it carried out a variety of regulatory responsibilities. It continued to review plant applications and to issue construction permits and operating licenses for new units. It also dealt with the identification of generic safety issues, the safety of the nuclear fuel cycle, the safeguarding of nuclear materials, and the development of procedures for granting licenses for the export of nuclear materials. Along with these matters, two events, which commanded particular attention during the early months of the NRC's existence, were the Browns Ferry fire and the publication of the final version of the Reactor Safety Study that the AEC had commissioned in 1972.

1.4.1 The Browns Ferry Fire

On March 22, 1975, a major fire occurred at TVA's Browns Ferry nuclear plants near Decatur, Alabama. This event was a close call that very nearly led to core damage. In the process of looking for air leaks in an area containing trays of electrical cables that supplied power to the plants' control room and safety systems, a technician set off the fire. He used a lighted candle to conduct the search, and the open flame ignited the insulation around the cables. The fire burned for over seven hours and nearly disabled the safety equipment of one of the two affected units. The accident was a blow to the public image of nuclear power and the recently-established NRC. It focused new attention on protecting against fires that could threaten plant safety and on the possibility of "common-mode failures," in which a single breakdown could initiate a chain of events that incapacitated even redundant safety features. A detailed description of the fire and subsequent events is included as Section 2.3.

1.4.2 The Reactor Safety Study

The Reactor Safety Study was prompted in part by a request from Senator John Pastore for a comprehensive assessment of reactor safety. The AEC's first response to this request was the WASH-1250 report entitled *The Reactor Safety Study of Nuclear Power Reactors (Light Water-Cooled) and Related Facilities*, which was published in final form in July 1973.[1] However, WASH-1250 did not provide a probabilistic assessment of risk as requested in Senator Pastore's letter. At the time, relevant probabilistic estimates were quite limited in scope and/or highly subjective. For example, in a policy paper dated November 15, 1971, to the commissioners proposing an approach to the preparation of environmental reports, the regulatory staff estimated that the probability of accidents leading to substantial core meltdown was 10^{-8} per reactor-year.[2] In retrospect, this was a highly optimistic estimate, but it typifies the degree to which meltdown accidents were considered "not credible."

In the summer of 1972, the AEC initiated a major probabilistic study, the Reactor Safety Study (RSS). Professor Norman C. Rasmussen of the Massachusetts Institute of Technology served (half-time) as the study director. Saul Levine of the AEC served as full-time staff director of the AEC employees that performed the study with the aid of many contractors and consultants. A draft Reactor Safety Study report, WASH-1400, was issued by the AEC for comment in August 1974. The draft drew extensive comments from government, industry, environmental groups, nuclear critics, and the public. The final report, WASH-1400 (NUREG 75/014), was issued in October 1975.[3]

The Reactor Safety Study attempted to make a realistic estimate of the potential effects of LWR accidents on the public health and safety. One BWR, Peach Bottom Unit 2, and one PWR, Surry Unit 1, were analyzed in detail. The Reactor Safety Study team used previous information from the Department of Defense and NASA to predict the effect of failures of small components in large, complex systems. Events that could potentially initiate core melt accidents were first identified. Event trees were then used to delineate possible sequences of successes or failures of systems provided to prevent core meltdown and/or the release of radionuclides. Fault trees were used to estimate the probabilities of system failures from available data on the reliability of system components. Using these techniques, thousands of possible core melt accident sequences were assessed for their occurrence probabilities. The consequences of such accident sequences were then estimated to complete the risk assessment.

The Reactor Safety Study indicated that risks to the public from potential U.S. LWR accidents were small compared to other risks encountered in a complex technological society. Other sources of risk that were compared in the study included fires, explosions, toxic chemical releases, dam failures, airplane crashes, earthquakes, tornadoes, and hurricanes. Figures 1.4-1 and 1.4-2 show these risk comparisons. These figures are interpreted in the following manner:

1. Pick a point on one of the curves.
2. The ordinate represents the frequency with which a consequence greater than or equal to the corresponding abscissa value will occur.

For example, in Figure 1.4-1, the probability of a nuclear power plant accident involving 1000 or more fatalities in any given year is approximately 10^{-6}.

In these figures, it is assumed that there are 100 power reactors and that they all have risks equal to the average risks for Surry and Peach Bottom. There is no evidence to support this assumption; however, the other 98 reactors would have to be orders of magnitude worse than Surry and Peach Bottom for the general conclusions to be rendered invalid. While the risks from nuclear power appear to be very low, the Reactor Safety Study did indicate that core melt accidents were more likely than previously thought ($\sim 5 \times 10^{-5}$ per reactor year for Surry and Peach Bottom), and that LWR risks are mainly attributable to core melt accidents. The Reactor Safety Study also demonstrated the wide variety of accident sequences (initiators and ensuing multiple equipment failures and/or operator errors) that have the potential to cause core melt. In particular, the report indicated that, for the plants analyzed, accidents initiated by transients or small LOCAs were more likely to cause core melt than the traditional design-basis LOCAs. Finally, the Reactor Safety Study investigations into containment failure suggested that different containment types (e.g., Mark I BWR versus subatmospheric) may differ in their capability to withstand core melt accidents (for which they were not designed).

The preceding findings have withstood the test of time; however, the Reactor Safety Study was to receive considerable valid criticism. In June 1977, the NRC appointed a Risk Assessment Review Group (the Lewis Committee, named after Harold Lewis, Chairman of the American Physical Society's

Study Group on Light Water Reactors) to review WASH-1400.[4] The review group's report to the Commission in September 1978 was highly critical:

> *We have found a number of sources of both conservatism and nonconservatism in the probability calculations in WASH-1400, which are very difficult to balance. Among the former are an inability to quantify human adaptability during the course of an accident, and a pervasive regulatory influence in the choice of uncertain parameters, while among the latter are nagging issues about completeness, and an inadequate treatment of common cause failure. We are unable to define whether the overall probability of a core melt given in WASH-1400 is high or low, but we are certain that the error bands are understated. We cannot say by how much. Reasons for this include an inadequate data base, a poor statistical treatment, an inconsistent propagation of uncertainties throughout the calculation, etc.*

While the Lewis Committee was critical of the quantitative results of WASH-1400, it provided positive encouragement for future use of the methods. The committee report states,

> *We do find that the methodology, which was an important advance over earlier methodologies applied to reactor risks, is sound, and should be developed and used more widely under circumstances in which there is an adequate data base or sufficient technical expertise to insert credible subjective probabilities into the calculations. ... Proper application of the methodology can therefore provide a tool for the NRC to make the licensing and regulatory process more rational, ...*

The NRC commissioners, seeming not to understand these conclusions, issued a January 1979 policy statement that seemed to discredit the entire Reactor Safety Study. The statement (a) withdrew any past endorsement of the Executive Summary of the report, (b) agreed that the peer review process for WASH-1400 was inadequate and (c) accepted the conclusion that WASH-1400's absolute values of risks should not be used uncritically, and (d) agreed that the numerical estimate of the overall risk of reactor accidents was unreliable.[5]

In spite of recommendations by the Advisory Committee on Reactor Safeguards and others that severe accident research and Reactor Safety Study methods be applied to improve the safety of reactors in operation and under construction, it was not until after the accident at Three Mile Island that serious efforts to address severe accident issues were undertaken.

1.4.3 TMI-2 Accident

On March 28, 1979, an accident at Unit 2 of the Three Mile Island nuclear station near Harrisburg, Pennsylvania forever put to rest the notion that severe nuclear power plant accidents were incredible. Technical details of the accident are presented in later modules. In summary, as a result of a series of mechanical failures and human errors, the accident uncovered the reactor's core and melted about half of it. The principal mechanical failure contributing to the accident was a pressure relief valve that stuck open and allowed large volumes of reactor coolant to escape. The reactor operators misread the signs of a loss-of-coolant accident. Although the emergency core cooling system was automatically actuated, the operating crew reduced the emergency core cooling system flow to a trickle for several hours. By the time that the nature of the accident was recognized and coolant flow to the reactor vessel was re-established, the reactor core had suffered irreparable damage. However, despite the substantial degree of clad oxidation and core melting that occurred, and the combustion of hydrogen from the oxidation in containment, the containment building kept the radionuclide releases to the environment very low. Of the 66 million curies of radioactive iodine-131 in the reactor at the time of the accident, only 14 or 15 curies escaped to the environment.

Uncertainty about the causes of the accident, confusion about how to deal with it, and contradictory information and appraisals of the level of danger in the days following the accident often made utility and government authorities appear inept, deceptive, or both. Press accounts fed public fears and fostered a deepening perception of a technology that was out of control. Two days after the onset of the accident (long after core cooling was restored), the Governor of Pennsylvania issued a pair of recommendations -- initially for sheltering within 10 miles (16 km) and later for closing schools and evacuating pregnant women and pre-school children within 5 miles (8 km). Despite the limited scope of the recommended evacuation, there was a spontaneous evacuation involving some 144,000 persons from 50,000 households. Approximately two-thirds of the households within 5 miles (8 km) of TMI-2 had at least one person evacuate. After one week the decision was made to re-open the schools, the evacuation order was lifted, and most of the evacuees returned.

Almost immediately after the TMI-2 accident, the government and the nuclear industry sought to identify the causes and began taking steps to reduce the likelihood of future accidents. Extensive corrective actions for U.S plants were required by the NRC's TMI Action Plan[6] (see Section 1.4.6). The first and most prominent formal investigation of the accident was conducted by the President's Commission on the Accident at Three Mile Island, also known for its chairman, John Kemeny.[7] Two important NRC-sponsored investigations were by the Special Inquiry Group or Rogovin Committee, which addressed broad accident issues, and the in-house Lessons Learned Task Force (NUREG-0585), which addressed concerns most germane to the NRC's own activities.[8,9] In their reports, the investigators emphasized many deficiencies for which corrective actions were already in progress. More significantly, the reports strongly criticized the NRC, the utility, the nuclear industry, and the reactor operators. The TMI-2 nuclear steam supply system design was found to have contributed to the accident much less than the human factors and attitudes involved. The investigators also validated that the major health consequence was

> *on the mental health of the people living in the region,"* including *"immediate short-lived mental distress produced by the accident.*

A majority of the President's Commission supported a moratorium on the licensing of new nuclear power plants; however, such a moratorium was not recommended in the Commission's final report due to a lack of consensus on guidelines for lifting the moratorium once it was put into force. A de facto moratorium ensued, however, as the NRC delayed granting reactor licenses pending resolution of relevant issues and lessons learned from TMI-2.

1.4.4 NRC Restructuring

The President's Commission was highly critical of the NRC and found

> *that the NRC is so preoccupied with the licensing of (new) plants that it has not given primary consideration to overall safety issues.*

In response to such criticisms, the NRC reorganized to strengthen accountability and give higher priority to plant safety. The NRC emphasis was shifted from licensing new plants to regulating operating plants. This was consistent with the work load resulting from post-accident modifications to existing plants, the de facto moratorium on licensing new plants, and the cancellations and lack of new orders that followed the TMI accident. In addition, over several years, most of the NRC's scattered headquarters offices in the Washington, DC metropolitan area were consolidated into a single building complex placing individuals with safety-related responsibilities (e.g., research, operating experience, and inspection and enforcement) in much closer proximity to each other.

The need for "increased emphasis and improved management" of NRC's inspection and enforcement functions was addressed by developing a strengthened enforcement policy with substantial penalties for "failure to report new 'safety-related' information" and for rule violations, expanding the resident inspector program to station at least two NRC inspectors at each plant site, and regularly conducting team inspections. These inspectors were now more concerned with understanding plant operations and safety than administrative compliance. One comprehensive team inspection is the Systematic Assessment of Licensee Performance (SALP) program which rates plants on a scale of one-to-three in each of seven areas. Systematic assessment of licensee performance, together with other NRC activities, were used to enforce higher organizational and management standards for licensees.

The NRC established a new Office for Analysis and Evaluation of Operational Data to systematically review information from the performance of operating plants. This action was in response to the belated recognition that malfunctions similar to those at TMI had occurred at other plants, but the information had not been assimilated or disseminated in a way that could have averted the TMI accident.

In addition to the organizational changes described above, the NRC initiated major changes affecting operator training and licensing, operating plant configurations, emergency response, severe accident research, plant licensing, and regulatory decision making. These initiatives are discussed in later sections.

1.4.5 Nuclear Industry Restructuring

The President's Commission concluded that the nuclear industry

> *must dramatically change its attitudes towards safety and regulations"* and *"must also set and police its own standards of excellence to ensure the effective management and safe operation of nuclear power plants.*

The Commission charged that the industry had a mind-set that plants were *"sufficiently safe"* and emphasized that this attitude

> *must be changed to one that says nuclear power is by its very nature potentially dangerous, and ... one must continually question whether the safeguards already in place are sufficient to prevent major accidents.*[7]

The industry response to the accident demonstrated a significant change in attitude. Three key issues were singled out for prompt attention: ineffective reactor safety information exchange, difficult operator-machine interfaces, and inadequate operator training. The U. S. nuclear utilities established several organizations to deal with these issues in the near term and with a broader spectrum of technical and management issues in the longer term.

The utilities established the Nuclear Safety Analysis Center (NSAC) under the Electric Power Research Institute (EPRI) to develop strategies for minimizing the possibility of future reactor accidents and to answer generic reactor safety questions. Nuclear Safety Analysis Center was also charted to recommend changes in safety systems and operator training, to act as a clearing house for technical information, to perform analyses of significant reactor transients, and to participate in performing probabilistic risk assessments.

The utilities also formed the Institute of Nuclear Power Operations (INPO). The Institute has served to establish industrywide qualifications, training requirements, and testing standards first for nuclear-plant operators and subsequently for technicians, engineers, and managers. The INPO plant evaluation program serves an audit and testing function for utility staffs. INPO provides guidance and training for those responsible for training programs, rather than dealing directly with individual operating personnel. Compliance with INPO criteria is judged by the National Nuclear Accrediting Board, an independent organization with expertise that encompasses training, university education, management, and regulation from both inside and outside the nuclear-utility industry. Each U. S. utility becomes a member of the INPO-chartered National Academy of Nuclear Training when accreditation is earned at each of its reactor sites for ten designated training programs. Continuing membership requires reaccreditation every four years.

The industry later established the Nuclear Utility Management and Resources Council (NUMARC) to deal with personnel-related and licensing issues, support self-initiated, self-policed plant performance and safety improvements.

The utilities also established a self-sponsored insurance program that provides coverage for replacement power costs in the event of a prolonged post-accident reactor shutdown. This, of course, is intended to limit the financial consequences of accidents (e.g., in 1980 the cost for the TMI-2 recovery was estimated at $973 million, exclusive of replacement power costs) and provide more stability on an industrywide basis.

1.4.6 Plant Modifications

The TMI accident led to a number of investigations of the adequacy of design features, operating procedures, and personnel of nuclear power plants to provide assurance of no undue risk regarding severe reactor accidents. The report "NRC Action Plan Developed as a Result of the TMI-2 Accident" (NUREG-0660, May 1980) describes a comprehensive and integrated plan involving many actions that serve to increase safety when implemented by operating plants and plants under construction.[6] The items approved for implementation by NRC are identified in the report "Clarification of TMI Action Plan Requirements" (NUREG-0737, November 1980).[10] The staff issued further criteria on auxiliary feedwater system improvements (derived from NUREG-0667), and instrumentation (Regulatory Guide 1.97, Revision 2).[11,12] The TMI Action Plan led to requirements for over 6,400 separate action items, an average of 90 action items per plant. There were 132 different types of action items approved. Of these, 39 involved equipment backfit items, 31 involved procedural changes, and 62 required analyses and reports.

Many of the action items addressed small-break and transient initiated accidents. Their significance had previously been identified by WASH-1400 and its reviews. Traditionally, historical attention had been on the design-basis large break LOCA. The emphasis on small breaks and transients was immensely affected by the TMI-2 accident. Many procedural, software, and hardware modifications were implemented to detect and mitigate such accidents as well as to monitor radiation-releases and other post-accident symptoms.

Considerable emphasis was placed on improving the operator-machine interface. Control rooms were reviewed for adequacy of the operator-machine interface as well as for habitability during accidents. Detailed analysis of operator tasks supported the development of new symptom-based operating procedures and improvements in control-panel hardware arrangements and markings, alarm and annunciator priorities and configurations, and computer-based data collection and display systems. Safety parameter display systems (SPDS) were installed to aid diagnosis and decision making. One example of a safety parameter display system, called a "PT-plot," graphs PWR primary and secondary system pressures and temperatures highlighting regions corresponding to over-cooling transients, under-cooling transients, and loss-of-coolant accidents. Emergency safety feature actuation systems were improved to provide an unambiguous control-room display of the status of all safety systems.

The TMI-2 accident led to increased emphasis on the importance of containment survival during severe accidents. While the changes to containments were not as numerous as the changes to other plant systems, additional hydrogen control measures were implemented for some plants. These changes are discussed in more detail in Module 4.

1.4.7 Operator Training and Licensing

The TMI-2 accident highlighted the importance of operators in responding to evolving accident conditions. In some countries, a "hands off" approach is taken, where the operators do not take action for a specified time period, so as not to make a situation worse before they understand what is going on. In the U.S., operators are actively involved from the outset, and it is important that the actions taken be positive ones. Following the TMI-2 accident, the NRC developed stringent new requirements for operator training, testing, and licensing, and for shift scheduling and overtime. In cooperation with industry groups, NRC promoted the increased use of reactor simulators. Before the TMI-2 accident, it was common for operators to train for requalification at a "generic" simulator, spending 90% of their simulator time on normal operations with the remainder emphasizing the design-basis large-break LOCA. Now each plant is required to have a plant-specific simulator, and simulator time is spent primarily on covering the entire spectrum of postulated transients and accidents. The NRC added extensive simulator exercises to the traditional reactor-operator (RO) and senior-reactor-operator (SRO) exams and plant walk-throughs. Annual requalification exams, similar to the initial NRC exams are now administered by the utility, subject to NRC approval and validation. In addition, the NRC added requirements for a new Shift Technical Adviser (STA) to provide engineering capability on each control-room shift.

1.4.8 Emergency Response Improvements

Given the confusion and uncertainty experienced during the TMI-2 accident and the subsequent evacuation, the NRC took steps to upgrade emergency preparedness and planning. New rules and guidelines were developed. Emergency response capabilities were expanded with improved plans, equipment, and facilities. Emergency response personnel from industry, the NRC, the Federal Emergency Management Agency (FEMA), and the local organizations now receive extensive training and are evaluated by periodic drills. Site plans and procedures address

- accident recognition and classification
- declaration and initial notification
- communication networks
- response readiness.

The NRC now requires dedicated emergency operations facilities (NUREG-0737, Rev. 1) to be constructed, maintained, and tested near each plant.[13] During any future accident, a joint information center would provide a common location for utility, federal, state, and local representatives to communicate with the media. Public notification and information channels have been established.

1.4.9 Seabrook and Shoreham

In the aftermath of the TMI-2 accident, the NRC temporarily suspended the granting of full power operating licenses. This de facto moratorium ended 16 months after the accident (August 19… when a full-power operating license was issued to North Anna-2. (Granting of low power licenses had resumed earlier, starting with Sequoyah.) During the rest of the 1980s, the NRC granted full-power licenses to over forty other reactors, most of which had received construction permits in the mid-1970s. In 1985 it authorized the undamaged Three Mile Island Unit 1, which had been shut down for refueling at the time of the TMI-2 accident, to resume operation.

Although many of the licensing actions aroused little opposition, others triggered major controversies. The two licensing cases that precipitated what were perhaps the most bitter, protracted, and widely publicized debates were Seabrook in New Hampshire and Shoreham on Long Island, New York. The key, though hardly the sole, issue in both cases was emergency planning. The Three Mile Island accident had vividly demonstrated the deficiencies in existing procedures for coping with an off-site nuclear emergency. The lack of effective preparation had produced confusion, uncertainty, and panic among members of the public faced with the prospect of exposure to radiation releases from the plant. After the accident, the NRC, prodded by Congress to improve emergency planning, adopted a rule that required each nuclear utility to come up with a plan for evacuating the population within a ten mile radius of its plant(s) in the event of a reactor accident.[14] The rule applied to plants in operation and under construction. It called for plant owners to work with state and local police, fire, and civil defense authorities on emergency plans that would be tested and evaluated by the NRC and the Federal Emergency Management Agency (FEMA). The NRC expected cooperation between federal, state and local government officials to upgrade emergency plans and provide better protection for the public should a serious nuclear accident occur.

The NRC did not, however, anticipate that state and local governments would try to prevent the operation of nuclear plants by refusing to participate in emergency preparations. That was precisely what the states of New York and Massachusetts sought to do in the cases of Shoreham and Seabrook. In New York, Governor Mario M. Cuomo and other state officials claimed that it would be impossible to evacuate Long Island if Shoreham suffered a major accident. Therefore, the state refused to join in emergency planning or drills. The NRC granted Shoreham a low-power operating license, but the state and the utility, Long Island Lighting, eventually reached a settlement in which the company agreed not to operate the plant in return for concessions from the state.

A similar issue arose at Seabrook, though the outcome was different. The plant is located in the state of New Hampshire, but the ten mile emergency planning zone extends across the state line into Massachusetts. By the time that construction of the plant was completed, Massachusetts Governor Michael S. Dukakis, largely as a result of Chernobyl, had decided that he would not cooperate with emergency planning efforts for Seabrook. New Hampshire officials worked with federal agencies to prepare an emergency plan, but Massachusetts, arguing that crowded beaches near the Seabrook plant could not be evacuated in the event of an accident, refused. As a result of the positions of New York regarding Shoreham and Massachusetts regarding Seabrook, in 1988 the NRC adopted a "realism rule," which was grounded on the premise that, in an actual emergency, state and local governments would make every effort to protect public health and safety.[5] Therefore, in cases in which state and/or local officials declined to participate in emergency planning, the NRC and Federal Emergency Management Agency would review and evaluate plans developed by the utility. On that basis, the NRC issued an operating license for the Seabrook plant. The arguments that raged over emergency planning and other issues at Shoreham and Seabrook attracted a great deal of attention, spawned heated controversy, and raised anew an old question of the relative authority of federal, state, and local governments in licensing and regulating nuclear plants.

1.4.10 Severe Accident Research

Following TMI-2, NRC research was redirected to focus on severe accidents. This research had several objectives, including:

1. to obtain a better understanding of the physical phenomena of severe accidents,
2. to develop models of these phenomena in order to predict the ways that severe accidents might progress,
3. to develop more realistic estimates of the radionuclide releases that could result from severe accidents, and
4. to examine available data sources and existing PRAs to identify the important accident sequences for various classes of reactors.

In order to meet these objectives, major research programs were started at the national laboratories and universities. Eventually the results of these efforts were integrated together in a major PRA for five reference plants (NUREG-1150).[15] NUREG-1150 essentially replaces the Reactor Safety Study in terms of providing current severe accident perspectives and insights. Both the severe accident research and NUREG-1150 are discussed in more detail in later modules.

The Industry Degraded Core Rulemaking (IDCOR) Program, under the sponsorship of the Atomic Industrial Forum, was conducted in parallel with the NRC research efforts. The Industry Degraded Core Rulemaking group concentrated on developing models for assessing the risks of severe accidents. Industry Degraded Core Rulemaking models were used to analyze four of the five NUREG-1150 reference plants. This facilitated the identification and resolution of modeling differences.

1.4.11 Severe Accident Policy

In August 1985, when the bulk of the actions required by the TMI Action Plan had been completed, the U.S. Nuclear Regulatory Commission issued a policy statement on severe accidents.[16] A policy statement is not a regulation in the sense that it does not impose specific requirements, but rather provides the Commission's rationale and motivation for future regulatory positions. On the basis of available information from the Severe Accident Research Program, the Commission concluded that existing plants pose no undue risk to the public and that no immediate additional regulatory changes were recommended for these plants to address severe accidents. Note that many changes had already occurred, such as changes in operator training and implementation of hydrogen control measures for some containment types. Even with these changes and the stated finding of no undue risk, the NRC recognized that there was still much uncertainty in the phenomena associated with severe accidents, and the Severe Accident Policy included rationale for continuation of the Severe Accident Research Program. If the research uncovers further issues or questions of undue risk, then the Commission can act at that time.

Past research has indicated the plant-specific nature of severe accident vulnerabilities. Therefore, the Severe Accident Policy stated the desirability of performing a systematic examination of each nuclear power plant in order to identify potential plant-specific vulnerabilities to severe accidents. Three years later, the NRC issued a generic letter (88-20) and guidance (NUREG-1335), which called for licensees to perform a systematic Individual Plant Examination (IPE) of each nuclear power plant operating or under construction.[17,18] The stated purpose of the Individual Plant Examination was to have each utility:

1. develop an appreciation of severe accident behavior;
2. understand the most likely severe accident sequences that could occur at its plant;
3. gain a more quantitative understanding of the overall probabilities of core damage and fission product releases; and
4. if necessary, reduce the overall probabilities of core damage and fission product releases by modifying, where appropriate, hardware and procedures that would help prevent or mitigate severe accidents.

The Individual Plant Examination Generic Letter makes it clear that a major benefit from this activity is the education of the utility staff in the area of severe accidents. The utilities are expected to perform much of the analysis in-house and not rely solely on consultants for performing the analysis.

Individual Plant Examination results were to be reported to the NRC within three years according to guidance provided in NUREG-1335. The results of the Individual Plant Examinations that have been received are currently being reviewed by the NRC. These results will be used, in part, to deal with Unresolved Safety Issues and Generic Safety Issues. The Individual Plant Examination submittals will indicate whether particular issues apply to the plant and the utility's case for resolution. If vulnerabilities are found, the utility is to provide a plan and schedule for resolving the problem.

The severe accident policy recommends that new plants be shown to be acceptable for severe accidents by meeting specified criteria and procedural requirements, which include completion of a Probabilistic Risk Assessment (PRA) and consideration of the severe accident vulnerabilities that the PRA exposes.

1.4.12 Chernobyl

On April 26, 1986, unit 4 of the nuclear power station at Chernobyl in the Ukraine underwent a violent explosion that destroyed the reactor, blew its top off, and spewed large amounts of radioactive material into the environment. The accident occurred during a test in which operators had turned off the plant's safety systems and then lost control of the reactivity in the reactor. The subsequent reactivity excursion led to a massive vapor explosion, followed by hydrogen combustion and a graphite fire. The areas around the plant became seriously contaminated and a radioactive plume spread far into other parts of the Soviet Union and Europe. Although the plume did not pose a threat to the United States, one measure of its intensity was that levels of iodine-131 around Three Mile Island were three times higher after Chernobyl than they were after the TMI-2 accident.[19]

The design of Chernobyl is entirely different from that of U. S. plants. For example, the Chernobyl design has a positive void coefficient of reactivity and is not inherently stable. It also lacks a high-strength containment building (although it would take an exceptional containment to withstand this particular accident). Exacerbating the design deficiencies was a series of operator blunders leading to the accident that defied belief. Supporters of nuclear power emphasized that a Chernobyl-type accident could not occur in commercial U.S. plants (or other nations), which featured safety systems and containments to prevent the release of radionuclides. But nuclear critics pointed to Chernobyl as the prime example of the hazards of nuclear power. The Chernobyl tragedy was a major setback to the hopes of nuclear proponents to win public support for the technology and to spur orders for new reactors. U. S. utilities had not ordered any new plants since 1978 and the number of cancellations of planned units was growing. The Chernobyl accident added a new source of concern to long-standing controversies over the licensing of U.S. plants.

1.4.13 Safety Goal Policy

Several TMI-2 investigators recommended that the NRC explicitly identify a safety goal -- a level of risk at which reactors would be safe enough. Establishing such a goal, advocates believed, would end the interminable question: When is a nuclear power plant safe enough? The NRC established both qualitative and quantitative safety goals in August 1986, after several years of deliberations.[20]

The qualitative safety goals are as follows:

1. *Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.*

2. *Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.*

The corresponding quantitative safety goals are:

1. *The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.*

2. *The risk to the population near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one tenth of one percent of the sum of cancer fatality risks resulting from all other causes.*

The average accident fatality rate in the U.S. is approximately 5×10^{-4} per individual per year, so the quantitative value for the first goal is 5×10^{-7} per individual per year. The *"vicinity of a nuclear power plant"* is defined to be the area within one mile (1.6 km) of the plant site boundary. The average U.S. cancer fatality rate is approximately 2×10^{-3} per year, so the quantitative value for the second goal is 2×10^{-6} per average individual per year. The population *"near a nuclear power plant"* is defined as the population within ten miles (16 km) of the plant site.

When first proposed in the early 1980s, the second of these quantitative goals set off a flurry of controversy. While a ten mile (16 km) radius around the plant site was selected for evaluation, the choice of a particular radius is arbitrary and somewhat controversial. When considering a 0.1 percent cancer rate within a fifty mile (80 km) radius, for example, this would amount to an average of three excess cancer fatalities per reactor per year (these would be excess over the expected 3000 cancer fatalities from normal causes). This would be a total of 13,500 excess deaths over the next thirty years in an industry comprised of 150 reactors -- a figure critics argued was too high. The NRC could have responded to this criticism by revising the second goal, perhaps by establishing a more stringent goal for risks to persons outside the ten mile (16 km) radius (not addressed in the original goal), but this would have triggered criticism from proponents of nuclear power, who would have argued that the goal was too strict compared with other risks that society accepts. Thus, both of the preceding quantitative safety goals remained as originally drafted.

Even when an acceptable safety goal can be agreed on, regulators still have to determine whether the goal actually has been met. The NRC recognized this, and announced that because of *"the sizable uncertainties ... and gaps in the data base,"* the quantitative safety goals would serve as *"aiming points or numerical benchmarks."* The NRC also indicated that the goals were intended to apply to the industry as a whole and not precisely to individual plants. The goals were not

> *in and of themselves meant to serve as a sole basis for licensing decisions. However, if pursuant to these guidelines, information is developed that is applicable to a specific licensing decision, it may be considered as one factor in the licensing decision.*

The safety goal policy makes it clear that the quantitative safety goals are not hard and fast requirements (such as a rule would be). This situation does not alleviate the fact that an actual implementation approach is not yet approved as of early 1993. Implementation is discussed more in Module 2.

The NRC has not yet attempted to apply the above safety goals to an actual plant design during a licensing process. Thus, all the safety goals and their objectives must be viewed as continuing to evolve. For example, the NRC staff has discussed setting the core damage objective for future reactor designs a factor of ten more restrictive than the once per 10,000 years proposed for currently operating reactors, although the NRC Commissioners voted in 1988 not to make this standard a formal policy goal. Rather, the NRC should encourage reactor designers to strive towards this improved core damage frequency.

1.4.14 Backfit Rule

Backfitting is defined in some detail in 10 CFR 50.109, but for purposes of discussion here it means measures which are directed by the Commission or by NRC staff in order to improve the safety of nuclear power reactors, and which reflect a change in a prior Commission or staff position on the safety matter in question.[21] The current Backfit Rule has evolved in three stages:

1. The 1970 Backfit Rule which allowed the NRC to take advantage of technological advances in safety,

2. The 1985 Final Backfit Rule which included cost impact in the consideration of backfits, and

3. The 1988 Amended Final Backfit Rule which dealt with legal problems associated with cost considerations.

The NRC promulgated its first rule concerning the "backfitting" or safety-enhancement of nuclear reactors in 1970. In explaining the need for such a rule, the NRC noted that

> *rapid changes in technology in the field of atomic energy result in the continual development of new or improved features designed to improve the safety of production and utilization facilities.*[22]

The rule addressed these technological changes by setting forth a standard governing when the NRC could require a plant previously licensed for construction or operation to incorporate a new safety feature. The rule stated that

> *the Commission may ... require the backfitting of a facility if it finds that such action will provide substantial, additional protection which is required for the public health and safety or the common defense and security.*[23]

The rule excepted from this standard any backfit that was necessary to bring a facility into compliance with its license or a Commission order, rule, or regulation. A backfit of this kind was apparently always required.

By the end of the 1970s, the backfit rule had become the target of widespread criticism. Some charged that the rule allowed the Commission to ignore the need for backfitting outmoded plants. For example, the President's Commission on the TMI-2 accident[24] stated that the rule had not forced the NRC to "*systematically consider*" the "*need for improvement of older plants.*" Others charged that the rule allowed the Commission to indiscriminately impose backfits without regard to their real necessity or cost. For example, NRC's Regulatory Reform Task Force claimed that

> *The staff's prior backfitting practices which have cost consumers billions of dollars have made nuclear plants more difficult to operate and maintain, have injected uncertainty and paralyzing delay into the administrative process and in some instances may have reduced rather than enhanced public health and safety.*[25]

All commentors appeared to agree that the rule had failed to systematize or rationalize the Commission's backfitting process.

In response to criticism of the 1970 rule, the NRC published an advance notice of proposed rule-making on September 28, 1983. The notice invited public comment on draft backfit rules proposed by the Commission's Regulatory Reform Task Force and the Atomic Industrial Forum, the trade association of the nuclear power industry. Fourteen months later, after having received and reviewed numerous comments the Commission published a proposed version of the final rule.[26] Parties commented on the rule, focusing especially on the authority of the Commission to consider economic costs when deciding whether to impose backfits.

On September 20, 1985, the Commission published its final rule, which became effective on October 21, 1985.[27] The heart of the final backfit rule is the standard governing the circumstances in which the Commission will order a backfit. The standard incorporated the 1970 rule's requirement that the backfit substantially increase protection to health and safety, but added an additional requirement that the benefits of the backfit justify its costs. Specifically, the rule provided:

> *The Commission shall require the backfitting of a facility only when it determines ... that there is a substantial increase in the overall protection of the public health and safety or the common defense and security to be derived from the backfit and that the direct and indirect costs of implementation for that facility are justified in view of this increased protection.*

The rule set forth in some detail the way in which the NRC would make the determination of whether a proposed backfit meets the governing standard. The rule requires that the NRC prepare a "*systematic and documented analysis*" of each proposed backfit, considering available information concerning nine factors:

1. the specific objectives of the proposed backfit;
2. the activity that would be required by the licensee to complete the backfit;
3. the potential change in risk to the public resulting from the backfit;
4. the potential impact of the backfit on the radiological exposure of the facility's employees;
5. the costs of installation and maintenance associated with the backfit, including the cost of facility downtime or construction delay;
6. the potential impact on safety of the changes in plant or operational complexity resulting from the backfit;
7. the estimated resource burden on the NRC associated with imposing the backfit;
8. whether the relevancy and practicality of the particular kind of backfit will vary from facility to facility; and
9. whether the backfit is an interim measure and, if so, the justification for imposing the backfit on an interim basis.

In addition to considering these nine factors, the rule required the NRC to take into account "*any other-information relevant and material to the proposed backfit*" in preparing the requisite analysis.

The rule also stated that "*backfit analysis is not required and the standard does not apply*" in three situations. The first exception, similar to the exception in the 1970 rule, is when a backfit is necessary to bring a facility into compliance with a license, the rules or orders of the Commission or written commitments of the licensee. The second exception is when

> *an immediately effective regulatory action is necessary to ensure that the facility poses no undue risk to the public health and safety.*

The rule provides that the imposition of a backfit falling within this exception

> *shall not relieve the Commission of performing an analysis after the fact to document the safety significance and appropriateness of the action taken.*

The third exception appears in a footnote appended to the subsection containing the second exception This footnote states:

For those modifications which are to ensure that the facility poses no undue risk to the public health and safety and which are not deemed to require immediately effective regulatory action, analyses, are required; these analyses, however, should not involve cost considerations except only insofar as cost contributes to selecting the solution among various acceptable alternatives to ensuring no undue risk to public health and safety.

The 1985 backfit rule and a related internal NRC Manual chapter which partially implemented it were challenged by the Union of Concerned Scientists. On August 4, 1987, the U.S. Court of Appeals for the DC Circuit rendered its decision vacating both the rule and the NRC Manual chapter which implemented the rule.[28] The Court concluded that the rule, when considered along with certain statements in the rule preamble published in the Federal Register, did not speak unambiguously in terms that constrained the NRC from considering economic costs in establishing standards to ensure adequate protection of the public health and safety as dictated by section 182 of the Atomic Energy Act. At the same time, the Court agreed with the Commission that once an adequate level of safety protection had been achieved under section 182, the Commission was fully authorized under section 161i of the Atomic Energy Act to consider and take economic costs into account in ordering further safety improvements. The Court therefore rejected the position of the Union of Concerned Scientists that economic costs may never be a factor in safety decisions under the Atomic Energy Act.

Because the Court's opinion regarding the circumstances in which costs may be considered in making safety decisions on nuclear power plants was completely in accord with the Commission's own policy views on this important subject, the Commission decided not to appeal the decision. Instead, the Commission decided to amend both the rule and the related NRC Manual chapter (Chapter 0574) so that they conform unambiguously to the Court's opinion.

The final amended backfit rule was published as 10 CFR 50.109 on June 6, 1988.[25] In the rulemaking the Commission has adhered to the following safety principle for all of its backfitting decisions.

The Atomic Energy Act commands the Commission to ensure that nuclear power plant operation provides adequate protection to the health and safety of the public. In defining, redefining or enforcing this statutory standard of adequate protection, the Commission will not consider economic costs. However, adequate protection is not absolute protection or zero risk. Hence safety improvements beyond the minimum needed for adequate protection are possible. The Commission is empowered under section 161 of the Act to impose additional safety requirements not needed for adequate protection and to consider economic costs in doing so.

The 1985 revision of the backfit rule, which was the subject of the Court's decision, required, with certain exceptions, that backfits be imposed only upon a finding that they provided a substantial increase in the overall protection of the public health and safety or the common defense and security and that the direct and indirect costs of implementation were justified in view of this increased protection. The final rule restates the exceptions to this requirement for a finding, so that the rule will clearly be in accord with the safety principle stated above. In response to the Court's decision, the rule now provides that if the contemplated backfit involves defining or redefining what level of protection to the public health and safety or common defense and security should be regarded as adequate, neither the rule's "substantial increase" standard nor its "costs justified" standard, see 50.109(a)(3), is to be applied (see 50.109(a)(4)(iii)). Also in response to the Court's decision, (see 824P.2d at 119) the rule now also explicitly says that the Commission shall always require the backfitting of a facility if it determines that such regulatory action is necessary to ensure the health and safety of the public and is in accord with the common defense and security. On instruction from the Commission, the NRC staff amended its Manual Chapter on plant-specific backfitting to ensure consistency with the Court's opinion.

Efforts are currently under way to more precisely define terms, such as "substantial additional protection," and to coordinate the Backfit Rule with the Safety Goal Policy. These issues are discussed in more detail in Module 2.

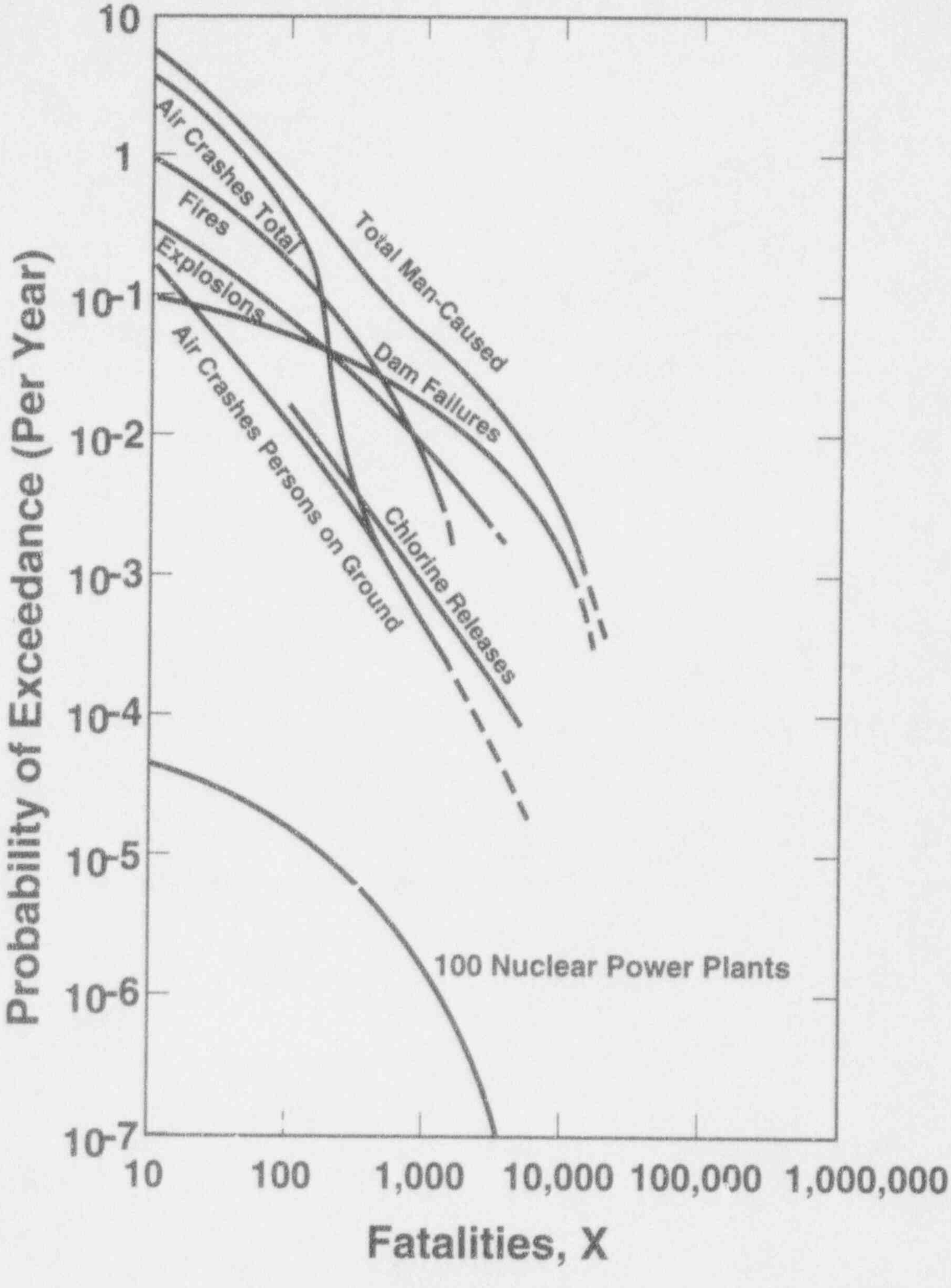


Figure 1.4-1 Frequency of man-caused events involving fatalities

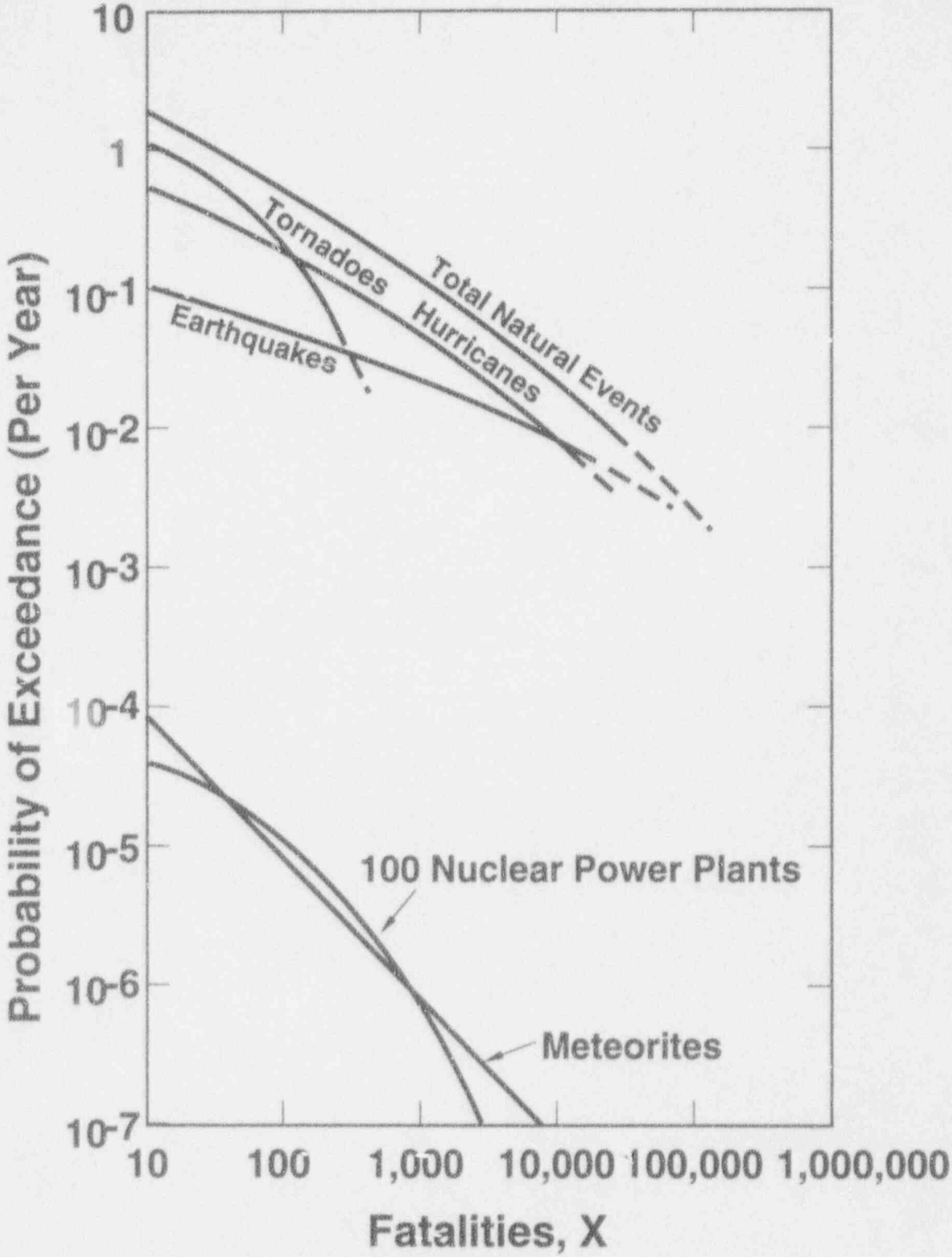


Figure 1.4-2 Frequency of natural events involving fatalities

References for Section 1.4

1. U.S. Nuclear Regulatory Commission, *The Safety of Nuclear Power Reactors (Light Water-Cooled) and related Facilities*, WASH-1250, July 1973.

2. Regulatory Staff to Commissioners, November 15, 1971 Policy Paper

3. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, October 1975.

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

5. J. Samuel Walker, *A Short History of Nuclear Regulation 1946-1990*, Historical Office, Office of the Secretary, Nuclear Regulatory Commission, June 1991, p38.

6. *NRC Action Plan Developed as a Result of the TMI-2 Accident*, NUREG-0660, May 1980.

7. John G. Kemeny, et al., *Report of the President's Commission on the Accident at Three Mile Island*, October 1979.

8. M. Rogovin, et al., *Three Mile Island, A Report to the Commissioners and to the Public*, NUREG/CR-1250, January 1980.

9. *TMI-2 Lessons Learned Task Force Final Report*, NUREG-0585, October 1979.

10. *Clarification of TMI Action Plan Requirements*, NUREG-0737, November 1980.

11. U.S. Nuclear Regulatory Commission, *Transient Response of Babcock & Wilcox-Designed Reactors*, NUREG-0667.

12. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.97, *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident*, Revision 2, December 1980.

13. *Clarification of TMI Action Plan Requirements*, NUREG-0737, U.S. Nuclear Regulatory Commission, November 1980, Supplement 1, January 1983.

14. 45 Federal Register 55,402, August 19, 1980.

15. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

16. 50 *Federal Register* 32138, August 8, 1985

17. U.S. Nuclear Regulatory Commission, Title 10 Code of Federal Regulations 50.54 (f) Generic Letter 88-20, *Individual Plant Examination for Severe Accident Vulnerabilities*, Nov 23, 1988.

18. *Individual Plant Examination: Submittal Guidance*, NUREG-1335, August 1989.

19. Knief, Ronal Allen, Nuclear Engineering, Theory and Technology of Commercial Nuclear Power, Second Edition, Hemisphere Publishing, 1992, p. 458.

20. Title 10, Code of Federal Regulations, *Safety Goals for the Operations of Nuclear Power Plants; Policy Statement, Federal Register*, August 4, 1988.

21. Title 10, Code of Federal Regulations, Part 50.109.

22. 35 *Federal Register* 5,317, March 31, 1970.

23. Title 10 Code of Federal Regulations, Part 50.109(a), 1971.

24. President's Commission on the Accident at Three Mile Island, Government Printing Office, Washington, DC, October 1979.

25. 53 *Federal Register* 20,603, June 6, 1988.

26. 49 *Federal Register* 47,034, November 30, 1984.

27. 50 *Federal Register* 38,097, September 20, 1985.

28. Union of Concerned Scientists versus U.S. Nuclear Regulatory Commission, 824 F.2d 103, August 24, 1987.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

Figure

2.0 ACCIDENT SEQUENCES

2.0.1 Introduction

This module discusses nuclear power plant accident sequences. The term accident sequence is used to denote the sequence of events that delineate an accident. These events include the accident initiator (the initiating event) and subsequent successes and failures of plant systems and/or operations.

Accident sequences are often grouped by their initiating events. The definition of an initiating event depends on whether the plant is producing power or not. For power operation, an *initiating event* is an event that requires a rapid shutdown or trip of the plant and challenges the safety systems to remove decay heat. For nonpower operation, an *initiating event* is an event that requires an automatic or manual response to prevent core damage. In either case, if an initiating event is not successfully responded to, core damage may result.

Initiating events are typically divided into two broad groups. *Internal events* include equipment failures and human errors occurring within the plant such as pipe breaks, stuck valves, damaged pumps, instrument failures, and operator errors. *External events* include natural and human-caused events outside the plant such as earthquakes, tornadoes and other severe weather, floods caused by heavy precipitation or dam failure, aircraft crashes, and volcanic activity. There are sometimes exceptions to the use of the plant boundary to distinguish internal from external events. For example, fires internal to the plant have traditionally been classified as external events (although many analysts now agree they should be classified as internal events).

The basic safety philosophy followed by both industry and the NRC in promoting the safety of nuclear power plants is defense in depth. As originally conceived (see Section 1.1.5) defense in depth referred primarily to design and siting considerations included to prevent accidents, contain radionuclides should an accident occur, and keep the public away from any radionuclides that might be released anyway. The philosophy was embodied in the form of a maximum credible accident, invariably a design-basis loss of coolant accident. After the TMI-2 accident, defense in depth expanded to include the consideration of accidents beyond the design basis. This module discusses both design-basis and beyond-design-basis accidents, as well as actual accident sequences, such as TMI-2.

Before proceeding, it is reasonable to ask "Why not design against all possible accidents?" In part, the answer to this question is the basis for defense in depth, namely, the recognition that human beings cannot think of everything. As indicated in the introduction to Chapter 1,

> "*one must continually question whether the safeguards already in place are sufficient to prevent major accidents.*"

Hence, the process of accident sequence delineation and analysis must and does continually change to reflect not only experience with operating plants, but also developments in a myriad of other government and industry activities that impact plant safety. In addition, however, there is usually a prohibitive cost associated with designing for the exceedingly unlikely (e.g., large meteor impact); and such expenditures may provide at best minimal improvements to plant safety or, in fact, make matters worse by grossly complicating existing designs. In fact, experience demonstrates that significant safety improvements can often be achieved with relatively simple, inexpensive changes to existing plants. Finally, advanced plants are being designed, utilizing the lessons learned from decades of reactor experience, both to prevent and to tolerate a wider spectrum of potential accidents than existing plants.

2.0.2 Learning Objectives for Module 2

At the end of this module, the student should be able to:

1. Describe three key conservatisms inherent in traditional design basis loss of coolant accident analysis with respect to long-term core coolability.

2. Define:
   a. Accident sequence
   b. Initiating event
   b. Severe accident
   c. Risk
   e. Source term

3. Explain with examples each of the following:
   a. Beyond design basis accident initiators
   b. Common cause failures

4. Describe three major differences between accidents initiated during full power and accidents initiated during low power or shutdown conditions.

5. Discuss the reasons why the Browns Ferry fire burned for so long.

6. List at least three important contributors to the accident at TMI-2.

7. Explain the use of event trees in delineating possible accident sequences.

8. Identify two features of U.S. plants not present at Chernobyl.

9. Discuss perspectives provided by NUREG-1150 in the following areas:
   a. PWR versus BWR core damage frequencies
   b. Magnitude of uncertainties in the core damage frequencies
   c. Relative importance of station blackout, ATWS, external events, and LOCAs at BWRs and PWRs
   d. Magnitude of risks compared to NRC safety goals and other risks.

10. Give three examples of risk based regulations and regulatory guidelines since TMI.

2.1 Design Basis Accidents

An applicant for a nuclear power plant construction permit or operating license must submit a Safety Analysis Report (SAR) to the NRC in accordance with regulations set forth in Section 50.34 of 10 CFR Part 50.[1] Additional guidance is provided in NRC Regulatory Guide 1.70 Rev. 3 entitled "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants."[2] Table 2.1-1, which is based on this Reg. Guide, indicates the major topics treated in the SAR. The NRC reviews the SAR to determine whether the plant can be built and operated without undue risk to the health and safety of the public. Guidelines for the NRC review are contained in NUREG-0800 entitled "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants."[3] The NRC findings are documented in a separate Safety Evaluation Report.

Chapter 2 of the SAR provides information on the geology, seismology, hydrology, and meteorology of the site and vicinity. It also provides information regarding nearby industry, transportation, and military facilities. Based on this information, design criteria are established for the magnitude of external phenomena such as floods, earthquakes, winds, tornadoes, and tsunami, which the plant must be capable of withstanding. Seismic design bases are discussed further in subsection 2.1.1.

Table 2.1-2 is a list of potential accident-initiating events (initiators), which applicants are specifically requested to address in SAR Chapter 15. Regulatory Guide 1.70 asks that the potential causes of each of these initiators be identified, and the estimated frequency of occurrence of each plausible initiator be assigned to one of the following categories:

a. Incidents of moderate frequency (expected to occur several times during the plant lifetime)

b. Infrequent events (may occur during the lifetime of the plant)

c. Limiting faults (not expected to occur but postulated because of the potential for the release of significant amounts of radioactive material).

For each of the eight initiator groups listed in Table 2.1-2, the potential exists for the release of radionuclides from successive barriers (fuel, cladding, the reactor coolant pressure boundary, and containment) to the environment. The plant must be designed to limit such releases such that offsite doses would not exceed the guidelines of 10 CFR Part 100 as a result of any accident in a set of design-basis accidents.[4]

A *design-basis accident (DBA)* is a postulated accident that a facility is designed and built to withstand without exceeding the offsite exposure guidelines of the NRC's siting regulation (10 CFR Part 100).

The assumptions used to delineate and analyze design-basis accidents are based on NRC regulations and guidelines that evolved as numerous applications for construction permits and operating licenses were reviewed. The subset of DBAs that are analyzed in detail in the SAR is selected in order to a) bound the offsite doses for DBAs in each of the eight initiation categories of Table 2.1-2, and b) to demonstrate the adequacy of key engineered safety features, in particular, the emergency core cooling systems and containment. Therefore, each of these analyzed DBAs invariably includes at least one significant failure of a component (or operator) to perform an intended safety function. Generally, equipment failures beyond those consistent with the single failure criterion of 10 CFR 50, Appendix A (see Section 1.3.4) are not postulated for DBAs. An exception arises when anticipated transients without scram (initiating event group 8 in Table 2.1-2) are treated as DBAs. Anticipated transients without scram are discussed separately in Section 2.7.1.

2.1.1 Design-Basis LOCAs

For many water cooled reactors, the DBA that results in the largest potential radiological consequences to the public begins with an instantaneous break in a large reactor coolant pipe. Such a break is postulated in spite of the extensive measures taken in the design, construction, testing and inspection, and operation and maintenance of the plant to assure that such breaks do not occur. In addition, a coincident loss of offsite power is postulated, and one of the emergency diesel generators is assumed to fail to start. This implies the loss of one of two or three AC powered trains in various safety systems.

Actually, a range of break sizes is considered, the largest being the hypothetical severance of the largest pipe in the system in such a way that reactor coolant would discharge unimpeded from both ends of the severed pipe. This type of break is referred to as a "double-ended guillotine break" and usually leads to the most severe calculated consequences. Because the reactor coolant system operates under high pressure, a reactor coolant pipe break would result in rapid expulsion of a large fraction of the reactor coolant into containment. In PWR containments, cold water sprays and/or ice racks are provided to condense the steam resulting from this expulsion while in BWRs, the steam would be condensed in the water-filled pressure-suppression pool. Condensing the steam limits containment pressure, which is the driving force for outward leakage. At the end of the blowdown (expulsion) period, the primary system would be filled mostly with saturated steam at the same pressure as that in the containment. In fact, a large-break LOCA or main steam line break usually establishes the peak internal pressure that the containment is designed to accommodate.)

In a large-break LOCA, the reactor would immediately go subcritical due to the loss of reactor coolant (neutron moderation). Successful actuation of the reactor protection system would keep the reactor subcritical when reflooded with emergency coolant. However, there would still be considerable thermal energy generated in the fuel from the decay of radioactive fission products. Immediately after shutdown, the generation rate of this "decay heat" is about 7% of the thermal power during operation. For example, a 1000 MWe nuclear plant generates about 3100 MWt during full power operation, but still generates about 225 MWt immediately after shutdown. The decay heat generation rate decreases fairly rapidly as indicated in Figure 2.1-1. However, if emergency cooling water were not supplied to remove heat from the core following the pipe break, core temperatures would increase to the point where energetic chemical reactions would occur between hot cladding and residual water-steam in the reactor pressure vessel. Given a prolonged failure to cool the core, large quantities of hydrogen could be generated, portions of the core would melt, and fission products would be released to containment and possibly to the environment. Such severe accident phenomena are discussed in more detail in subsequent modules.

In order to limit the consequences of a LOCA, each LWR is provided with an emergency core cooling system (ECCS). An automatic control system senses the occurrence of a LOCA and coordinates the operation of the different parts of the ECCS as they are needed. The function of the ECCS is to supply water to the core (via spray and/or flooding systems) to cool and limit the temperature increase of the cladding, thus preventing significant core damage and release of radionuclides from the fuel rods.

2.1.2 Design-Basis Analysis Conservatisms

In determining the acceptability of a proposed ECCS, the NRC reviews LOCA calculations performed by the applicant, and measures the results against five acceptance criteria specified in 10 CFR Part 50, Section 50.46 and Appendix K, which require that:[5]

- Peak cladding temperature cannot exceed 2200°F (1204°C),
- Oxidation cannot exceed 17% of cladding thickness,
- Hydrogen generation from hot cladding-steam interaction cannot exceed 1% of its potential,
- The core geometry must be retained in a coolable condition, and
- Long-term cooling must be provided.

These criteria do not represent threshold levels, which if exceeded will automatically result in a specific public safety problem. What they do represent is "a conservative statement of conditions which, if generally met, will provide a high degree of confidence that public safety is protected even if a highly unlikely loss of coolant accident occurs."[6]

In the traditional approach employed in the analysis and evaluation of the design-basis LOCA many pessimistic assumptions are invoked (per 10 CFR Part 50, Appendix K). This results in a calculated peak cladding temperature well above the value obtained using more realistic assumptions. In addition, the design of the ECCS must be shown to provide the required performance in spite of the loss of one train of AC power. Table 2.1-3 is a partial list of some of the conservative assumptions used in traditional design-basis LOCA calculations, illustrating the multiplicity of conservatisms. The table also contains a comparison with more realistic assumptions. A calculation of peak cladding temperature using the Appendix K conservatisms is provided in Figure 2.1-2. Removing some of the conservatisms can reduce the predicted peak clad temperature by as much as 700°F (390 K).[7]

Note that the decay heat generated in this time interval is significant, amounting to almost one third of the energy added to the containment atmosphere. As indicated in Table 2.1-3, decay heat is conservatively (usually 20%) above best estimate values in such design-basis LOCA calculations. Of course, this is also conservative with respect to the calculated peak clad temperature.

In September 1988, 10 CFR 50.46 and 10 CFR 50 Appendix K were modified to allow more realistic calculations to be used in estimating peak cladding temperatures. The new requirements, while less stringent, required that uncertainties in the calculations be considered and that the models provide:

> *"assurance of a high level of probability that the performance criteria of 50.46(b) would not be exceeded."*

Traditional offsite dose analyses for the design-basis LOCA postulate releases of radioactive fission products from the reactor fuel to the containment (and thus available for leakage to the environment) that are worse than actually expected from the design-basis LOCA. NRC Regulatory Guides 1.3 and 1.4 (for BWRs and PWRs respectively) recommend the assumption that 25% of the radioactive iodine inventory developed from full-power operation of the core be immediately available for leakage from containment.[8,9] A release to containment of this magnitude could only occur if the ECCS had minimal effectiveness, thereby permitting significant core melting.

One of the most significant barriers to the release of fission products to the environment from a postulated loss-of-coolant accident is the containment building. This structure is designed to have a very low leakage rate even given the peak internal pressure that would result from the design-basis LOCA. This peak pressure would rapidly decrease as heat was absorbed by the internal structures and lost by conduction to the outside air. In addition, spray systems in PWR containments would be automatically operated to condense the steam and reduce the building pressure, while in a BWR containment pressure would be reduced by steam condensation in the pressure suppression pool. For accident calculations, however, the containment is conservatively assumed to leak at a rate corresponding to the peak accident pressure for the first 24 hours and at 50% of that rate for the remaining duration of the accident.

The design-basis accident analyses take into account the reduction in the amount of radioactive material available for leakage to the environment by engineered safety features such as containment sprays and recirculating filtration systems. The amount of cleanup is evaluated for each system using conservative assumptions for parameters such as adsorption and filtration efficiencies.

The potential doses at the exclusion area boundary and the low population zone are calculated assuming that the accident occurs when the meteorological conditions are worse (from the standpoint of the calculated doses) than those that would be expected to prevail at the site approximately 95% of the time [Regulatory Guides 1.3 and 1.4]. Table 2.1-4 presents the results from typical calculations of potential offsite doses due to several kinds of design basis accidents. Even with the considerable number of pessimistic assumption employed, the calculated doses that a person out-of-doors in the vicinity of the plant might receive for the entire course of the accident are usually well below the 10 CFR Part 100 guidelines.

2.1.3 Comparison with Realistic Analyses

The conservative assumptions used for DBA analyses in safety analysis reports assure that the calculated consequences will exceed those that would be expected were the accident sequence to actually occur. For example, studies show fuel cladding temperatures in the range from 1200°F to 1600°F (650°C to 870° C) being predicted for more realistic calculations, as compared to 2100°F to 2200°F (1150°C to 1200°C) for conservative SAR calculations. Similarly, the radiological consequences that might realistically result from the unlikely event of a LOCA have been explored in connection with environmental evaluations. Table 2.1-5 presents some realistic dose estimates obtained for typical PWR events and accidents. Note that the realistic exclusion radius dose for a design-basis LOCA is over two orders of magnitude less than the corresponding conservatively calculated dose estimate in Table 2.1-4.[6] The most significant difference between the conservative and realistic dose calculations is in the release from fuel that is assumed. Realistically, ECCS would protect the core from melting, even given the postulated partial failure of AC power, and far less than 25% of the radioactive iodine inventory would escape from the fuel to the reactor containment.

In short, very conservative DBA analyses predict radiation doses to the public that are below 10 CFR Part 100 guidelines, and realistic DBA analyses predict much lower doses. This is not to say that accidents resulting in doses exceeding Part 100 guidelines are impossible; however, such accidents would realistically have to involve both:

a. More component failures than postulated for DBAs in order for ECCS to fail, core melting to occur, and significant quantities of radionuclides to be released from the fuel, and

b. Some significant breach or bypass of containment in order for significant quantities of radionuclides to be released to the environment. To assess the likelihood and consequences of such beyond-design basis accidents, both deterministic and probabilistic analyses are performed.

2.1.4 Seismic Design Basis

Design basis events are postulated in each safety analysis report for external events such as earthquakes, tornados, floods, accidents at nearby industrial facilities, etc. The approach to designing against many potential ex-plant (external) accident initiators can be illustrated by considering the seismic design basis.

Seismic safety considerations were largely overlooked for the first several power reactors, which were built east of the Rocky Mountains. Then, in the period 1963-1965, reactors were proposed for sites near Bodega Bay, San Onofre, and Malibu, California. During the AEC and ACRS review of these sites seismic concerns were raised.[10] The originally proposed requirements for seismic design were made two or three times more stringent. Even so, the Bodega Bay and Malibu sites were rejected due to seismic concerns.

In 1965, the AEC regulatory staff initiated work with its consultants to develop more specific seismic engineering criteria. In a May 1967, the AEC sent a draft document entitled "Seismic and Geologic Siting Criteria for Nuclear Power Plants," to the ACRS for review and comment.[10] Ultimately this draft evolved into Appendix A to 10 CFR Part 100.

The draft and subsequent revisions reflected the traditional philosophy that nuclear power plants should be designed against two levels of potential seismic events. Nuclear power plants are designed to continue to operate given earthquakes of moderate intensity and to safely withstand the effects of larger earthquakes. The operating basis earthquake (OBE) is the largest earthquake that

> *"could reasonably be expected to affect the plant site during the operating life of the plant"*[11]

and for which the plant is designed to continue operating without undue risk to the health and safety of the public. Nuclear power plants have instruments to warn of and measure earthquake motion. At the first indication of an earthquake, the operator is alerted. If the earthquake does not exceed the magnitude of the OBE, the plant can be kept on line to provide needed electrical power, and no inspection or evaluation of the plant would be required after the event. If the earthquake exceeds the magnitude of the OBE, the plant is shut down and could not be restarted until inspections and evaluations confirmed that it would be safe to do so.

The safe shutdown earthquake (SSE) is

> *"based upon an evaluation of the maximum earthquake potential considering the regional and local geology and seismology and specific characteristics of local subsurface material."*[12]

An earthquake of this magnitude may never have been experienced (and may never occur) at the site, but it determines the maximum vibratory ground motion for which plant safety features are designed to remain functional. At this level other plant features might be damaged, but the plant could be safely shut down.

Plant features (including foundations and supports) that are designed to remain functional given a SSE are designated Seismic Category I.[13] These include features that are "*necessary to assure:*

1. *The integrity of the RCS pressure boundary,*

2. *The capability to shut down the reactor and maintain it in a safe condition, or*

3. *The capability to prevent or mitigate the consequences of accidents that*

> *could result in potential offsite exposures comparable to the guideline exposures of 10 CFR Part 100."*[14]

By a combination of structural analysis and testing during plant design, plant structures and equipment important to safety are built to survive the SSE. Seismic analyses of structures, systems, and components are discussed in SAR sections 3.7 and 3.8, and guidance regarding such analyses is provided in the corresponding Standard Review Plan sections and references. In these seismic analyses conservative assumptions permit all vibratory parameters to be determined from the peak value of the horizontal ground acceleration caused by the earthquake such as 0.3 g (30% of the gravitational acceleration). Vibration tests are conducted to confirm key analyses. Such tests are often done on the first models of individual components including piping, fuel elements, pressure vessels, pumps, and valves and on full-scale reactor structures. Whole reactor buildings have been tested using mechanical shakers attached to the structure, and high explosives have been detonated nearby to simulate strong earthquakes.

Several items included in or omitted from the 1967 draft seismic criteria sparked considerable debate. One item, the proposed minimum design basis (or floor) of 0.1 g for the SSE, was particularly controversial. Not until November 1971, after many major re-drafts, did the AEC issue a Notice of Proposed Rule-Making to amend the 10 CFR Part 100, by adding Appendix A: "Seismic and Geologic Siting Criteria for Nuclear Power Plants."[10] The criteria were adopted in 1973 and reflected the practice which had been followed in actual construction permit reviews. Guidance was provided regarding the general extent of the geologic and seismic investigation required; however, no clear method was provided for selecting the SSE based on the results of such investigations.

The limited seismic audit performed on two reactors for the 1975 Reactor Safety Study identified several errors and deviances in seismic design. In 1977, the Nuclear Regulatory Commission initiated a major new research program in seismic safety including the application of probabilistic techniques (see subsection 2.2.2). In 1978 and 1979, based on new analyses of existing seismic data, the NRC required reevaluation of the seismic design bases for several reactors constructed by the Tennessee Valley Authority. In early 1979, five operating reactors were shut down for an extended period by the NRC in order to permit re-analysis and possible modifications because errors had been made in the seismic design of important piping systems. A large number of other reactors have since reported errors in their seismic design, and the adequacy of detailed seismic design has received considerable NRC attention.

Currently, 10 CFR 100 Appendix A requires that the maximum vibratory ground motion of the OBE be one-half that of the SSE.[15] It further requires a suitable dynamic analysis or qualification test to demonstrate that structures, systems, and components necessary for continued safe operation are capable of withstanding the effects of the OBE.[16] In some cases (e.g., piping) this has caused the OBE requirements to have more design significance than the SSE. The NRC has agreed that the OBE should not control the design of safety systems.* As a result, the regulation is being amended to permit future applicants for construction permits to set the maximum OBE vibratory ground motion based on one of two options:[20]

*SECY-90-16.

"(i) one-third or less of the SSE, where OBE requirements are satisfied without an explicit response or design analyses being performed, or

(ii) a value greater than one-third of the SSE, where analysis and design are required."

In either case, the plant must be shut down for inspection if the OBE is exceeded. In addition to changes in the selection of OBE's the NRC is proposing changes in the definition of SSEs for new plants.[21] The new approach adds probabilistic considerations to the previous methods and proposes that:

"the probability of exceeding the Safe Shutdown Earthquake Ground Motion at a site be lower than the median probability of exceedance computed for the current population of the operating plants."

The Changes proposed are intended to assure that future plants are as safe as current plants, while allowing for incorporation of recent findings from earthquake research activities.

TABLE 2.1-1

CHAPTER TITLES FROM REGULATORY GUIDE 1.70 REVISION 3
STANDARD FORMAT AND CONTENT OF
SAFETY ANALYSIS REPORTS FOR NUCLEAR POWER PLANTS

Chapter 1	Introduction and General Description of Plant
Chapter 2	Site Characteristics
Chapter 3	Design of Structures, Components, Equipment, and Systems
Chapter 4	Reactor
Chapter 5	Reactor Coolant System and Connected Systems
Chapter 6	Engineered Safety Features
Chapter 7	Instrumentation and Controls
Chapter 8	Electric Power
Chapter 9	Auxiliary Systems
Chapter 10	Steam and Power Conversion System
Chapter 11	Radioactive Waste Management
Chapter 12	Radiation Protection
Chapter 13	Conduct of Operations
Chapter 14	Initial Test Program
Chapter 15	Accident Analysis
Chapter 16	Technical Specifications
Chapter 17	Quality Assurance

TABLE 2.1-2

REPRESENTATIVE INITIATING EVENTS
TO BE ANALYZED IN SECTION 15.X.X OF THE SAR

1. **Increase in Heat Removal by the Secondary System**

   1.1 Feedwater system malfunctions that result in a decrease in feedwater temperature.

   1.2 Feedwater system malfunctions that result in an increase in feedwater flow.

   1.3 Steam pressure regulator malfunction or failure that results in increasing steam flow.

   1.4 Inadvertent opening of a steam generator relief or safety valve.

   1.5 Spectrum of steam system piping failures inside and outside of containment in a PWR.

2. **Decrease in Heat Removal by the Secondary System**

   2.1 Steam pressures regulator malfunction or failure that results in decreasing steam flow.

   2.2 Loss of external electric load.

   2.3 Turbine trip (stop valve closure).

   2.4 Inadvertent closure of main steam isolation valves.

   2.5 Loss of condenser vacuum.

   2.6 Coincident loss of onsite and external (offsite) a.c. power to the station.

   2.7 Loss of normal feedwater flow.

   2.8 Feedwater piping break.

3. **Decrease in Reactor Coolant System Flow Rate**

   3.1 Single and multiple reactor coolant pump trips.

   3.2 BWR recirculation loop controller malfunctions that result in decreasing flow rate.

   3.3 Reactor coolant pump shaft seizure.

   3.4 Reactor coolant pump shaft break.

TABLE 2.1-2 (cont.)

REPRESENTATIVE INITIATING EVENTS
TO BE ANALYZED IN SECTION 15.X.X OF THE SAR

4. Reactivity and Power Distribution Anomalies

4.1 Uncontrolled control rod assembly withdraws from a subcritical or low power startup condition (assuming the most unfavorable reactivity conditions of the core and reactor coolant system), including control rod or temporary control device removal error during refueling.

4.2 Uncontrolled control rod assembly withdraws at the particular power level (assuming the most unfavorable reactivity conditions of the core and reactor coolant system) that yields the most severe results (low power to full power).

4.3 Control rod maloperation (system malfunction or operator error), including maloperation of part length control rods.

4.4 Startup of an inactive reactor coolant loop or recirculating loop at an incorrect temperature.

4.5 A malfunction or failure of the flow controller in BWR loop that results in an increased reactor coolant flow rate.

4.6 Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant of a PWR.

4.7 Inadvertent loading and operation of a fuel assembly in an improper position.

4.8 Spectrum of rod ejection accidents in a PWR.

4.9 Spectrum of rod drop accidents in a BWR.

5. Increase in Reactor Coolant Inventory

5.1 Inadvertent operation of ECCS during power operation.

5.2 Chemical and volume control system malfunction (or operator error) that increases reactor coolant inventory.

5.3. A number of BWR transients, including items 2.1 through 2.6 and item 1.2.

TABLE 2.1-2 (cont.)

REPRESENTATIVE INITIATING EVENTS
TO BE ANALYZED IN SECTION 15.X.X OF THE SAR

6. **Decrease in Reactor Coolant Inventory**

6.1 Inadvertent opening of a pressurizer safety or relief valve in a PWR or a safety or relief valve in a BWR.

6.2 Break in instrument line or other lines from reactor coolant pressure boundary that penetrate containment.

6.3 Steam generator tube failure.

6.4 Spectrum of BWR steam system piping failures outside of containment.

6.5 Loss-of-coolant accidents resulting from the spectrum of postulated piping breaks within the reactor coolant pressure boundary, including steam line breaks inside of containment in a BWR.

6.6 A number of BWR transients, including items 2.7, 2.8, and 1.3.

7. **Radioactive Release from a Subsystem or Component**

7.1 Radioactive gas waste system leak or failure.

7.2 Radioactive liquid waste system leak or failure.

7.3 Postulated radioactive releases due to liquid tank failures.

7.4 Design basis fuel handling accidents in the containment and spent fuel storage buildings.

7.5 Spent fuel cask drop accidents.

TABLE 2.1-2 (cont.)

REPRESENTATIVE INITIATING EVENTS
TO BE ANALYZED IN SECTION 15.X.X OF THE SAR

8. Anticipated Transients Without SCRAM

8.1 Inadvertent control rod withdrawal.

8.2 Loss of feedwater.

8.3 Loss of a.c. power.

8.4 Loss of electrical load.

8.5 Loss of condenser vacuum.

8.6 Turbine trip.

8.7 Closure of main steam line isolation valves.

TABLE 2.1-3
PARTIAL COMPARISON OF REALISTIC ASSUMPTIONS WITH CONSERVATIVE ASSUMPTIONS OF LOCA CALCULATIONS

Realistic Assumptions	Conservative Assumptions
<u>Accident Initiation</u>	
1. Crack in large pipe, rupture of smaller pipe, or limited break in large pipe resulting in shutdown and repair.	1. A spectrum of pipe breaks is analyzed including instantaneous double-ended breaks of any reactor coolant, feedwater, or main steam line. See Figure 4.1-10.
<u>System/Component Reliability</u>	
1. Off site power is available.	1. Off-site power is lost concurrent with initiating event.
2. All components of emergency AC, ECCS, and containment ESFs function properly.	2. The worst single active failure is postulated for each accident analyzed.
<u>Reactor Power</u>	
1. The plant is operated at 100% power or less.	1. The plant is operated at 102% power continuously.
2. Hottest region of core has expected peaking factor.	2. Hottest region of core assumed to be at the maximum allowable peaking factor due to abnormal condition.
3. Decay heat follows best estimate prediction.	3. Decay heat is conservatively above best estimate to account for uncertainties in prediction.
<u>ECCS and Containment ESFs</u>	
1. Break occurs in system such that some of water from ECCS reaching broken loop is effective.	1. For postulated PWR cold leg breaks all ECC water directed to the broken loop is diverted to containment until the end of blowdown.
2. ECCS pumps deliver at higher than design flow rate.	2. ECCS pumps deliver at design flow rate or less.

TABLE 2.1-3 (Continued)
PARTIAL COMPARISON OF REALISTIC ASSUMPTIONS WITH CONSERVATIVE ASSUMPTIONS OF LOCA CALCULATIONS

Realistic Assumptions	Conservative Assumptions
ECCS and Containment ESFs (Continued)	
3. Reactor coolant pumps continue to run.	3. Reactor coolant pumps are tripped and coasting down or assumed to have a locked impeller.
4. Best estimate fluid discharge and heat transfer correlations apply.	4. Conservative fluid discharge and heat transfer correlations are used.
5. Fuel rods would have a distribution of temperature.	5. ECCS acceptance criteria apply to the hottest single fuel rod.
6. Initial containment temperature and ultimate heat sink temperature would be nominal.	6. Initial containment temperature and ultimate heat sink temperature would be at upper limits.
Consequence Calculations	
1. At most radionuclides in reactor coolant and gap activities in a few fuel rods would be released to the containment.	1. 100% of the noble gasses and 25% of the core iodine inventory is immediately released to containment. [Reg.Guides 1.3 and 1.4]
2. Containment leakage would be some nominal fraction of the design leak rate even when the containment was at its peak pressure.	2. Containment leaks at the rate incorporated as a technical specification requirement for the first 24 hours and at half this rate for the remaining duration of the accident. [Reg. Guides 1.3 and 1.4]
3. Best-estimate atmospheric dispersion and transport models apply.	3. Conservative atmospheric dispersion and transport models are used. [Reg.Guides 1.3 and 1.4]
4. Emergency planning would be implemented to protect the surrounding population from any radionuclides that might be released to the environment.	4. Doses are calculated for a hypothetical person standing outside in the radioactive plume, for 2 hours at the exclusion area boundary and during the entire period of plume passage at the low population zone outer boundary. [10 CFR 100 (d)]

TABLE 2.1-4

POTENTIAL OFFSITE DOSES DUE TO DESIGN-BASIS ACCIDENTS
(CONSERVATIVE CASE)

Accident	Two Hour Exclusion Boundary (3200 feet or 975 meters)		Duration of Accident Low Population Zone (4 miles or 6.4 km)	
	Thyroid (Rem)	Whole Body (Rem)	Thyroid (Rem)	Whole Body (Rem)
Loss of Coolant	155	3	81	3
Control Rod Ejection	<1	<1	<1	<1
Fuel Handling	2	2	<1	<1
Steam Line Break	16	1	3	1
10 CFR 100 Dose Guideline	300	25	300	25

TABLE 2.1-5
POTENTIAL OFFSITE DOSES DUE TO RELEASES AT A TYPICAL PWR*
(REALISTIC CASE)

Event/Accident	Individual Dose at Exclusion Radius (rem/event)	Individual Dose at 25 miles or 40 km (rem/event)	Dose to Population Within 50 miles or 80 km (rem/event)
10 gallons per day continuous leak rate from sources outside containment	5×10^{-6}	1×10^{-8}	2×10^{-2}
Gases from inadvertent discharge of part of boric acid condensate tank	5×10^{-9}	1×10^{-11}	2×10^{-5}
Loss of load	2×10^{-8}	4×10^{-11}	8×10^{-5}
Fuel handling accident inside containment (3 days after shutdown)	6×10^{-6}	1×10^{-8}	2×10^{-2}
Fuel handling accident outside containment	3×10^{-4}	6×10^{-7}	1×10^{0}
Large-break LOCA	8×10^{-3}	2×10^{-5}	3×10^{1}

* From WASH-1250. Doses are whole body doses. Natural background dose is approximately 10^5 man-rem/yr for the assumed population within the 50 mile or 80 km radius of the nuclear plant (i.e., 750,000 to 1,000,000 people).

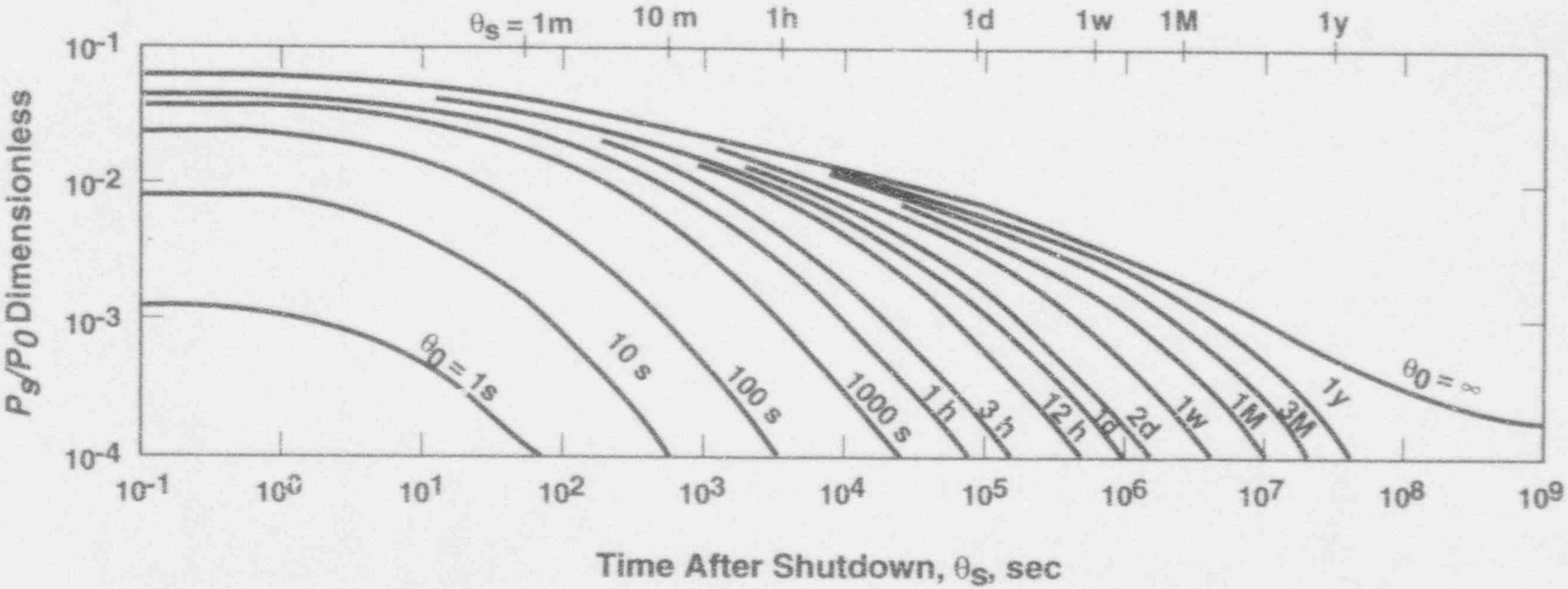


Figure 2.1-1 Ratio of power after, to power before shutdown for various operation times before shutdown: s, sec; m, min; d, day; w, week; M, month; y, year

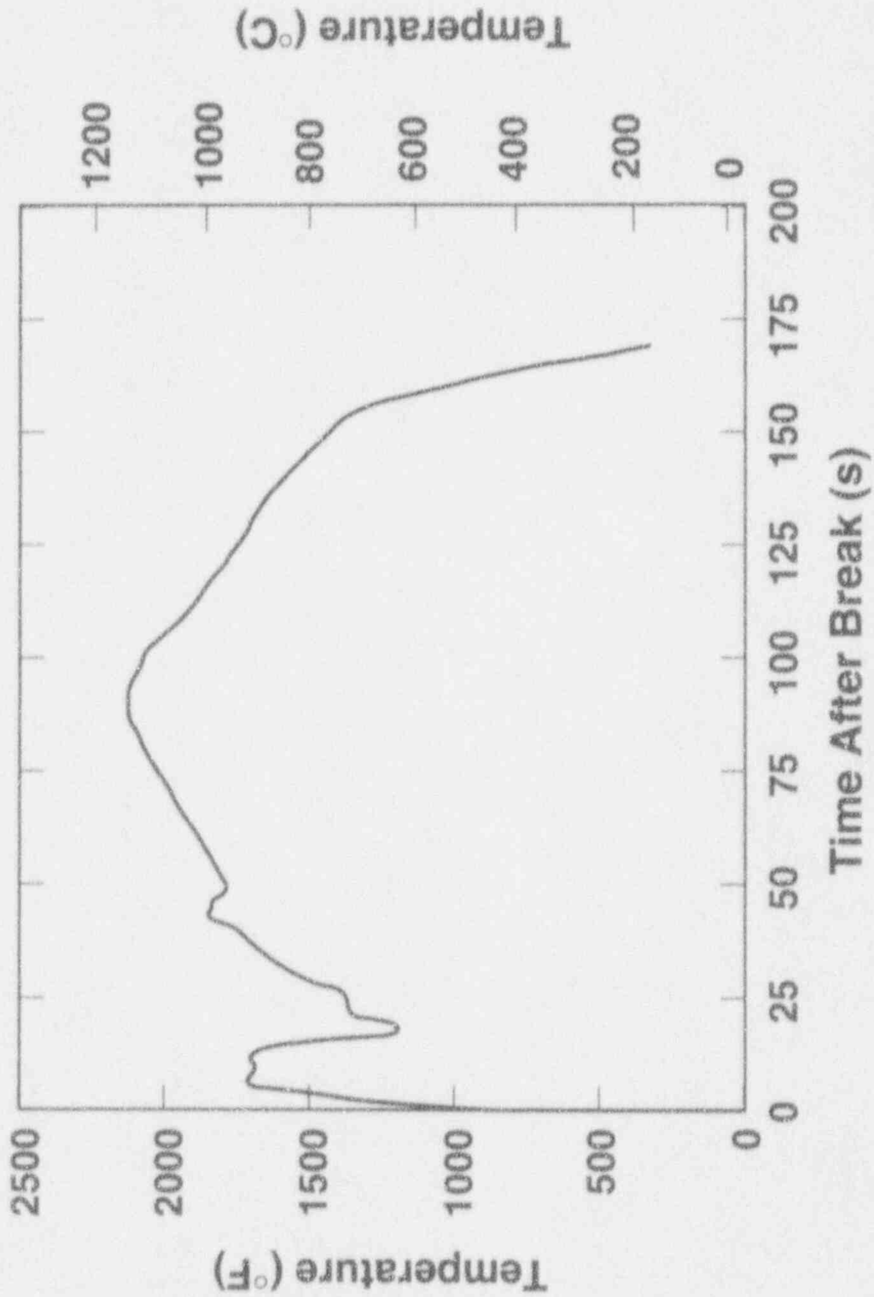


Figure 2.1-2 Conservative estimate of peak clad temperature

References for Section 2.1

1. Title 10, Code of Federal Regulations, Part 50.34, Jan 1, 1991

2. U.S. Nuclear Regulatory Commission Regulatory Guide 1.70, Rev. 3, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants ( ).

3. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, NUREG-0800, Nuclear Regulatory Commission.

4. Title 10, Code of Federal Regulations, Part 100.11(a), footnote 1, see Module 1, page 1.2-6.

5. Title 10, Code of Federal Regulations, Part 50.46 (b), Jan 1, 1991.

6. U.S. Nuclear Regulatory Commission, *The Safety of Nuclear Power Reactors (Light Water-Cooled) and Related Facilities*, WASH-1250 (1973), p.5-8.

7. R. Steiger, Extended BE/EM Study, Idaho National Engineering Laboratory letter STIG-177-77 (1977), cited in B. E. Boyack, et. al., *Quantifying Reactor Safety Margins*, Nuclear Engineering and Design, (1991).

8. U.S. Atomic Energy Commission Regulatory Guide 1.3, *Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Boiling Water Reactors, Revision 2*, (June 1974).

9. U.S. Atomic Energy Commission Regulatory Guide 1.4, *Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Pressurized Water Reactors, Revision 2*, June 1974.

10. David Okrent, *Nuclear Reactor Safety: On the History of the Regulatory Process*, The University of Wisconsin Press, Madison, Wisconsin, 1981, Chapter 17.

11. Title 10, Code of Federal Regulations, Part 100, Appendix A, III(d), Jan 1,1990.

12. Title 10, Code of Federal Regulations, Part 100, Appendix A (III)(c), Jan. 1, 1990.

13. Guidance for the seismic classification of structures, systems, and components is provided in Regulatory Guide 1.29, *Seismic Design Classification*

14. Title 10, Code of Federal Regulations, Part 100, Appendix A, III.(c). January 1, 1991.

15. Title 10, Code of Federal Regulations, Part 100, Appendix A, V(a)(2). January 1, 1991.

16. Title 10, Code of Federal Regulations, Part 100, Appendix A, VI(a)(2). January 1, 1991.

17. Draft Title 10, Code of Federal Regulations, Part 50, Appendix S, Earthquake Engineering Criteria for Nuclear Power Plants, 1992.

18. Draft Revision to Title 10, Code of Federal Regulations, Part 100, Appendix A, 1992.

2.2 Beyond-Design-Basis Accidents

2.2.1 Introduction to Severe Accidents

Given the conservatism inherent in the design-basis Loss of Coolant Accident (LOCA) analysis, industry proponents argued for years (until the TMI-2 accident) that more severe accidents, although theoretically possible, were too incredible to warrant significant study. Yet, with the China Syndrome, the concept of containment as a bulwark came into question, and with WASH-1400, the AEC/NRC began to examine the likelihood and potential consequences of accidents beyond the design basis.[1,2] Such accidents include those initiated by events, such as reactor pressure vessel rupture or a seismic event more severe than the safe shutdown earthquake, that are not analyzed in the Safety Analysis Report (SAR). Other accidents beyond the design basis include accidents involving multiple component failures or operator errors, that is, failures beyond those postulated under the single failure criteria. In general, a *beyond-design-basis accident* is an accident more severe than those analyzed in the Safety Analysis Report.

Figure 2.2-1 illustrates a breakdown of nuclear power plant accidents according to their severity. Not all accidents that exceed the plant design basis would result in damage to the reactor core. Even though they were not specifically designed to do so, given appropriate operator responses, plant systems (including non-safety-grade systems) are capable of handling many beyond-design-basis accidents. However, there are beyond-design-basis accidents, such as LOCAs in which emergency core cooling systems fail to provide adequate flow, that would lead to core damage. For some core damage accidents, the extent of damage would be minor (e.g., 10 CFR 50 Appendix K cladding temperature limit exceeded for a brief time period).[3] However, a subset of core damage accidents (e.g. accidents involving a prolonged failure of core cooling systems) would result in substantial core damage. Such accidents are called severe accidents (or Class 9 accidents).[4]

A *severe accident* is a reactor accident more severe than design-basis accidents in which, as a minimum, substantial damage is done to the reactor core.

As indicated in the preceding section, the radionuclide releases from fuel assumed in conservative design-basis LOCA analyses could only be realized if significant core melting occurred. Consequently, for a severe accident in which containment remained functional, the resulting offsite doses would be comparable to those conservatively calculated in the SAR for the design-basis LOCA. Yet, the possibility remains of severe accidents in which containment is either bypassed or breached as a result of severe accident phenomena. Depending on the mechanism, location, and timing of containment failure, and the meteorological conditions, offsite doses could be substantially (100 times) worse than conservatively calculated for the design-basis LOCA.

In this light, several questions arise. What types of accidents could result in significant core damage? How likely are they? What would be the consequences of such severe accidents? The remainder of Section 2.2 discusses the types of accidents that could result in core damage. Section 2.6 addresses the frequency of severe accidents, and Module 5 address the consequences of severe accidents.

2.2.2 Beyond-Design-Basis Initiating Events

Severe accidents are often classified by their initiators. There is considerable variability from plant to plant; however, important accidents often fall into one of the following categories:

1. Station Blackout (loss of offsite and onsite ac power),
2. Loss of Coolant Accidents (LOCAs),

3. Anticipated Transients Without Scram (ATWS),
4. Transients (other than ATWS).
5. Special initiators

LOCAs may be further subdivided into large, intermediate, small, and very small depending on the injection systems required to successfully respond to the LOCA. Transients initiators are usually events related to the balance of plant (BOP). Some typical transient initiators are listed for BWRs and PWRs in Tables 2.2-1 and 2.2-2.[5] These transients are explicitly considered in probabilistic risk assessments, as discussed in Section 2.6. Note that these initiators are somewhat more specific than the design-basis initiators presented in Table 2.1-2 and include more events, although there is some overlap in the respective lists.

Design-basis initiators can lead to core damage if additional failures occur (a design-basis initiator can lead to a beyond-design-basis accident). Special initiators include failures in plant support systems (AC or DC busses, cooling water, service water, instrument air, HVAC, etc.) Special initiators also include failures of components that separate the high pressure reactor coolant from lower pressure regions, for example steam generator tube ruptures or failure of the valves isolating the reactor coolant system from the decay heat removal system. Accidents resulting from the latter initiators are called interfacing systems LOCAs.

In addition to the in-plant (internal) initiators discussed above, there are external initiators that can occur with variable magnitudes. These include:

1. Aircraft impacts
2. External and internal flooding
3. Extreme winds and tornadoes (and associated missiles),
4. External and internal fires,
5. Accidents in nearby industrial or military facilities,
6. Pipeline accidents (gas, etc.),
7. Release of chemicals stored at the site,
8. Seismic events,
9. Transportation accidents,
10. Turbine-generated missiles.

An external initiating event of sufficient magnitude may have the potential to cause multiple failures and lead to core damage with few, if any, additional failures. For example, the Browns Ferry fire, which is discussed in Section 2.3, damaged numerous electrical cables and components, thus disabling multiple cooling systems. As discussed in Section 2.6, fires and seismic events are the two most important external events for most plants.

The significance of a seismic event is proportional to the magnitude of the earthquake, in terms of the ground acceleration felt by the plant. If a seismic event results in a ground acceleration slightly above the level allowed for continuous operation (the Operating Basis Earthquake level, see Section 2.1.2), the plant would be shut down for post-earthquake examination. Such a shutdown constitutes a transient that could challenge safety related systems only if compounded by random equipment failures or operator errors. At somewhat higher ground acceleration levels, offsite power may be lost due to failure of the ceramic insulators on high tension electrical transmission lines. Plant equipment that is not Seismic Category I may also fail during such events, since it is not typically designed to withstand the seismic loadings. Finally, for ground acceleration levels above the Safe Shutdown Earthquake, safety related equipment can fail as a direct result of the seismic event.

External events include not only naturally-occurring phenomena, but also unintentional human-caused events. Human-caused external events that could conceivably damage a nuclear reactor facility and initiate core damage include aircraft impact, dam failure, accidents at nearby military or industrial facilities, and pipeline and transportation accidents. Also, failures within the reactor site, not directly related to reactor operations could possibly initiate core damage. Examples of such events include spillage of hazardous, toxic, flammable or radioactive materials.

Traditionally, accidents initiated at low power and shutdown have not been considered to be particularly important. However, efforts initiated in France and now underway in the U.S. indicate that accidents initiated at low power and shutdown may be more significant than previously thought.[6,7] There are several reasons for this. During low power and shutdown, there are fewer technical specification requirements. Particularly during shutdown, many systems are inoperable because components are out for maintenance. The operators often have a poor concept of the status of plant systems during shutdown because components are being taken in and out of service frequently and not all instrumentation is available. Furthermore, there are more people in the control room and many control room indicator lights are on because so much equipment is out of service. There is complacency, a common perception that the plant is in a safe condition when it is shutdown. However, while it is true that the decay heat generation rate decreases to about 1 percent after 1 day, it declines very slowly thereafter. One percent of full power production is sufficient to cause fairly rapid heatup of an uncooled core, given loss of residual heat removal as an initiating event. Further, during shutdown the reactor coolant level is lowered close to the top of the active fuel to permit the reactor head to be removed for refueling. LOCAs could be initiated by inadvertent opening of drain lines and the core could be uncovered rapidly. There are seldom any written procedures for dealing with accidents at shutdown. Finally, accidents at shutdown can occur while the containment is open and occupied, thereby increasing the potential for radiological health effects.

Up to this point we have discussed the possibility of severe accidents that result from accidental initiating events. An additional possibility is that someone could intentionally commit acts intended to lead to a severe accident, i.e., commit an act of sabotage. Sabotage is the commission of acts intended to cause harm or damage. For nuclear facilities, acts of sabotage could come from outside of the plant (e.g., an attack on the facility), from within the plant, or both. They could be perpetrated by an outside individual or organization, or by one or more persons who are permitted access to the plant either as workers or as visitors. An act of sabotage could be committed by individuals or groups having diverse motives, such as terrorists intending to cause a large release of radioactive material or a disgruntled worker intending to seek revenge on a single individual. Requirements for physical protection of plants and materials are described in 10 CFR Part 73.[8]

2.2.3 Multiple Failures Leading to Severe Accidents

Given an initiating event, core damage can result only if one or more of the following key functions are lost:

1. Reactivity control
2. Coolant inventory control
3. Core heat removal

All reactors have redundant means of performing these functions. Table 2.2.3 presents examples of the systems that would perform these functions for a typical BWR and a typical PWR. In many cases, there is redundancy within individual systems. Often, in BWRs, a single coolant injection system, in combination with appropriate support systems, can perform both the coolant inventory control and core heat removal function. Pump suction alignments determine whether coolant is added to the system from a storage tank or recirculated from the suppression pool. Core heat removal depends upon support system alignments that eventually transfer heat to an ultimate heat sink.

Except for a few unusual initiators, such as pressure vessel rupture or an extremely large earthquake, an initiating event must be followed by multiple, additional failures in order for core damage to occur. An important part of current design requirements for U.S. nuclear power plants is the single failure criterion:[9]

10 CFR 50, APPENDIX A

SINGLE FAILURE: A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electrical systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly) results in a loss of the capability of the system to perform its safety function.[*]

---

[*] *Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development.*

For example, consider a plant that must provide a minimum coolant flow rate of say 1000 gpm (.063 m^3/s) in order to prevent core damage following certain accident initiators. The plant systems will be successful if they provide 1000 gpm (.063 m^3/s) on demand. This is the injection *success criteria* for such accidents. The plant systems will withstand single failures if 1000 gpm (.063 m^3/s) can be provided in spite of the failure of any single component to perform its intended function. This can be achieved through the use of two systems (or one system with two trains) containing similar components, provided that each system (or train) alone is capable of delivering 1000 gpm (.063 m^3/s) on demand. The two systems (or trains) are said to be redundant if they contain essentially identical components, for example, each train might contain a motor driven pump and several motor operated valves. The trains would be diverse, or partially diverse, if they rely on different energy sources, for example, one train might contain a steam driven pump rather than a motor driven pump.

Assuming that a plant can withstand single failures, any accident that leads to core damage must involve multiple failures. For example, in a two train injection system, one of the two pumps might fail to start, and an isolation valve on the other system (or train) might fail to open. Components and systems can fail in various ways, including:

- Failure on Demand
- Failure to Run
- Unavailable due to Maintenance or Testing
- Explicitly Dependent Failures (see Section 2.2.3.2)
- Human Errors of Omission (Failures to Follow Procedures)
- Human Errors of Commission (See Section 2.2.3.5)
- Common Cause Failures (see Section 2.2.3.3)
- Subtle Failures (see Section 2.2.3.4)

2.2.3.1 Independent Versus Dependent Failures

Multiple failures may be either independent or dependent. Two events are said to be independent if the occurrence of one does not effect the likelihood of the other, otherwise the events are said to be dependent. Most important severe accidents are expected to include events that are at least partially dependent, due to common underlying causes of failure or interactions among systems. Dependent failures defeat the redundancy or diversity of plant systems that provide key functions such as coolant injection. The term *system interaction* is used to describe dependent failures that involve or affect more than one plant system. Examples of actual accidents that illustrate various types and modes of failure are presented in Section 2.3 and Appendices 2A and 2B. Dependent failures can be divided into three categories: explicitly dependent events, common cause failures, and subtle failures. The distinctions between these categories are based on the manner in which the impact of the dependent events are (or are not) treated in risk assessments (Section 2.6). The following subsections describe these three categories of dependent failures in more detail.

2.2.3.2 Explicitly Dependent Events

Many interactions and dependencies involve the explicit dependence of one system upon another. For example, many emergency core cooling systems are explicitly dependent upon support systems providing electrical power, instrument air, cooling water, *etc.* Cascading or propagating failures are also important. For example, a pump may fail to start due to the malfunction of a circuit breaker in the pump control circuit. Categories of explicit dependencies include:

Initiating event dependencies - Accident initiators can cause the unavailability of more than one system

Support system dependencies - Operation of front-line reactor core and containment safety systems can be directly or indirectly dependent on certain support systems (i.e., electrical power, heating, ventilation, cooling, actuation, and isolation).

Shared equipment dependencies - Individual components which are shared by more than one system (*e.g.*, the BWR suppression pool, and other components used in various modes of Residual Heat Removal).

Human errors - Operator failure to respond according to procedures can result in the failure or unavailability of more than one component or system.

Propagating failures - Failure of one component due to the failure of another component to which it is directly linked (*e.g.*, failure of a thermostat leads to room overheating and failures of components in the room).

2.2.3.3 Common Cause Failures

In addition to the explicit dependencies noted above, other dependencies are included by accounting for *common cause events*.

A *common cause failure* is the simultaneous failure or unavailability of more than one component due to some underlying common cause.

As indicated in Figure 2.2-2, potential underlying common causes can be grouped under engineering and operations each with two subcategories: design and construction under engineering, procedural and environmental under operations.[10]

A functional design deficiency might result from an unrecognized deficiency in some component (e.g., a sensing instrument that does not provide the required sensitivity), unanticipated changes in plant operating conditions that leave the protection system inadequate for its purpose, or misunderstanding of the behavior of process variables in the design of the protection system. Realization faults include design errors and failures due to a common element unrecognized in the design. Grouped under construction are deficiencies due to improper manufacture, installation, and/or pre-operational testing of all components of a similar type.

Common causes arising in plant operations include procedural errors such as incorrect calibration of all of the components of a given type, inadequate testing, mistakes made in maintenance work that might apply to a series of similar components, incorrect or outdated operating or maintenance instructions, and operator errors. The environment to which plant components are subjected can also be a common cause of failures. This includes such things as high temperatures, moisture, vibration, wear, dirt, and various more severe environmental events such as storms, fires, floods, earthquakes and accident conditions that might act in more or less the same way upon similar components throughout the plant.

Examples of component groups that are susceptible to common cause failures include:

- Safety Relief Valves (SRVs)
- Motor Operated Valves (MOVs)
- Motor Driven Pumps (MDPs)
- Air Operated Valves (AOVs)
- Diesel Generators (DGs)
- Batteries
- Circuit breakers.

For example, BWRs can have sixteen or more SRVs, and it is possible that more than one of these valves could fail to reclose in an accident due to some common design, manufacturing, or maintenance error. (The data for multiple failures of Target Rock SRVs indicate two events in 300 reactor years in which two SRVs failed to reclose and no events where three or more SRVs failed to reclose.*)

2.2.3.4 Subtle Failures

Subtle failures are certain types of dependent failures that involve complex features that do not allow the failures to be easily categorized. These types of interactions are sometimes buried in the depths of the design and operation of the system and can be difficult to uncover. Subtle failures are best explained by example. Six examples follow.

2.2.3.4.1 Sneak Circuits Following Power Restoration

A potential problem in the Reactor Core Isolation Cooling (RCIC) system circuitry of a particular BWR was identified. Within this particular RCIC control system, because of the design of the RCIC steam leak detection circuit, it is possible for a sneak circuit to occur and cause an unintended, nonrecoverable isolation of the RCIC pump in conjunction with a station blackout. There are at least three subtle design aspects which lead to the occurrence of this failure mode: (1) the RCIC system contains an isolation circuit, (2) the isolation circuitry is deenergized given a loss of offsite power (i.e., the circuitry is not fed by a noninterruptible, battery-backed vital AC power supply), and (3) the isolation circuit contains a seal-in circuit.

---

*Target Rock Data

2.2.3.4.2 Pump Room Cooling

A particular plant design may be such that, given the loss of room cooling, the maximum room temperature remains below the temperature for which a pump and its control circuits are qualified. However, upon further investigation, it may be found that a room cooler isolation control circuit exists, and this circuit is set to trip the pump at 200°F (93°C). This temperature would be reached within twenty minutes following loss of room cooling; therefore, room cooling is actually required for the pump.

Room cooler test procedures have been found inadequate at some plants. At one plant, it was determined that cooling of the Engineered Safety Features switchgear room was required. The cooling system was safety-grade and was tested monthly. The cooling system was actuated by a wall-mounted thermostat. However, the monthly test required the cooler to be started via a switch which bypassed the thermostat portion of the actuation circuit. The plant has since changed the test procedure so that the availability of the thermostat is verified monthly. The plant now uses a hot air blower to actuate the thermostat.

2.2.3.4.3 Air Binding of Cooling Water Systems

There have been several incidents involving the failure or partial failure of the cooling water systems because of air binding caused by leaks in a load being cooled. The plant compressed air systems have both compressor cooling and aftercoolers that are supplied with some form of cooling water. If a leak develops in these coolers, the higher pressure air will enter the cooling system and could result in air binding. This is a problem, particularly with closed-cooling systems, but could also be a problem with open systems. Air binding can result in failure of multi-train systems. Depending on the other loads on the cooling system, this potential failure of the air system and the entire cooling system can be important as an initiating event, or as a compounding support system failure.

2.2.3.4.4 Passive Component Failures

At one PWR an important accident sequence involves failure of a manual butterfly valve in the discharge of the nuclear service water system. This valve is in a common line that nearly all of the service water loads discharge to before returning to the lake. Failure of this valve in a manner that blocks flow prevents cooling of most safety loads. This scenario is difficult to diagnose and even more difficult to recover from. Although passive failures (e.g., stem/disc separation) of valves are rare, these events need to be considered, particularly in common support systems. It is also interesting to note that the plant has experienced this failure mode in a service water valve of the same design and size as the common valve. The valve that did fail is further upstream and only blocked flow from one RHR heat exchanger.

2.2.3.4.5 Normal Operating Configuration

The normal operating configuration of systems cannot always be inferred from plant P&IDs. For example, the P&ID may show valves as normally closed when, in reality, the plant operates with these valves open. In another case, the P&ID indicated that a room containing three high-pressure injection pumps had two room coolers, each receiving power and cooling water from a different division. Discussions with the plant revealed that, during normal operation, only one of the two room coolers is normally operating. Further discussion also revealed that it is permitted to power the cooler fan from Division 1 and supply the cooling water to the cooler heat exchanger from Division 2. Because of the normal operating configuration of this system, several single failures of the three high-pressure injection pumps were identified.

2.2.3.4.6 Locked Door Dependencies

During a station blackout, the security system at some plants locks the powered security restrictive and key-locked doors, that is, they do not fail open, thereby, potentially restricting accident response actions. The plant configuration is not always obvious during special types of accidents such as a station blackout.

2.2.3.5 Human Factors, Heroic Acts, Errors of Commission

The previous subsection noted that operators may fail to follow written procedures in some instances, thus exacerbating the event. However, an additional problem is that they may "think for themselves" and or intentionally violate written procedures by undertaking actions that they believe will aid in achieving a desired plant condition. Such acts may indeed improve the situation (see discussion of Davis Besse loss of feedwater event in Appendix 2B) in which case they are defined as *heroic acts*. Frequently, however, such acts initiate or exacerbate accidents in which case they are called *errors of commission*. Both the Three Mile Island (Section 2.4) and Chernobyl (Section 2.5) nuclear accidents were exacerbated by such errors of commission. We would not expect that a licensed reactor operator would actually turn the emergency core cooling system off during a loss of coolant accident, yet that occurred at Three Mile Island. Similarly, operators' are not expected to disable large numbers of safety related systems in violation of technical specifications, yet this was done at Chernobyl.

2.2.4 Operating Plant Data and Severe Accident Precursors

Each year the NRC receives an extensive amount of information from licensees and other sources regarding nuclear power plant experience. Table 2.2-4 lists some of the sources of information and indicates those that are required by law. Prompt phone notifications and written Licensee Event Reports (required by 10 CFR 50.72 and 10 CFR 50.73) are the predominant sources of information having potential safety implications.[11,12] The NRC systematically reviews and analyzes the information it receives to identify instances where the margin of safety established through licensing has been degraded. In such cases, the NRC then identifies and implements corrective actions that will restore the originally intended margin of safety. Any proposed improvements in this margin of safety must be separately identified and justified as new licensing actions.

The feedback of operating data or experience is an inherent and important aspect of NRC activities and involves all NRC organizational elements at one time or another. The principal NRC organizations involved are the Office of Nuclear Reactor Regulation (NRR) and the Office for Analysis and Evaluation of Operational Data (AEOD). AEOD was established several months after the TMI-2 accident to identify and feedback significant safety lessons of operational experience to the NRC, its licensees, the nuclear industry as a whole, and the public. Table 2.2-5 lists some of the NRC-originated documents that are used to disseminate relevant nuclear power plant experience. Of particular interest to licensees are Bulletins, Information Notices, and NRR Generic Letters.

Information Notices provide information but do not require specific actions. They are rapid transmittals of information that may not yet have been completely analyzed by the NRC, but that licensees should be aware of. Licensees receiving an Information Notice are expected to review the information for applicability to their current and future licensed operations. If the information is applicable to their facility, licensees are expected to take action necessary to avoid repetition of the problem described in the Information Notice.

Bulletins provide information about one or more similar events and require that licensees take specific actions, usually to assure that the intent of an existing rule or requirement is being satisfied. Prompt response by licensees is required and failure to respond will normally result in NRC enforcement action. NRC Bulletins generally require one-time action and are not intended as substitutes for formally issued regulations or for imposed license amendments.

NRR Generic Letters can compel licensees to provide information concerning specific safety issues. The licensees may have to perform analyses of the significance of particular issues at their respective plants. The Generic Letter may indicate a resolution process for the issue that is acceptable to the NRC and ask the utilities to respond, either accepting the proposed resolution process or presenting an alternative approach for the NRC to consider.

Given the years of nuclear power plant experience accrued in the U.S., one would expect a large number of accident sequences that could potentially lead to core damage to have been revealed by incidents involving beyond-design-basis initiators and/or sequences of events. Such incidents are commonly referred to as precursors of severe accidents. Several studies of such precursors have been conducted.[13] Regulatory actions have been taken to reduce the threat from some of the accidents identified in precursor studies. For example, station blackout, loss of feedwater, and Anticipated Transients Without Scram (ATWS) are discussed in Section 2.7.

Table 2.2-1 Generic Transient Events for BWRs

1. Electric load rejection
2. Electric load rejection with turbine bypass valve failure
3. Turbine trip
4. Turbine trip with turbine bypass valve failure
5. Main Steam Isolation Valve (MSIV) closure
6. Inadvertent closure of one MSIV
7. Partial MSIV closure
8. Loss of condenser vacuum
9. Pressure regulator fails open
10. Pressure regulator closed
11. Inadvertent Open Relief Valve (IORV)
12. Turbine bypass fails open
13. Turbine bypass or control valves cause increased pressure (closed)
14. Recirculation control failure, increasing flow
15. Recirculation control failure, decreasing flow
16. One recirculation pump trip
17. Recirculation pump trip (all)
18. Abnormal startup of idle recirculation pump
19. Recirculation pump seizure
20. Feedwater (FW) increasing flow at power
21. Loss of FW heater
22. Loss of all FW flow
23. Trip on one FW or condensate pump
24. FW, low flow
25. Low FW flow during startup or shutdown
26. High FW flow during startup or shutdown
27. Rod withdrawal at power
28. High flux from rod withdrawal at startup
29. Inadvertent insertion of rods
30. Detected fault in Reactor Protection System (RPS)
31. Loss of offsite power
32. Loss of auxiliary power (transformer)
33. Inadvertent startup High Pressure Coolant Injection (HPCI or HPCS)
34. Scram from plant occurrences
35. Spurious trip via instrumentation RPS fault
36. Manual scram, no out-of-tolerance condition
37. Cause unknown

Table 2.2-2 Generic Transient Events for PWRs

1. Loss of Reactor Coolant System (RCS) flow (one loop)
2. Uncontrolled rod withdrawal
3. Control Rod Drive (CRD) mechanical problems and\or rod drop
4. Leakage in primary system
6. Low pressurizer pressure
7. Pressurizer leakage
8. High pressurizer pressure
9. Inadvertent safety injection signal
10. Containment pressure problems
11. Chemistry and Volume Control System (CVCS) malfunction -boron dilution
12. Pressure, temperature, power imbalance -rod position error
13. Startup of inactive coolant pumps
14. Total loss of RCS flow
15. Loss or reduction in Feedwater flow (one loop)
16. Total loss of FW flow (all)
17. Full or partial closure of MSIV (one loop)
18. Closure of all MSIVs
19. Increase FW flow (one loop)
20. Increase FW flow (all loops)
21. FW flow instability -operator error
22. FW flow instability -miscellaneous mechanical
23. Condensate pumps loss (one)
24. Condensate pumps loss (all)
25. Loss of condenser vacuum
26. Steam generator leakage
27. Condenser leakage
28. Miscellaneous leakage in secondary system
29. Sudden opening of steam relief valves
30. Loss of circulating water
31. Loss of component cooling
32. Loss of service water
33. Turbine trip, throttle valve closure, EHC problems
34. Generator trip or generator caused faults
35. Loss of offsite power (LOSP)
36. Pressurizer spray failure
37. Loss of power to necessary plant systems
38. Spurious trips, cause unknown
39. Auto trip, no transient
40. Manual trip, no transient
41. Fire within secondary system

TABLE 2.2-3
SAFETY FUNCTION SYSTEM REQUIREMENTS

BWRs

Safety Function	Plant System
Reactivity Control	Reactor Protection System
	Standby Liquid Control System
Coolant Inventory Control and Core Heat Removal	High Pressure Coolant Injection System
	Reactor Core Isolation Cooling System
	Low Pressure Coolant Injection System
	Low Pressure Core Spray System
	Control Rod Drive Cooling System
	Condensate System
	High Pressure Service Water System

PWRs

Safety Function	Plant System
Reactivity Control	Reactor Protection System
Coolant Inventory Control	Chemical and Volume Control System
	High Pressure Injection System
	High Pressure Recirculation System
	Low Pressure Injection System
	Low Pressure Recirculation System
Core Heat Removal	Main Feedwater System
	Auxiliary Feedwater System
	Residual Heat Removal System

TABLE 2.2-4

NRC SOURCES OF REACTOR OPERATIONAL DATA

1. **Prompt notification**
   - Required by 10 CFR 50.72
   - Violations of Plant Technical Specifications
   - Approximately 2000 per year

2. **Licensee Event Reports**
   - Required by LER Rule, 10 CFR 50.73
   - Violations of Technical Specifications
   - Focus on Events Significant to Safety
   - NRC Receives Several Thousand per Year

3. **Construction Deficiency Reports**
   - Required by 10 CFR 50.55(e)
   - Approximately 200 in FY83

4. **Component Deficiencies**
   - Required by 10 CFR 21
   - Approximately 200 in 1983

5. **Other Sources**
   - Inspection findings
   - DOE reactor experience
   - Licensee reports and requests
   - Industry Groups
     - Institute of Nuclear Power Operations
     - Nuclear Plant Reliability Data System
     - Electric Power Research Institute
     - Nuclear Safety Analysis Center
   - Informal Communication
   - Foreign Event Information

TABLE 2.2-5

NRC FEEDBACK OF NUCLEAR POWER PLANT EXPERIENCE

Operating Reactors Licensing Actions Summary (NUREG-1272) Vol. 5, No. 1
(AEOD Annual Report)

Bulletins (2 + 1 supplement in 1990) (1 + 1 supplement in 1991)

Information Notices (82 + 12 supplements in 1990) (78 + 15 supplements in 1991)

NRR Generic Letters (10 + 18 supplements in 1990) (18 + 1 supplement in 1991)*

AEOD - review licensee event reports (about 2100 per year)

AEOD - published case studies (about one per year)

AEOD - special studies (about 2 per year)

AEOD - published engineering evaluations (10 in 1990)

AEOD - published technical review reports (18 in 1990)

AEOD - published Power Reactor Events Reports (will resume in 1992)

Report to Congress on Abnormal Occurrences, NUREG-0090 (4 per year)

Miscellaneous NUREGs; case-related hearing testimonies, transcripts, etc.

Plant-Specific Individual Plant Examinations (IPEs)

Performance Indicators for Operating Commercial Nuclear Power Plants (Quarterly)

---

* 91-02, dated December 28, 1990 was considered to be issued in 1990.

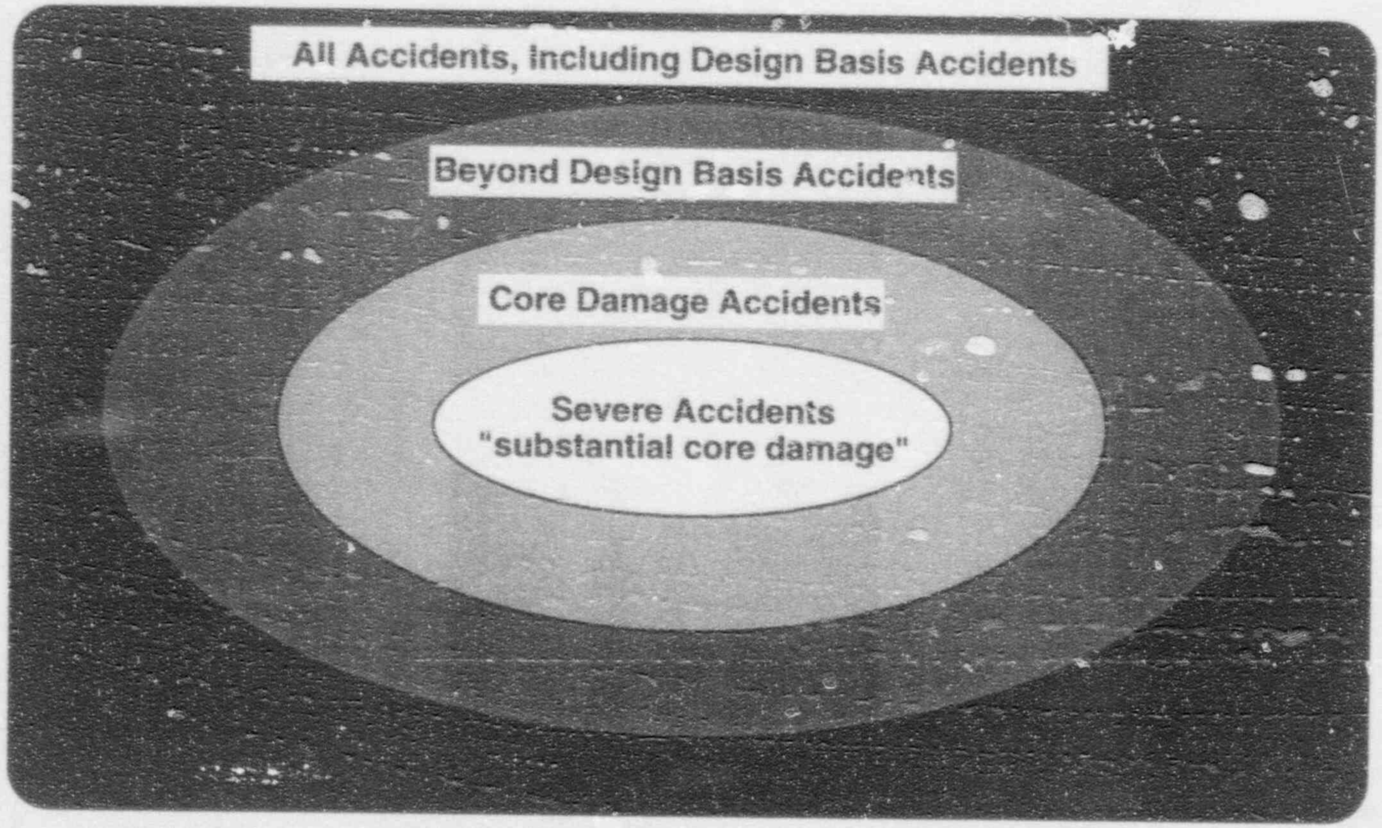


Figure 2.2-1 Breakdown of nuclear power plant accidents by severity

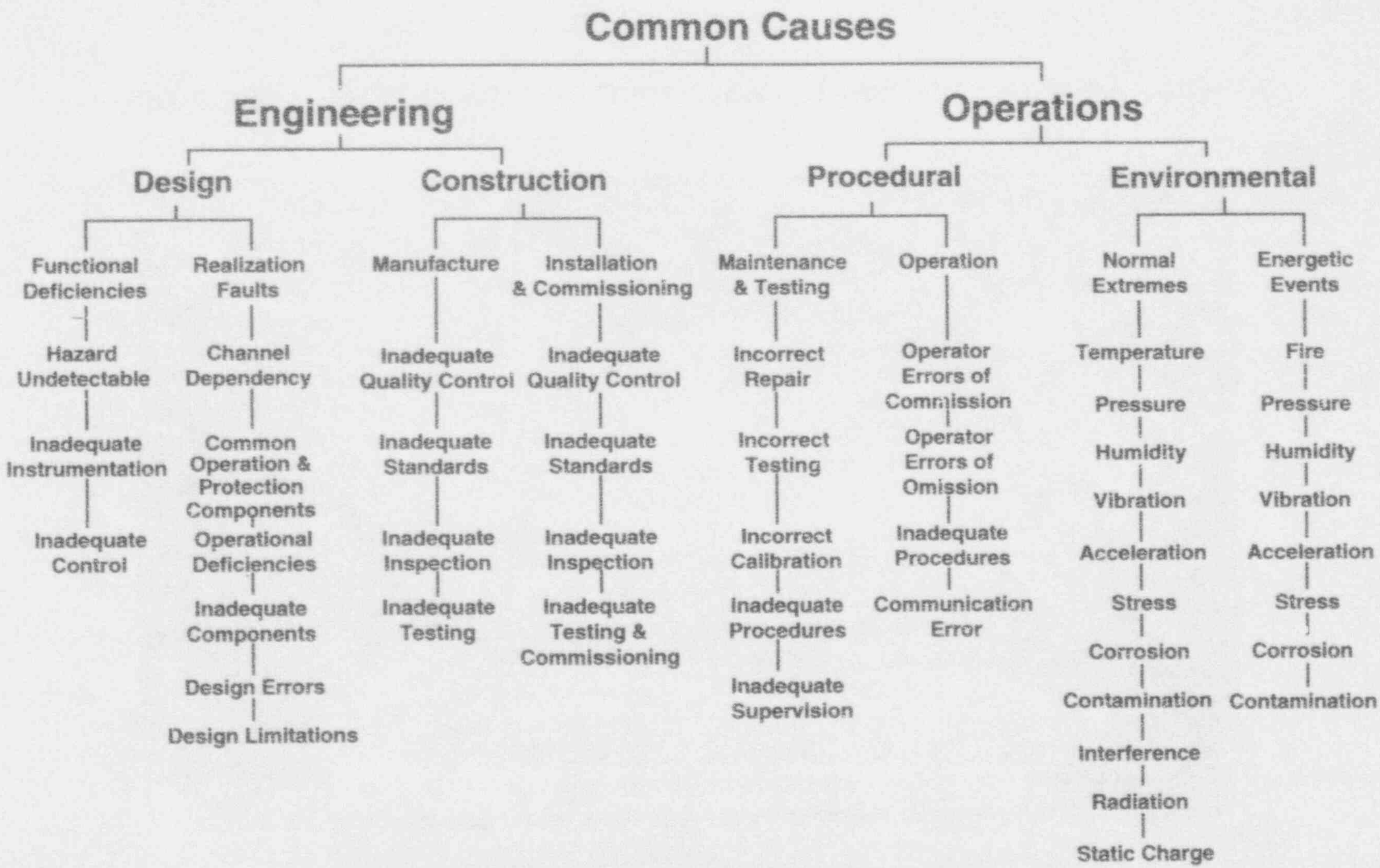


Figure 2.2-2 Common Causes of Failure

2.2.5 References for Section 2.2

1. ACRS subcommittee meeting minutes, June 3, 1966, reproduced in Nuclear Reactor Safety: *On the History of the Regulatory Process* by David Okrent, 1981), pp99-101.

2. Reactor Safety Study, *An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, NUREG-75/014, Appendices III AND IV., Oct. 1975.

3. Title 10, Code of Federal Regulations, Part 50, Appendix K, January 1, 1991.

4. NUREG-1070, *NRC Policy on Future Reactor Designs, Decisions on Severe Accident Issues in Nuclear Power Plant Regulation*, July 1985.

5. D.M. Ericson, *Analysis of Core Damage Frequency: Internal Events Methodology*, Jr., et al,. NUREG/CR-4550, Vol. 1., January 1990

6. J. M. Lanore, et al., CEA/IPSN- France, EPS 900, *A Probabilistic Safety Assessment of the Standard French 900 MWe Pressurized Water Reactor*, April, 90.

7. D. W. Whitehead, *BWR Low Power and Shutdown Accident Sequence Frequencies Project, Phase 2-Detailed Analysis of Pos 5*, NUREG/CR-6143, Nuclear Regulatory Commission, August 31, 1992.

8. Title 10, Code of Federal Regulations, Part 73, January 1, 1991.

9. Title 10, Code of Federal Regulations, Part 50, Appendix A, January 1, 1991.

10. Pickard, et al.,*Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, EPRI NP-5613, Vol 1., U. S. Nuclear Regulatory Commission, January 1988.

11. Title 10, Code of Federal Regulations, Part 50.72, January 1, 1991.

12. Title 10, Code of Federal Regulations, Part 50.73, January 1, 1991.

13. J. W. Minarick, et al., Precursors to Potential Severe Core Damage Accidents, NUREG/CR-4674, Nuclear Regulatory Commission, August 1991.

2.3 Browns Ferry Fire

This section reviews the March 22, 1975 fire at the Browns Ferry nuclear power plant. Most of the material contained here is extracted from an article by R. L. Scott that appeared in *Nuclear Safety* in 1976.[1]

The Browns Ferry nuclear power plant, located near Decatur, Alabama, is owned by the Tennessee Valley Authority (TVA). In early 1975, it was the largest nuclear power plant in the world, having three units with a maximum design power output of approximately 3195 MWe. Units 1 & 2 were operating at a combined level of 1100 MWe. Unit 3 was still under construction. On March 22, 1975, the Browns Ferry plant was subjected to a fire that lasted 7 hours, caused an estimated damage of $10 million, and resulted in two operating units being incapacitated for over a year. As a result of the shutdown of the two units, additional costs of about $10 million were incurred each month for replacement power.

The fire was initiated by a small (3" to 4" or 7 to 10 cm) lit candle that was being used to check for air leakage of the reactor containment building (Figure 2.3-1). The flame ignited some polyurethane used to seal leakage paths, and the fire burned for 7 hours before being extinguished (Figure 2.3-2). The reactor building is maintained at a negative pressure with respect to the exterior of the walls in order to ensure that any airflow is always into the reactor building. It was this design feature that aggravated the fire. The purpose of maintaining a negative pressure on the reactor building is to continuously remove the air and pass it through filters to remove any radioactivity that might be present. However, in order for radioactivity to be present in the reactor building, it would first have to escape from the primary containment or piping. Then, any radioactivity that managed to get into the reactor building would be removed by the filters, with no effect or impact on public health and welfare. The cable-tray penetrations through the wall of the reactor building are sealed to minimize inleakage, thus maintaining an adequate negative pressure in the reactor building. The penetrations are filled with a polyurethane foam to form the seal, and then a flameproofing compound is applied 3 to 6 mm (~0.1") thick over the foam and over the cables on both sides of the penetration for a distance of 30 cm (12") to form a fire barrier (Figure 2.3-3).

The penetration where the fire originated had been disturbed at some time after the initial installation, because holes had been punched through the flameproofing and sealant to provide openings for additional cables through the penetration. The result was that the polyurethane sealant was exposed. Leakage tests had been performed previously on the reactor building, and the results indicated that inleakage should be reduced. An extensive program was therefore under way for resealing penetrations through the wall of the reactor building.

The method used to check the effectiveness of the sealing operation was to hold a lit candle near the penetration opening. If the opening was not fully sealed, the lower pressure in the reactor building would cause air to be pulled through the opening, giving a good visual indication of leakage even where the area was poorly lit. The use of an open flame to test for air leakage in a condenser vacuum was then a commonplace practice for the utility industry.

2.3.1 Initiating Events

On March 22, three teams, each consisting of an engineering aide and an electrician, were working in the cable-spreading room testing and sealing penetrations. Work proceeded during the day without incident until about 12:15 p.m., when an engineering aide observed a hole about 50 to 100 mm (2 to 4") wide in a cable-tray penetration through the wall. The hole was approximately 20" or 0.5 m back into the penetration from the face of the concrete wall, and the entire penetration was congested with cable trays, making the hole difficult to reach (Figure 2.3-4). The engineering aide passed a lit candle by the hole, and the flame blew horizontally into the hole,indicating a significant leakage path into the reactor building. The aide had difficulty reaching into the penetration, but he tried to stuff two pieces of sheet polyurethane foam into the hole. (This sheet polyurethane was not the same type as that used originally for the sealant; this type is far more flammable.) He then re-lit the candle and re-checked the penetration. The flame was again pulled horizontally, indicating a large airflow and leakage path, and apparently the foam ignited at this time -12:20 p.m. The aide observed a low red glow and yelled "fire." His attempt to beat the fire out with a flashlight was unsuccessful. He then tried to smother the fire with rags, but this also failed. He then discharged a CO_2 fire extinguisher twice, but the CO_2 was pulled right through the hole without putting the fire out. Two more dry-chemical fire extinguishers were discharged into the hole, but each gave "only one good puff" and the fire continued. The electrician then called for someone to notify the reactor operations shift engineer that there was a fire in the cable-spreading room. Meanwhile, the fire had moved deeper into the hole because of the airflow and was now also on the reactor-building side of the wall; thus there were two fires to contend with -- one in the cable-spreading room and one in the reactor building.

2.3.2 Cable-Spreading Room Fire

About 15 min after the fire started (at approx. 12:35 p.m.), a siren alarm sounded to warn personnel in the cable-spreading room to evacuate because the permanently installed CO_2 Cardox fire-extinguishing system was to be actuated. This system flushes the room with enough CO_2 to displace most of the oxygen required for the survival of the personnel. After the room was evacuated, an assistant shift engineer attempted to actuate the Cardox system at the Unit 1 cable-spreading room control station but found that the power had been shut off at the disable switch at the Unit 2 entrance to the room. This isolation procedure was a safety measure taken while men were leak-testing the penetration. The engineer then turned the power on at Unit 2, apparently without success, after which he attempted to use the manual crank system. However, he found that a metal plate had been installed under the breakout glass to prevent inadvertent operation of the CO_2 system. The actuation at Unit 2 appeared to be unsuccessful because there was a 3-min delay from the time of actuation due to travel time from central storage, but at about 12:40 p.m. the Cardox system began discharging CO_2 for the first time.

Between 12:40 p.m. and 3:00 p.m., the Cardox system was actuated two more times as the fire fighting continued under the direction of an assistant shift engineer. At about 1:45 p.m., firemen from the Athens, Alabama, Fire Department arrived and began to assist in the fire-fighting efforts. At about 2:00 p.m., the Fire Chief recommended the use of water on the fire, but the Plant Superintendent decided against this because of the possibility of shorting circuits, which could further degrade conditions such that control of the shutdown and cooling of the reactors would be more difficult. Furthermore, the fire was progressing slowly (.8" to 1.2"/min. or 2 to 3 cm/min). The use of CO_2 and dry chemicals kept the fire suppressed, but, on several occasions when the fire was reported to be out, it flared up again because of the high energy content in the cables. At 3:00 p.m., a shift engineer arrived at the site, proceeded to the cable-spreading room, and assumed charge of the fire fighting. The fire in that room was finally reported to be extinguished at about 4:20 p.m.

2.3.3 Reactor-Building Fire

The fire that started on the cable-spreading room side of the penetration spread into the reactor building because of the inward airflow. Two construction workers in the cable-spreading room, on seeing that the fire was spreading into the reactor building, went there to fight the fire. One of the workers notified a TVA Public Safety Officer that there was a fire in the reactor building. The two workers were joined by a third, and all three, equipped with dry-chemical fire extinguishers, proceeded to the fire in the reactor building. The fire was burning in cable trays that were *20' or 6.1 m above the second floor* of the reactor building. A worker climbed a ladder placed next to the fire and discharged a dry-chemical extinguisher on the fire, but he was then forced to leave because he could not breathe. This dry-chemical application suppressed the flames but not the temperature, and the fire flared up again.

At about 12:34 p.m. the general fire alarm was actuated. An assistant shift engineer arrived, climbed the ladder, and discharged a dry-chemical extinguisher on the fire, after which he discharged a CO_2 extinguisher on the fire. He also experienced breathing difficulty, and by this time smoke was becoming so dense that a breathing apparatus was requested. Until the apparatus arrived, CO_2 was applied to the cable trays from the floor. When the apparatus (air packs) arrived, fire fighting continued until visibility became so poor that the workers could not get near the fire.

The assistant shift engineer left the area and called the Athens Fire Dept. at 1:09 p.m. The fire truck arrived at 1:30 p.m., and, by 1:45 p.m., seven firemen had been admitted to the plant and were prepared to assist in fighting the fire but in support of, and under the direction of, Browns Ferry personnel. It has been stated that there appears to have been no central organized direction of the fire-fighting efforts in the reactor building between approximately 1:00 p.m. and 4:20 p.m. However, it should be noted that the ventilation system was lost at 12:45p.m. and was not reestablished until 4:00 p.m. The consequence was excessive smoke, making visibility poor and necessitating air-breathing equipment. Also, lighting was lost in the reactor building at about 1:30 p.m. In addition, there was a shortage of air-breathing equipment, and the available equipment was used by workers who were manually aligning valves in an attempt to get the reactor into a shutdown cooling mode. Once the plant was depressurized and a positive source of water was going into the reactor, attention was focused on the fire in the reactor building. At about 4:30 p.m. the shift engineer who had directed the activities in the cable-spreading room until that fire was extinguished took charge of the fire-fighting activities in the reactor building. Temporary DC lighting was set up both inside and outside the reactor building, and a routine was established of sending in two or three fire fighters at a time to use dry chemicals on the fire. At about 6:00 p.m. the Athens Fire Chief again recommended the use of water (his first recommendation was at 2:00 p.m.). Water had not been used because of the electrical shock hazard, and the Plant Superintendent had not wanted to de-energize the circuits because he felt some of them were needed for controlling the shutdown of the reactors.

At approximately 7:00 p.m. the Plant Superintendent agreed to the use of water on the fire, contrary to the recommendation of the TVA Public Safety Officer, because the reactors were in a more stable condition. Another shift engineer took the fire hose, climbed the scaffolding to the fire, and sprayed water on the fire, using a water fog-type nozzle. He had difficulty breathing, and so he jammed the nozzle of the hose into the cable tray so that it would continue spraying water on the fire area and then climbed down and left the building. Later, two shift engineers returned and sprayed the area again. At 7:45 p.m. the fire was declared to be out.

2.3.4 Fire Damage And Assessment

The fire-damaged areas of the cable-spreading room and the reactor building are shown in Figure 2.3-5. As indicated, the damage in the cable-spreading room extended only about 1.5 m (5 ft.) north of the wall penetration. Most of the damage occurred in the reactor building, extending up to 11.4 m (37 ft.) from the wall penetration. A total of 117 conduits, 26 cable trays, and 1611 cables were damaged. In all, about 9300 conductors had to be replaced or spliced. Of the 1611 cables damaged, 628 were safety related.

At 4:00 p.m. on Saturday, March 22, the Atlanta Regional Office of the NRC Office of Inspection and Enforcement was notified of the fire, in accordance with requirements. The Atlanta office immediately initiated an investigation that ultimately required 280 man-days of effort. The detailed report was given to TVA and made available to the public on July 28, 1975, along with a Notice of Violation of NRC requirements and a list that identified areas of concern. It should be noted that the Notice of Violation was corrective rather than punitive; that is, the aim was to correct deficiencies.

2.3.5 Effect of Fire on Unit 1

Since the control room for the reactor is common to both Units 1 and 2, activity at one unit could be observed by the operators of both units. About 20 min after the fire started, the Unit 1 operator noted anomalous behavior of controls and instrumentation for systems designed to provide emergency cooling of the reactor core. For the next several minutes, a mounting number of events occurred, such as the automatic starting of pumps and equipment, which the operator would shut down when he determined that they were not needed, only to have them automatically start again.

At 12:51 p.m. the reactor was scrammed, shutting the reactor down. This stopped the chain reaction and eliminated nuclear fission as a direct source of heat; however, heat generation in the core continued as a result of radioactive decay of fission products in the reactor fuel. It was this aspect that was of major concern to the nuclear reactor operators, because continuous cooling of the fuel to remove this decay heat must be provided to prevent damage to the fuel. During the first few hours after shutdown, the decay-heat level can be 2 to 3% of the heat output at full power, decreasing to 1% after 1 day and declining very slowly thereafter. Therefore the most urgent need for cooling is during the first few hours after the reactor is shut down.

About 4 min after the reactor was shut down, several electrical boards that supplied control voltages and power to many of the systems used in cooling the reactor after shutdown were lost. Also, many of the instruments and indicating lights were put out. Shortly after 1:00 p.m. the main-steam-isolation valves closed automatically, causing several problems. First, the steam generated by the decay heat could not be passed to the condenser, thus eliminating this method of removing the decay heat. Second, the valve closure resulted in the loss of steam that was driving the feedwater pumps, thus eliminating another method of providing high-pressure cooling water to the core. Fire had also disabled the High Pressure Coolant Injection and Reactor Core Isolation Cooling systems. Even though a control-rod-drive-system pump was supplying flow at around 400 liters/min (105 gpm), the water level over the fuel began to decrease because of boiling caused by the decay heat. Condensate booster pumps were operable, but these pumps can only inject water into the pressure vessel at pressures of 2.4 MPa (~ 350 psi) or less. Given these conditions, the operator chose to depressurize the reactor, which was 7.4 MPa (1070 psi) at this time, by remote control of the relief valves to permit the use the low-pressure systems that were still available.

The pressure-relief valves were manually opened from the control room, and the steam was transferred from the pressure vessel to the pressure-suppression pool (still within primary containment) and condensed. By this method the pressure in the vessel was reduced to about 1.8 MPa (260 psi) in 20 min; the condensate booster pumps were then used to maintain an adequate water level in the reactor vessel. During the depressurization period the water level in the core decreased but did not drop below a point 1.2 m (4 ft.) above the top of the fuel. Normal level is 5.08 m (200"), but the 1.2 m (4 ft.) level is still 0.76 m (2.5 ft.) above the level at which the core spray and residual-heat-removal systems are actuated. Once the reactor pressure was reduced below 2.4 MPa (350 psi), one condensate booster pump and one condensate pump provided adequate makeup water, and the normal water level above the fuel was attained.

This mode of core cooling was adequate until about 6:00 p.m., when loss of control air prevented further manual control of the remaining (4 out of 11) operable pressure-relief valves. The valves closed, and pressure in the vessel started building up again. As pressure increased above 2.4 MPa (350 psi), the condensate booster pumps could no longer inject water into the vessel and thus only the control-rod-drive-system pump was adding water.

After the fire was declared out at 7:45 p.m., the smoke began to clear, and reliance on breathing apparatus decreased so that a more orderly approach to obtaining shutdown cooling could be taken. The actual valve conditions (opened or closed) were determined, and control power to motor operators, pump controls, etc., was established using temporary jumpers.

After about 3 1/2 hours (at about 9:50 p.m.) control of the relief valves was restored, the reactor was depressurized, and the condensate booster pump again pumped water into the reactor. With low-pressure operation now secured, adequate makeup water could be supplied by one of the condensate pumps. In addition, two additional condensate booster pumps and two additional condensate pumps were available to the operator. Another alternative would have been to use a nonstandard system configuration and manual valve alignment. Two residual-heat-removal-pumps in Unit 2 could have been aligned to the Unit 1 reactor through a crosstie pipe, and, as an additional backup, river water could have been used from either of two available service-water pumps. At 4:10 the next morning, normal shutdown cooling was established.

A chart displaying equipment and system availability is shown in Figure 2.3-6. It should be pointed out that, with the reactor at high pressure, there were other alternatives for obtaining makeup water to the reactor. A few examples of other alternatives are listed below:

1. The Unit 2 control-rod-drive (CRD) pump and a shared spare CRD pump could have been used in addition to the CRD pump on Unit 1.

2. The standby liquid-control pumps could have been made available by performing a manual valve alignment, actuating two valves, and manually restoring power to the pumps.

3. The reactor core-isolation cooling system (RCICS) could have been made available by installing a special short piece of pipe that was stored nearby.

The point is that adequate cooling-water makeup was provided throughout the incident, and additional alternatives could have been used to provide makeup water with the reactor at either high or low pressure.

2.3.6 Effect of Fire on Unit 2

The effect of the fire on Unit 2 was less pronounced. A few minutes after Unit 1 was shut down, abnormal events, such as decreasing reactor power, sounding of many alarms, and loss of some indicating lights, began to occur in Unit 2. The operator shut the reactor down at 1:00 p.m. About 3 minutes later the main-steam-line isolation valves closed automatically and high-pressure cooling systems were successfully initiated. After depressurization, low-pressure pumps were used to provide cooling. By 6:30 p.m., stable conditions were obtained,and normal means for cooling the core were established by 10:45 p.m.

2.3.7 Lessons Learned

The extent of damage caused by the fire is attributable to the length of time the fire burned. TVA's rationale for not using water to suppress the fire earlier in the sequence of events was stated as follows: "The Plant Superintendent made the conscious decision not to use water because of the possibility of shorting circuits and further degradation of the plant to a condition that would have been more difficult to control. Reactor safety concerns under the circumstances took precedence over extinguishing a localized fire." This position reflected a fairly widespread reluctance on the part of licensees at the time to use water on a fire involving electrical cables. However, the failures caused by the fire as it continued to burn were largely responsible for the difficulties encountered in bring the plant to a safe stable state, and the fire was extinguished rather quickly when water was finally applied. Hence the main lesson learned is that, if initial attempts to extinguish a cable fire with nonwater means are unsuccessful, water should be used.

The damage to electrical power and control circuits resulted in the loss of redundant subsystems and equipment. This was surprising in view of the independence and separation criteria that had been applied in the design of the plant. The two principal reasons for the failures were found to be: (1) failure to recognize potential sources of failure of safety equipment (i.e., the interconnection of safety equipment and nonsafety circuits such as the indicator-light circuits); and (2) contrary to what had been considered good practice, the conduit used to isolate cables from their redundant counterparts did not protect the cables adequately.

Although damage inflicted by the fire resulted in the loss of a number of systems, in particular the emergency core-cooling system, alternatives were available, and adequate cooling was provided throughout the event. In addition, other systems were restored both during and after the fire, and some equipment was restored by manual operation -- especially valves using handwheels. Therefore, loss of the emergency core-cooling systems made the situation more difficult, but not impossible because of the numerous alternatives.

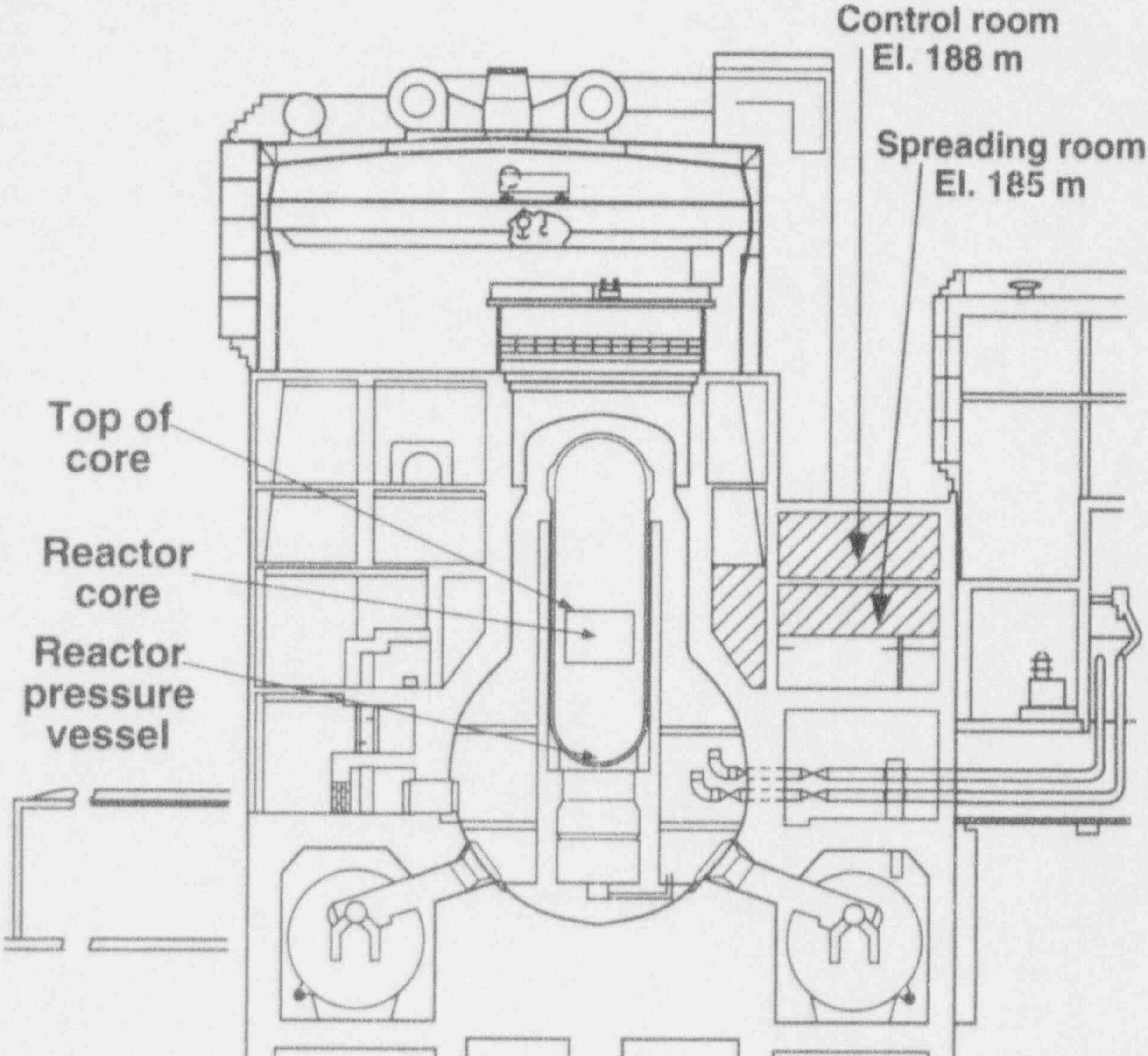


Figure 2.3-1 Vertical cross section of plant showing reactor building control room, and spreading room

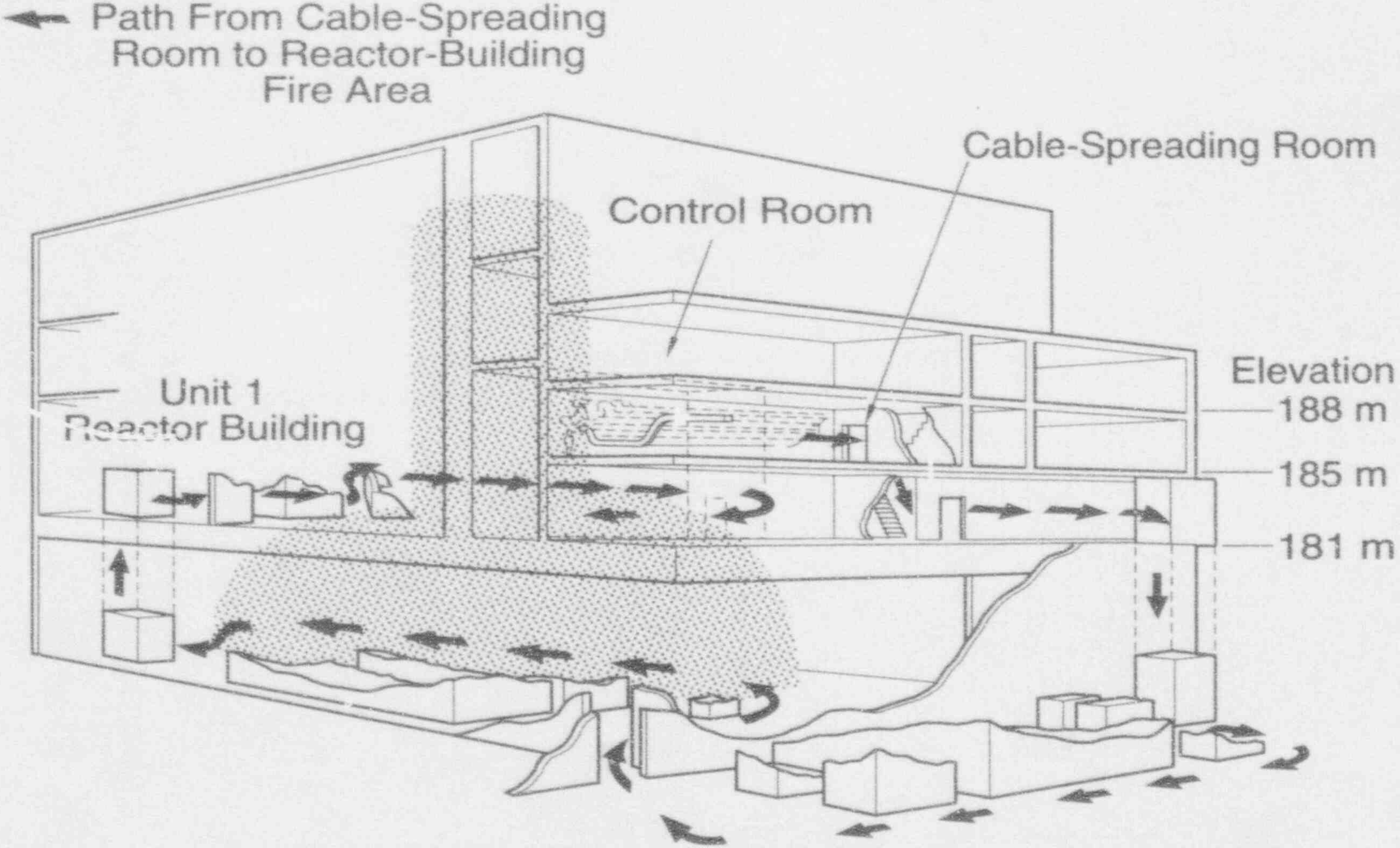


Figure 2.3-2 The Browns Ferry nuclear plant

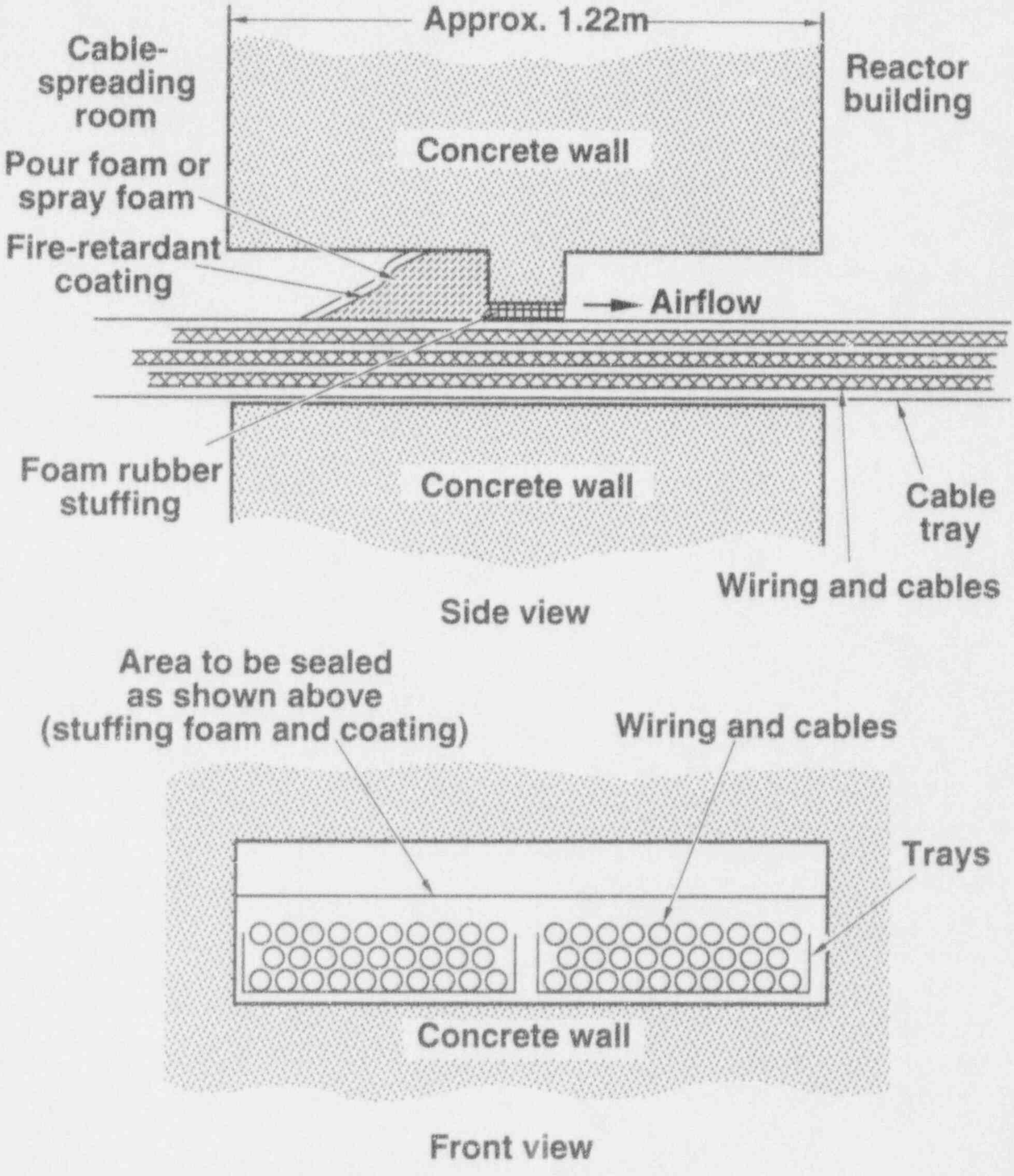


Figure 2.3-3 Cable-tray penetration. Overall simplified depiction (not to scale).

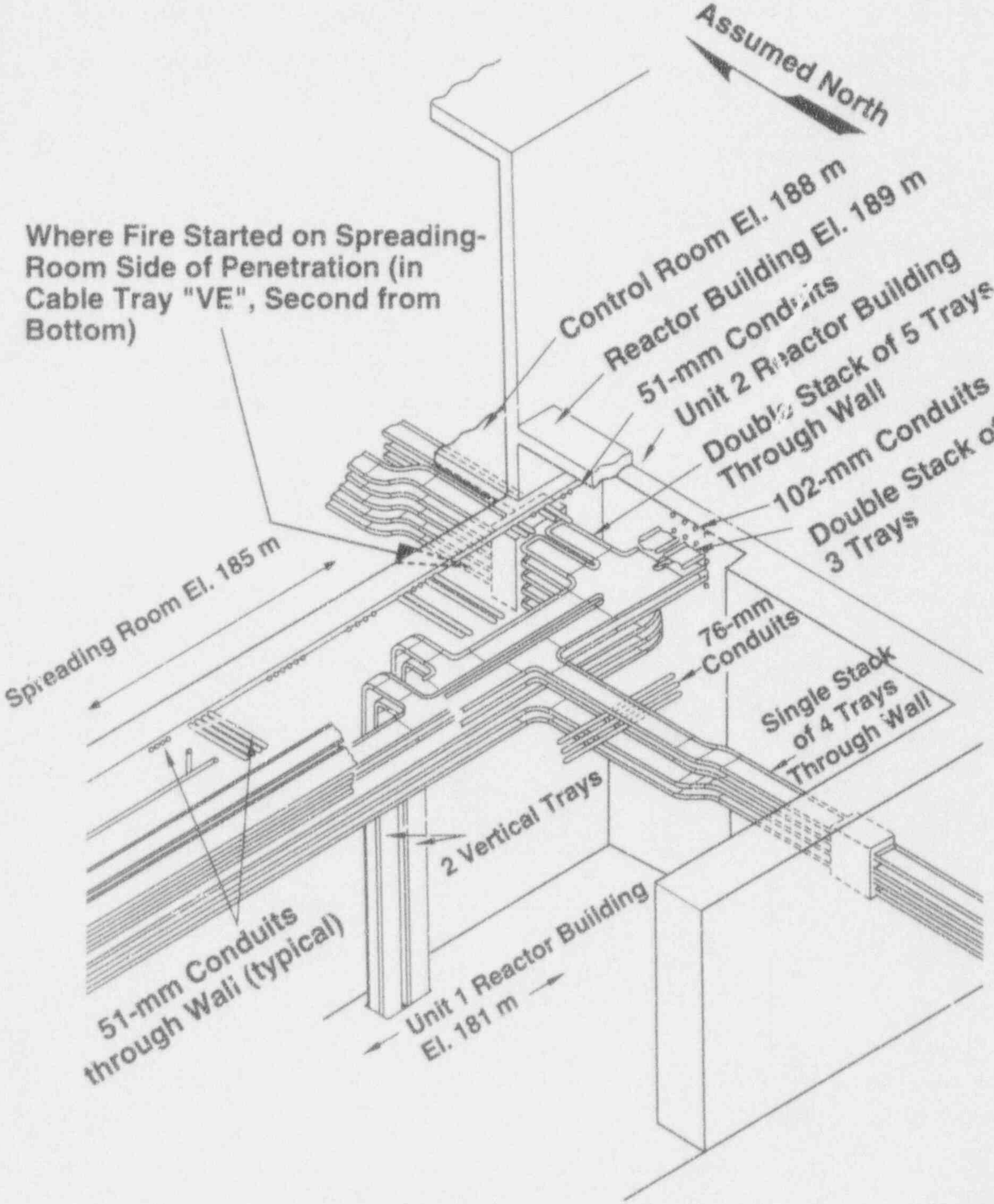


Figure 2.3-4 Area where fire started

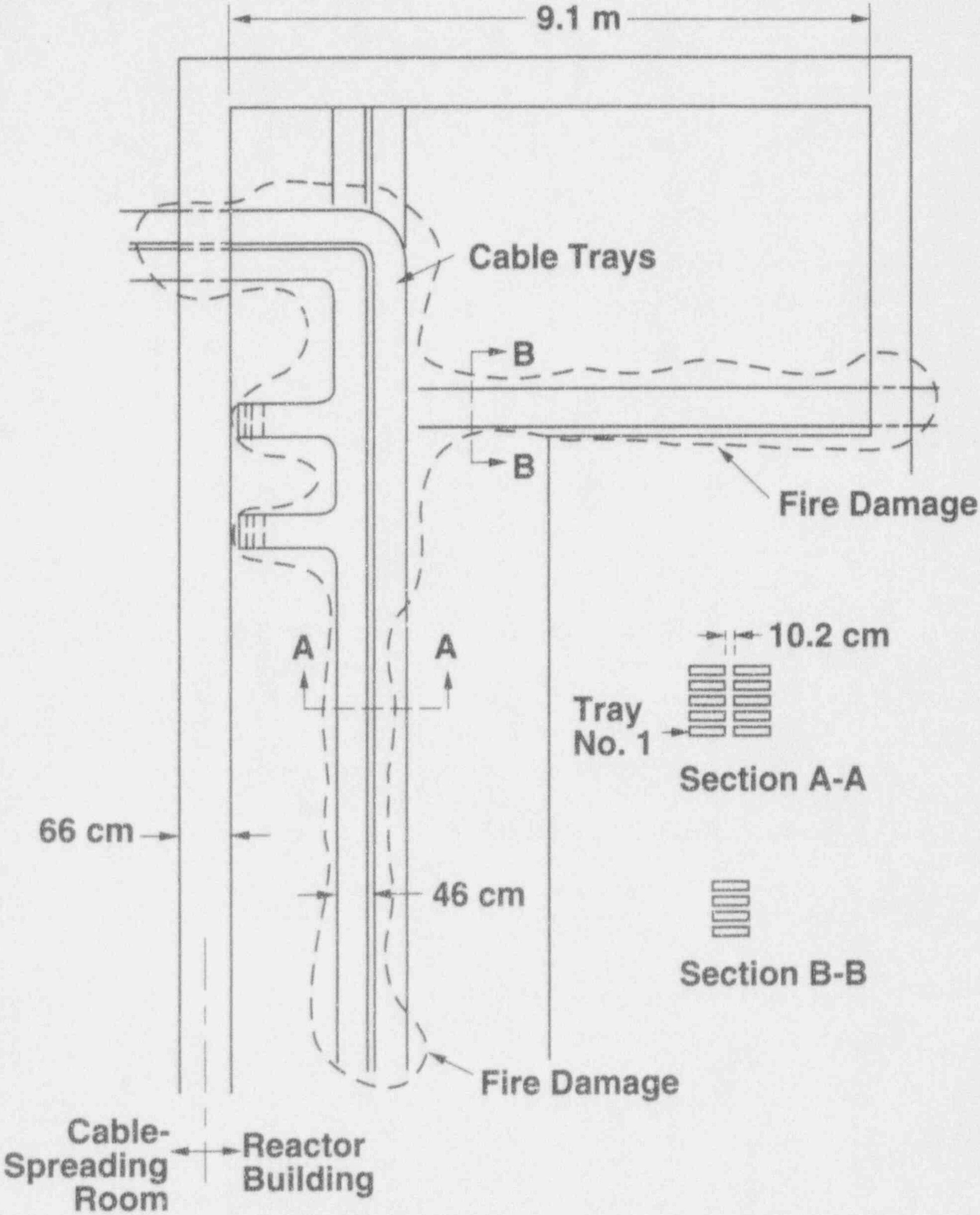


Figure 2.3-5 Fire-damaged area

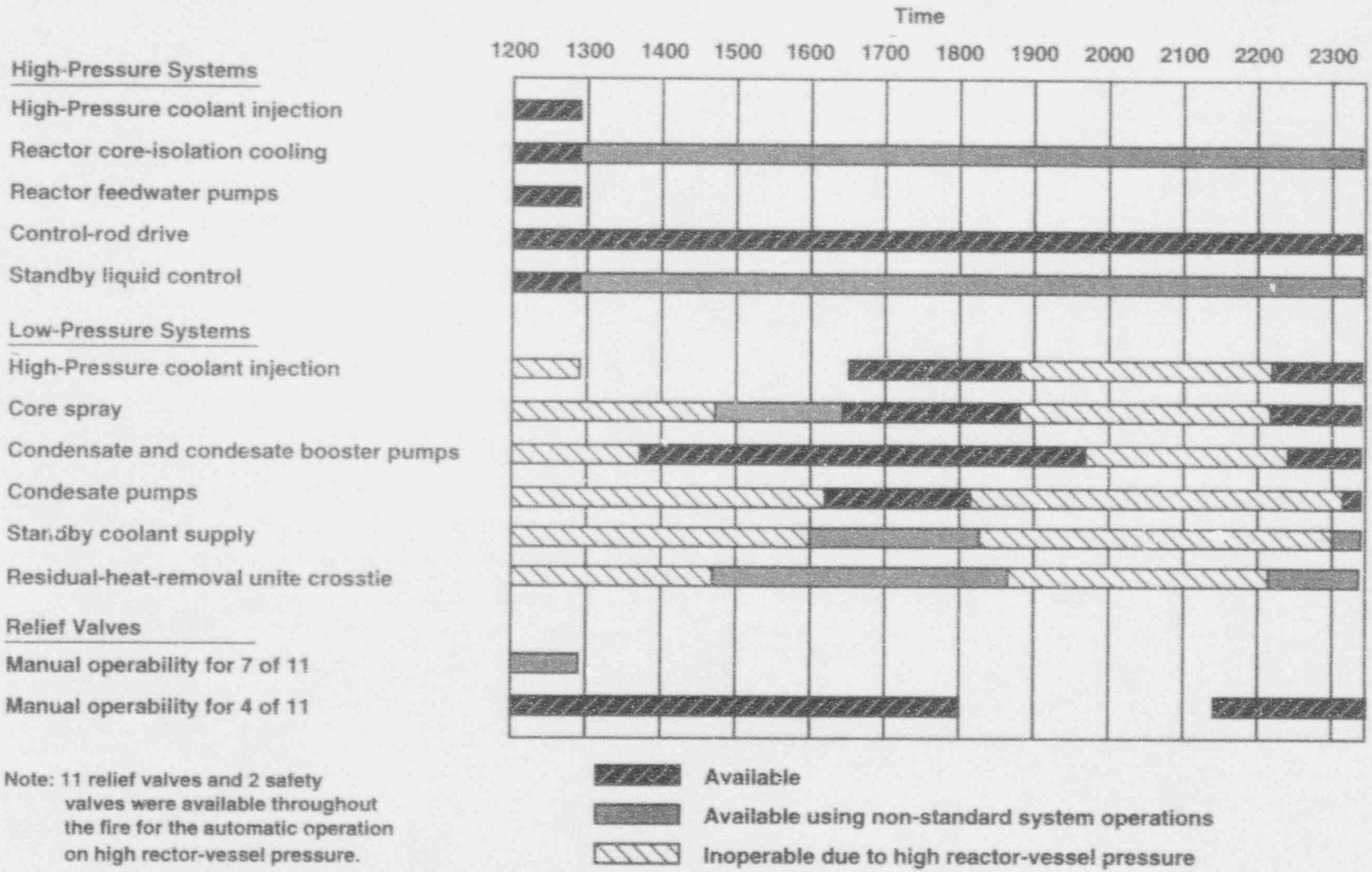


Figure 2.3-6 Equipment availability during and immediately following the Ma. 22, 1975, fire.

References for Section 2.3

1. Scott, R.L. "Browns Ferry Nuclear Power Plant Fire on March 22, 1975" *Nuclear News* Volume 17, No. 5, September-October 1976, p. 592.

2.4 TMI-2 Accident Sequence

2.4.1 Introduction

The Three Mile Island (TMI) Nuclear Station is operated by the Metropolitan Edison Company, a member of the General Public Utilities Corporation. TMI is located near Middletown, Pennsylvania, about 10 miles southeast of Harrisburg, the state capitol. At the time of the accident, the station had two Babcock & Wilcox PWR's, Unit 1 rated at 792 MWe and Unit 2 rated at 880 Mwe. Figure 2.4-1 depicts the nuclear steam supply system including the reactor vessel, two once-through steam generators, four reactor coolant pumps (two per loop), and the pressurizer. The hot-leg piping carries heated coolant from the reactor outlet nozzles to an inlet at the top of each steam generator. Two cold-leg pipes carry reactor coolant from the bottom head of each steam generator to the respective reactor coolant pumps and back to the vessel through inlet nozzles. Other features shown on Figure 2.4-1 include the core flood tank, the reactor coolant drain tank, and the reactor building sump. The entire nuclear steam supply system depicted in Figure 2.4-1 is in a cylindrical steel-lined concrete containment called the reactor building.

The following description of the sequence of events that occurred during the TMI-2 accident is condensed from several sources.[1,2,3,4,5,6] In particular, the NRC investigation produced a scenario that runs over 100 pages.[1]

2.4.2 Pre-existing Problems

The TMI-2 reactor, the 880 MWe unit, was operating at 97% of rated power before the accident. Figure 2.4-2 is a simplified drawing that depicts the pre-accident conditions in the reactor coolant system. Figure 2.4-2 indicates a reactor coolant system pressure of 2150 psig (14.8 MPa), flow of subcooled water through both reactor coolant loops, a steam bubble in the pressurizer, and boiling of secondary water in both steam generators. Similar drawings are used to indicate conditions in the reactor coolant system as the accident progresses.

Before the accident began, there had been a persistent leak of reactor coolant from the pressurizer to the reactor coolant drain tank. The leak was known by the operators to be through either the electromagnetic Pilot-Operated Relief Valve (PORV) or one or both of the pressurizer safety valves. The safety valves and PORV are provided, as their names imply, to relieve abnormally high reactor coolant pressures. The safety valves open automatically on high pressure to prevent rupture of the reactor coolant system. The PORV opens automatically at a lower pressure to prevent inadvertent and unnecessary opening of the safety valves. In spite of the leak, the pressurizer water level and the reactor coolant pressure were being held at normal levels by the operators. Consequently, they were not particularly upset by the leak. (The NRC later concluded that this pre-existing leak exceeded technical specification limits.) The leak played a role in subsequent events in at least one respect. It created high temperature indications in the downstream piping, and these pre-existing indications later disguised a more serious loss of coolant.

Figure 2.4-3 shows the condensate and feedwater system. Steam from the steam generators passes through the turbine and condenses in the condenser. Water from the condenser hotwell is pumped first by the condensate pumps through the condensate polishers, then by the condensate booster pumps through the low pressure feedwater heaters, and finally by the feedwater pumps through the high pressure feedwater heaters to the steam generators. The condensate polishers use ion exchange resins to purify the feedwater. For roughly 11 hours prior to the accident, shift foremen and auxiliary operators had been attempting to transfer spent resins from the condensate polishers to a resin regeneration tank.

Under normal circumstances, compressed air is used to "fluff" spent resins, which are then transferred in demineralized water through a transfer line between the tanks. But a resin block developed in the transfer line driving water back through the isolation valve between the demineralizer and the condensate pumps. As a result, water entered an instrument air line through a check valve that had frozen open. This apparently caused the polisher inlet and/or outlet isolation valves to drift toward the closed position. The accident began when all the isolation valves on the condensate polishers closed. This in turn caused one of the two operating condensate pumps and both of the condensate booster pumps to trip initiating the TMI-2 accident at 4:00:36 a.m. on Wednesday, March 28, 1979.

2.4.3 Loss of Feedwater

A fairly detailed chronology of the TMI-2 accident is provided in Table 2.4-1. The reader may find it useful to refer to this chronology and the associated Figures frequently. For the most part, times in the following discussion are measure in hours (h), minutes (min), and seconds (s) from turbine trip, which occurred 1 s after the condensate pump trip. Where clock times are specified, they are denoted with an a.m. or p.m. suffix, as in 4:00:36 a.m.

Within the first second of the accident, condensate pump 1A, the two condensate booster pumps, the two feedwater pumps, and the turbine tripped. The resulting loss of main feedwater to the steam generators drastically reducing the rate of heat removal from the reactor coolant system. During the initial seconds following the loss of main feedwater, the reactor continued to operate, and the reactor coolant began to heat up and expand. This caused the rapid initial increase in reactor coolant pressure and pressurizer level shown in Figure 2.4-4. About 3 s after turbine trip, the reactor coolant pressure exceeded the PORV setpoint of 2255 psig (15.55 MPa) causing the PORV to open. The reactor coolant pressure continued to rise until, at about 8 s, the reactor automatically scrammed on high reactor coolant pressure. As a result of the reactor trip, the volume of the liquid reactor coolant began to contract, and the reactor coolant pressure began to fall as indicated in Figure 2.4-4.

2.4.4 Loss of Coolant, Core Cooled (13 s to 101 min)

2.4.4.1 PORV Sticks Open

The opening of the PORV and the reactor trip functioned as designed to prevent overpressure in the reactor coolant system. However, trouble developed at 13 s when the reactor coolant pressure dropped below the 2205 psig (15.21 MPa) setpoint for PORV closure. A mechanical failure caused the PORV to stick open. Because the PORV remained open, steam continued to flow, undetected, through the stuck-open PORV, and reactor coolant pressure continued to fall rapidly as indicated in Figure 2.4-4. A loss-of-coolant accident (LOCA) had been initiated. It went undetected because control room personnel did not realize that the PORV was stuck open. A control board indicating light signalled that the PORV was closed. In fact, this merely indicated that the actuating solenoid was de-energized. No direct reading of actual valve position was available.

Had they recognized the PORV was open, the operators could have closed a block valve manually, thereby mitigating the effect of the stuck-open relief valve and totally preventing subsequent damage to the reactor core. Should the operators have known enough to close the block valve in spite of the erroneous indicating light? Certainly a rapid drop in reactor coolant pressure as depicted in Figure 2.4-4 is not a normal response to a loss of feedwater. The operators virtually ignored this symptom, and (as discussed later) focused instead on the pressurizer level behavior depicted in Figure 2.4 -4.

Another way of determining the position of the PORV is by reading the temperature in the pipes leading from this valve to the reactor coolant drain tank. An abnormally high temperature indicates the presence of escaping reactor coolant. In fact, such readings were made and high temperatures were noted, but they were thought to be caused by the same valve leakage that the operators were aware of before the accident.

The open PORV could also have been inferred from the reactor coolant drain tank pressure. This pressure began increasing when the PORV first opened 3 s after turbine trip. At about 3 min 12 s, the relief valve on the reactor coolant drain began opening intermittently. At 14 min 48 s, the tank's rupture disk blew, as designed, at 192 psig. The pressure in the tank then dropped rapidly. Had an operator observed the drain tank pressure meter before the rupture disk blew, the fact that the PORV was open could have been diagnosed. However, the meter was on a panel behind the roughly 7-ft-high reactor console on which all critical instruments were placed. The plant's data acquisition computer did contain a time history of the tank pressure. However, data printout lagged significantly during the intense activity associated with the accident.

Clearly, there were reasons for the operators in these early minutes of the accident to have missed the fact that leakage was continuing through the PORV. But there were to be persistent signs of a serious loss of coolant that would be ignored. In short, the operators at Three Mile Island didn't realize they had a loss of coolant through the relief valve until 139 min. By then matters had passed the point of no return.

2.4.4.2 Loss of Auxiliary Feedwater

The auxiliary feedwater system is designed to compensate for a loss of main feedwater and prevent the steam generators from going dry. The three auxiliary feedwater pumps (two electric-driven and one steam-driven) started automatically within 1 s of the trip of the main feedwater pumps. The automatic auxiliary feedwater isolation valves also opened, as designed, after two conditions had been met: (a) the auxiliary feedwater pumps were delivering their normal discharge pressure (at least 875 psig); and (b) the water level in the steam generators was 30 inches or less. Condition (a) was satisfied 14 s after turbine trip. Condition (b) was satisfied at about 30 s.

There are also block valves in the auxiliary feedwater lines to the steam generators. These block valves are required to be open while the plant is operating. Records indicated that the valves had been reopened following maintenance completed 2 days earlier; however, they were not open at the time of the accident. It took the operators 8 min to discover the valves were closed, in part, because tags on the control room panel inadvertently covered the valve position indicator lights. As a result, there was no flow of auxiliary feedwater from the condensate storage tank to the steam generators until an operator opened the block valves at 8 min 18 s.

Babcock & Wilcox claimed that, had there been auxiliary feedwater, the temperature of the reactor coolant might have remained relatively stable until the problem of the condensate pumps was corrected and normal feedwater was reinstated. This view has been contested not only by the NRC but also by the utility-sponsored Nuclear Safety Analysis Center, an investigative arm of the Electric Power Research Institute. Their investigations indicate that, except for adding another dimension to the areas of concern within the main control room, the early unavailability of auxiliary feedwater did not significantly affect the progression of the accident, which was dominated by the uncompensated loss of reactor coolant.

2.4.4.3 Throttling of High Pressure Injection

In a normal loss of feedwater scenario, without the stuck open PORV, the reactor coolant continues to contract after reactor trip. Letdown flow is reduced or stopped, and makeup flow is increased to maintain the normal water level in the pressurizer. With this in mind, at 41 s, an operator manually started a second makeup pump (1B) to reverse the downward trend in the pressurizer level shown in Figure 2.4-4.

At about 1 min, the water level in the pressurizer indeed began to increase. But this was not solely due to increased makeup flow. With the stuck open PORV, the reactor coolant pressure continued to decrease and the NRC contends that as early as 1 min and continuing thereafter the reactor coolant experienced either a general expansion, as might occur with distributed voids, or the formation of one or more discrete steam vapor voids. As reactor coolant circulating through the core became saturated, it expanded and its pressure increased. The force exerted by this expanding reactor coolant through the pressurizer surge line caused the water level in the pressurizer to increase.

The pressurizer heaters, which would normally be used to keep the coolant in the RV subcooled, had tripped. Even if they had been operational, their energy addition capacity was far exceeded by the rate of energy loss out the stuck open PORV.

About 2 min after turbine trip, the reactor coolant pressure dropped below 1600 psig as a result of the stuck-open PORV. At this pressure the emergency core cooling system was automatically actuated. Makeup pump 1C started and makeup pump 1B tripped leaving pumps 1A and 1C running as high-pressure injection pumps. The makeup valves opened to admit the full, 1000 gpm, output of the pumps into the reactor coolant system. The pressurizer water level was increasing rapidly as shown in Figure 2.4-4. In part this was due to high pressure injection (HPI), but expansion due to vapor formation in the reactor coolant was also contributing to the pressurizer level increase.

The operators had been trained to avoid filling the pressurizer and causing the primary system to go "water solid." With the primary system full of liquid a very small temperature increase could cause the pressure to rise to the point where the safety valves would open. It is not unusual for safety valves to leak after they lift, thereby necessitating costly repairs. Procedures for a turbine trip, which the operators were attempting to follow, require the operators to switch to manual control and reduce makeup flow as soon as the pressurizer regains normal level.

At 3 min 13 s, after verifying that all of the emergency core cooling systems had started normally, the operators bypassed the high pressure injection system. Bypassing the system did not shut it down but merely permitted the operators to control high pressure injection flow manually. At 4 min 38 s, to avoid overfilling the pressurizer, the operators shut off makeup pump 1C, severely throttled HPI flow from makeup pump 1A, and initiated letdown flow in excess of 160 gpm. After a brief pause, the pressurizer level continued to increase due to thermal expansion of the reactor coolant. The coolant supplied by HPI was less than the amount being lost through the PORV. The stage was set for a severe accident unless the loss of coolant was diagnosed and corrected.

Figure 2.4-5 depicts the reactor coolant system condition at 8 min. Reactor coolant pressure had decreased to 1500 psig. Saturated reactor coolant was being pumped through both loops by all four reactor coolant pumps. The pressurizer was full, and the steam generators were dry.

2.4.4.4 Release Pathways

Because of the discharge of reactor coolant through the open PORV, the pressure in the reactor coolant drain tank increased rapidly. While the tank was being pressurized, some reactor coolant was forced through the vent line into the vent gas header. This damaged portions of the vent gas system creating paths by which radioactive gases would eventually leak to the auxiliary and fuel handling buildings.

The reactor coolant drain tank relief valve began opening intermittently at 3 min 12 s. Reactor coolant then began accumulating in the reactor building sumps. At 7 min 29 s, a reactor building sump pump started automatically. A second reactor building sump pump came on at 10 min 19 s. The sump pumps' discharge was aligned to the auxiliary building sump tank, which had a blown rupture disk. Water, therefore, spilled onto the auxiliary building floor.

The two reactor building sump pumps were turned off at about 38 min when an auxiliary operator noticed that they were on and that the reactor building sump level was at its high limit (6 feet). Approximately 8,260 gallons of water were pumped from the reactor building sump to the auxiliary building before the sump pumps were turned off.

Reactor building (containment) isolation would have prevented the transfer of water from the reactor building sump to the auxiliary building. However, the rate of coolant loss associated with the stuck open PORV was not sufficient too cause the 4 psig reactor building pressure required for automatic isolation. When the reactor coolant drain tank rupture disk blew at 14 min 48 s, there was a 1 psig pressure spike in the reactor building, but the 4 psig set point for reactor building (containment) isolation was not approached until about 60 min (1 h).

The pathway for releases from the auxiliary building is depicted in Figure 2.4-6. The water initially pumped to the auxiliary building by the reactor building sump pumps contained low radionuclide concentrations characteristic of reactor coolant during normal operation. As the accident progressed, however, fission products escaped from a damaged core, and some were entrained in letdown flow to the makeup tank. The letdown line was, in fact, the major path for transporting radionuclides from the reactor building. There was some liquid leakage from the makeup and purification system to the auxiliary building floor. But the main pathway for radionuclide releases occurred during venting of the makeup tank to the damaged vent header. This venting began over 24 h after accident initiation, and resulted in the leakage of volatile radionuclides to the auxiliary and fuel handling buildings. Gases from these buildings are picked up by the ventilation system, passed through filters, and discharged through the stack. The filters remove chemically active species like iodine, but have no effect on inert noble gases.

2.4.4.5 Auxiliary Feedwater Restored

As discussed earlier, about 30 s after turbine trip, the conditions required for admission of auxiliary feedwater to the steam generators had been met. But, because the auxiliary feedwater block valves were closed, no water flowed to the steam generators. It appeared to the operators that the automatic valves were opening at an unusually slow rate, causing a delay in feeding the steam generators.

About 8 min after turbine trip an operator noticed steam generator level at 10 inches on the startup range. This indicated the steam generators were dry. The fact that the auxiliary feedwater block valves were shut was diagnosed, and these valves were opened resulting in dry steam generators being fed with relatively cool water. Auxiliary feedwater sprayed directly onto the hot tubes evaporated immediately. This caused a rapid increase in steam pressure, which had previously dropped when the steam generators boiled dry. This positive indication of feed flow to generators was confirmed by a decrease in the auxiliary feedwater pump discharge pressure and by hammering and crackling of the vibration and loose-parts monitor speaker, set up to listen to the steam generator. Hot and cold leg temperatures dropped as did the reactor coolant pressure. Although evaporation of auxiliary feedwater increased the steam pressure, no water collected in the bottom until the tubes cooled down. There was about a 14 min lag in recovery of steam generator level.

2.4.4.6 Undiagnosed LOCA Continues

At the beginning of the accident, the computer alarm printout was synchronized with real time. The alarm printer could only type one line every 4 s, however, and during the accident, several alarms per second were occurring. Within a few minutes, the alarms being printed were for events that had occurred several minutes earlier.

At about 15 min, reactor coolant pump alarms started going off. This indicated insufficient pressure at the pump inlets. There was also a continual slow reduction in reactor coolant pump flow, and low flow alarms sounded at various times.

Pressure at the reactor coolant pump inlets is required to be significantly above the saturation pressure. This requirement is called the net positive suction head (NPSH) requirement. If this NPSH requirement is not met, the formation of vapor bubbles on the suction side causes pump cavitation. Associated vibration could damage the pump seals or even the attached piping.

Operators ignored the NPSH requirement and let the reactor coolant pumps continue to operate. As long as the reactor coolant pumps provided forced circulation, even of froth, the core was cooled.

At ~20 min, the steam bubbles in the reactor coolant caused the out-of-core source-range neutron detector to read higher than expected. Normally, water in the downcomer annulus, outside the core but inside the reactor vessel, shields these detectors. But, because the water was now frothy, it was not shielding the detectors as well as usual. Not realizing that the apparent increase in neutrons reaching the detectors was caused by steam bubbles in the reactor coolant, the operators feared the possibility of a reactor restart. Although it is now known that their fears were unfounded, at the time they were one more source of distraction.

About 25 min after turbine trip, the operators received a computer printout that indicated the PORV outlet temperature was high, 285°F. This indication of an open PORV, however, was not interpreted as such by the operators. When the PORV opened in the initial transient, the PORV outlet temperature would have increased even if the PORV had closed as designed. The operators supposed that the abnormally slow cooling of the outlet pipe was caused by the pre-existing PORV or safety valve leak. Evidence of the open PORV now included: (a) the low reactor coolant pressure; (b) the rapid rise in reactor coolant drain tank pressure and temperature; (c) the fact that the rupture disk had blown; (d) the rise in reactor building sump level (with operation of the sump pumps); and e) the continuing high PORV outlet temperature. Nevertheless, the ongoing LOCA was not diagnosed.

The reactor coolant voids and the low reactor coolant pump flows decreased the efficiency of primary to secondary heat transfer in the steam generators. The rate of boiling on the secondary side was low, and operators found it difficult to keep the secondary water level from creeping up. One auxiliary feedwater pump was shut off at 36 min.

As control room personnel struggled to understand what was happening in the plant, hundreds of alarms went off, signaling such things as unusual conditions in the reactor coolant drain tank, high temperature and pressure in the reactor building, and low reactor coolant pressure. Conditions were beyond those that control room personnel had experienced in their training or in their operation of the plant. The symptoms described in the emergency procedures did not fit the situation and proved to be of little help. The operators were well aware that something was wrong, and, about one hour after turbine trip, they called the on-call operating engineer to the site.

The condition in the reactor coolant system at 60 min (1 h) is depicted in Figure 2.4-7. The PORV was still open, and the reactor coolant pressure had decreased to 1050 psig. Unknown to the operators the reactor coolant was a saturated liquid-steam mixture. A large steam bubble had probably formed in the upper reactor vessel head. Pressurizer level was high and was only barely being held down. The reactor coolant pumps were operating but with decreasing flow and increasing vibration. Heat removal via the steam generators was ineffective. To add to the confusion, the condenser was no longer available, the alarm computer lagged so badly that it was virtually useless, radiation alarms were beginning to come on, and the reactor building pressure and temperature were gradually increasing.

2.4.4.7 Loop B Pumps Turned Off

At ~74 min, the operators shut down reactor coolant pump 1B. A few seconds later reactor coolant pump 2B was shut down. (Pressurizer spray comes from the A loop.) The action to shut down the loop B reactor coolant pumps was taken because reactor coolant pump performance was seriously impaired as indicated by high vibration, low flow (60 percent of normal), low amperage, and inability to meet NPSH requirements.

Shutting down the two B loop reactor coolant pumps reduced the flow of coolant through the reactor core. There was still enough mass flow in the steam-water mixture being pumped by the two loop A pumps to keep the core from overheating. The open PORV was, however, still reducing the reactor coolant inventory and pressure. The remaining liquid reactor coolant continued to vaporize, and, although this vaporization removed core decay heat, it further impeded forced circulation via the loop A reactor coolant pumps.

A sample of reactor coolant analyzed a few minutes after the loop B pumps were shut off indicated a low boron concentration. This finding, coupled with apparently increasing neutron levels, increased the operators' fears of a reactor restart. As explained earlier, the source range neutron detector count rate was increasing because steam bubbles in the downcomer allowed more neutrons to reach the detector. There was no actual danger of re-criticality. It is now believed the sample was diluted by condensed steam, causing the indication of low boron concentration.

At 80 min, an operator had the computer print out the PORV (283 °F) and pressurizer safety valve (211°F and 219°F) outlet temperatures. Because there had been essentially no change in these temperatures, the operators should have realized that the PORV had not closed. At about the same time, the letdown line radiation monitor indicated a sevenfold increase. The letdown line radiation monitor was notoriously sensitive, but the implications of the reading were not understood by the operators.

At 87 min (1 h 27 min), steam generator B was isolated. Operators observed increases in reactor building pressure and noted that the secondary pressure in steam generator B was 300 psi lower than in generator A. They believed that secondary steam was leaking from generator B into the reactor building. In hindsight, the lower pressure in generator B was caused by reduced heat transfer in loop B after reactor coolant pumps 1B and 2B were shut off.

Figure 2.4-8 depicts the condition in the reactor coolant system at 90 min (1 h 30 min). The reactor coolant pressure was 1050 psig. The pressurizer was nearly full. The loop B reactor coolant pumps were off, the B steam generator was isolated, and the steam and liquid phases had separated in loop B. The reactor coolant pumps in loop A were still on, circulating the steam-water mixture through steam generator A.

2.4.5 Initial Core Damage (101 min to 174 min)

2.4.5.1 Loop A Pumps Off, Core Uncovered

Approximately 5 to 10 min after the loop B reactor coolant pumps were shut off, the loose-parts monitor again indicated increasing pump vibration. In f[illegible] standing in the control room, the operators said they could feel the vibrations. The operators also reported flow instability, as the loop A flow continued to decrease. At ~101 min (1 hr 40 min 40 s), the loop-A reactor coolant pumps were turned off. This action sealed the fate of TMI-2.

The operators asserted during interviews that they were concerned about a inducing a LOCA by a reactor coolant pump seal failure, and decided to go on natural circulation. To establish natural circulation would have required (among other things) subcooled reactor coolant. The operators assumed that, because the pressurizer level was high, the core must be covered. In actuality, natural circulation was precluded by the steam that had formed in the reactor coolant system. It was the higher pressure of steam bubbles formed in the reactor vessel that kept the water level high in the pressurizer. After shutting off the loop A pumps, the operators did not see any indications that natural circulation had been established.

After shutdown of the last two reactor coolant pumps, vapor that had previously been mixed with liquid to form a frothy reactor coolant, separated and rose to the higher portions of the reactor vessel and the rest of the reactor coolant system. Water continued to escape from the stuck-open PORV and HPI flow remained throttled. By 103 min (1 h 42 min 30 s), the separation of steam and liquid phases in the reactor vessel had again reduced the shielding of the source-range neutron detectors, which indicated increasing neutron levels. The operators increased high pressure injection flow to avert a restart by providing emergency boration. Reactor coolant pressure increased, and the neutron count rate dropped significantly.

For at least a few minutes after the loop A reactor coolant pumps were shut off, it would have been possible to terminate the accident without extensive core damage. If full HPI flow had been initiated, the reactor coolant system could have been refilled. The block valve upstream of the PORV could have been shut to repressurize the system and collapse the vapor bubbles. These actions would have permitted sustained core cooling by forced (reactor coolant pump) or natural circulation, but the actions were not taken.

2.4.5.2 Hydrogen from Zircaloy Oxidation

Figure 2.4-9 depicts the situation at 120 min (2 h). The reactor coolant pressure was about 750 psig. The PORV was still open, HPI flow was still throttled, and all reactor coolant pumps were off. There was essentially no flow through the core, and the liquid and vapor in both loops had separated. With this separation, the hot-leg temperature became much higher than the cold-leg temperature. The actual loop A hot-leg temperature was 558°F. In retrospect, this indicated the presence of superheated steam in the hot leg. For superheated steam to exist in the hot leg, a substantial portion of the upper part of the core must be uncovered.

It is now known that the water level in the core region continued to fall until the top two-thirds of the core uncovered and became very hot. Steam generated by the boiling of water covering the bottom portion of the core flowed upward and oxidized the hot Zircaloy fuel cladding releasing additional energy and large amounts of hydrogen.

As long as the upper part of the reactor coolant system contained only steam, the bubble could have been condensed (collapsed) by refilling (with full HPI) and repressurizing (by closing the PORV block valve) the system. However, with large amounts of noncondensible hydrogen in the system, the bubble could no longer be collapsed.

At about 120 min (2 h), a conference phone call began between the control-room technical superintendent and (at their homes) the station superintendent, the vice president of generation, and the Babcock & Wilcox site representative. The conference call lasted 38 min. Conferees realized that something was abnormal since the reactor coolant pumps were off yet they were unable to get a steam bubble in the pressurizer. The blown out rupture disk on the reactor coolant drain tank and the water on the reactor building floor did not seem surprising, since this had happened before. The condition of the block valve upstream of the PORV was questioned. It was reported to be shut, but it was not. The conferees decided to restart a reactor coolant pump, and all officials planned to report to the control room.

At ~134 min (2 h 14 min), the reactor building air sample particulate radiation monitor went off scale. This was the first of many radiation alarms that could definitely be attributed to gross fuel damage.

2.4.5.3 PORV Block Valve Closed

At 139 min (2 h 19 min), a shift supervisor who had just come into the control room isolated the PORV by closing the upstream block valve. Apparently, he did this to see whether it would have an effect on the anomaly of high pressurizer level and low steam pressure. Noting that the downstream temperature for the PORV was 35°F higher than for the safety valves, it was recognized that a leak had been stopped. The operators also noted an immediate drop in reactor building temperature and pressure. With closure of the block valve, reactor coolant pressure began to increase from a low of 660 psig until it reached 1300 psig about 3 hours later.

Core degradation continued after the PORV block valve was closed because there was still no way to cool the uncovered portion of the core. Although steam generator A contained 50% cold water, there was no circulation of reactor coolant through the steam generators. In some ways the situation was worse than before the PORV was closed. As the reactor coolant pressure increased, it took less energy to evaporate each pound of residual water covering the bottom portion of the core.

2.4.5.4 Initial Melting In Core Region

Post-accident analyses of plant data and core debris indicate that by 140 min (2 h 20 m) the core liquid level had dropped to about midcore. The upper regions of the core had heated sufficiently (1500°F to 1700°F) to result in cladding failure and release of gaseous fission products.

At about 149 min (2 h 29 min), the narrow range hot-leg temperature went offscale high (620°F). The narrow range cold-leg temperature was already offscale low (520°F). Wide range temperature measurements were still available, but the operators were in the habit of using the narrow range temperatures, which can be read more precisely. One meter, which indicates the average of the hot-leg and cold-leg temperatures, read 570°F (the average of the constant readings of 620°F and 520°F). This steady average temperature evidently convinced the operators that the situation was static.

Between 150 and 160 min, temperatures got high enough to cause melting and downward relocation of some core materials, which refroze on colder surfaces to begin the formation of a crust that would subsequently act like a crucible holding molten material in the core region.

At 158 min (2 h 38 min) a letdown cooler radiation monitor went off-scale high, reflecting the severe core damage that was occurring.

During the period of core damage, there was virtually no information on conditions in the core. Incore thermocouples, which measure reactor coolant temperature at the exit from the core, could only show temperatures as high as 700°F due to limits imposed by the signal conditioning and data logging equipment, not by the thermocouples themselves.

Figure 2.4-10 shows the conditions in the reactor coolant system at 158 min (2 h 48 min). The PORV block valve was shut, and the reactor coolant pressure had increased to 1200 psig. Upper portions of the reactor coolant system were filled with the steam-hydrogen mixture. The Zircaloy oxidation continued, and some melting and relocation of core materials was indicated.

2.4.6 Quenching and Related Core Damage (174 min to 375 min)

2.4.6.1 Restart of Reactor Coolant Pump 2B

At 174 min (2 h 54 min) the operators restarted reactor coolant pump 2B. Flow was indicated for a few seconds and then dropped to zero. The pump was shut off 19 min later. The core was partially quenched as liquid remaining in the cold leg was pumped into the core. This probably caused some collapse of rubble in the core region. With the block valve closed, the steam generated during the partial quench caused the reactor coolant pressure to increase to 2200 psig.

At 176 min (2 h 56 min), a technician reported that letdown sample lines had an extremely high radiation level (600 R/hr). A radiation level of 1 R/hr had previously (2 h 30 min) been reported in the makeup tank area of the auxiliary building. The auxiliary building was evacuated, and a site emergency was declared.

The conditions in the reactor coolant system 180 min (3 h) into accident, are depicted in Figure 2.4-11. The reactor coolant pressure was at 2050 psig. Reactor coolant pump 2B was on, but no flow was indicated. The pressurizer level was offscale high. Most incore thermocouples were reading off scale. The actual hot-leg temperatures were nearly 800°F. This indicates that at least the upper part of the core was dry. There were many high radiation alarms, indicating that extensive fuel damage had occurred. Fifty to sixty people were in the control room by this time, attempting to resolve the crisis.

2.4.6.2 Core Region Reflooded

At 192 min (3 h 12 min) the PORV block valve was reopened in an attempt to control reactor coolant pressure. Opening the valve resulted in an increase in the valve outlet temperature, a limited pressure spike in the reactor coolant drain tank (rupture disk had previously burst at ~15 min), an increase in reactor building pressure, and pathway by which hydrogen radionuclides from the damaged core could reach the reactor building.

After the PORV block valve was opened, the reactor coolant pressure began dropping rapidly. In response, at 200 min (3 h 20 min), engineered safeguards were manually initiated. Makeup pump 1C started and the makeup valves fully opened. Reactor coolant temperature dropped rapidly as cold water was injected into the reactor vessel. The out-of-core neutron levels dropped rapidly due to the rapid water level increase in the downcomer. The water added was sufficient to ensure that the core region was recovered.

The sudden injection of cold water onto the hot core materials caused additional releases of volatile radionuclides due to thermal shock. These radionuclides could then flow out letdown line to the auxiliary building or through the open PORV block valve into reactor building. The radiation level in the reactor building dome increased to 8 R/hr. The vent stack alarm also went off at about this time. Many other radiation monitors registered alarms. The control building, except for the control room itself, was evacuated.

At 203 min (3 h 23 min 23 s, 7:24 am), a general emergency was declared on the basis of the many radiation alarms, and the potential for offsite releases of radionuclides. The utility notified State and Federal officials when it declared the site and general emergencies.

At ~209 min (3 h 29 min) a borated water storage tank alarm was received. Water for high pressure injection is taken from the borated water storage tank. There were still 53 feet of water in this tank. Nevertheless, the fact that the level was falling caused concern that continued high pressure injection would exhaust the borated water storage tank inventory. Highly radioactive water from the reactor building sump would then have to be used for high pressure injection. The makeup pumps and associated pipes and valves in the auxiliary building would then have become contaminated with radionuclides. This could cause grave problems if repairs became necessary. There was, therefore, an inclination to use as little HPI flow as possible. Emergency safeguards were reset, and makeup pump 1C was stopped. At the same time, the PORV block valve was shut. Closing this valve, with makeup pump 1A still running, caused a rapid increase in pressurizer level.

The condition in the reactor coolant system at 210 min (3 h 30 min) is depicted in Figure 2.4-12. The opening of the block valve for 17 min together with the operator-initiated increase in HPI flow had reduced the reactor coolant pressure to 1500 psig. The vessel had been refilled and the core recovered. Temperatures in the reactor coolant system were decreasing, but steam and hydrogen gas was trapped in the hotlegs, blocking circulation of water through the system. Most of the damage to the core had been done, and radiation levels in the plant were high.

2.4.6.3 Pour of Molten Core Material

At about 222 min (3 h 42 min) the PORV block valve was reopened for the second time. It remained open until 315 min (5 h 15 min).

At about 224 min (3 h 44 min), it is now known that approximately 20 tonnes of molten core material poured from the core region into the reactor vessel lower head. A rapid increase in reactor coolant pressure between 224 and 226 min indicates substantial quenching of relocated material by water in the lower head. The phenomena associated with the formation, holdup, and relocation of molten core materials is discussed in Chapter 3.

2.4.6.4 HPI On, Off, Finally Sustained

At 236 min (3 h 56 min), engineered safety features actuated on high (4 psig) reactor building pressure. Makeup pump 1C started.

Both makeup pumps (1A and 1C) tripped at 258 min (4 h 18 min). Two unsuccessful attempts were made to restart pump 1A. The control switch was then put in the "pull-to-lock" position. This completely defeated automatic starts of the pump. The pressurizer indicated full, and the operators were concerned about full high pressure injection flow coming on with an apparently solid primary system. Actually, a very large part of the reactor coolant system was filled with steam and hydrogen gas, and the system was far from being water solid. This condition could have been recognized from the fact that the temperatures in the hot legs were consistent with superheated steam.

By 266 min (4 h 26 min) high pressure injection was reestablished. From this time on, high pressure injection flow was continuously maintained at varying flow rates after having been shut off altogether for at least 5 min.

Between 4 h and 4 h 30 min, incore thermocouple temperature readings were taken off the computer. Many registered question marks. Shortly after, at the request of the station superintendent, an instrumentation control engineer had several foremen and instrument technicians go to a room below the control room and take readings with a millivoltmeter on the wires from the thermocouples. The first few readings ranged from about 200°F to 2300°F. These were the only readings reported by the instrumentation control engineer to the station superintendent. Both later testified that they discounted or did not believe the accuracy of the high readings because they firmly believed the low readings to be inaccurate. In the meantime, the technicians read the rest of the thermocouples. Their readings, a number of which were above 2000°F, were entered in a computer book, which was later placed on a control room console. The technicians subsequently left the area when nonessential personnel were evacuated.

Only a small amount of heat could be removed by the unisolated A steam generator because the upper part of the primary system was filled by a mixture of steam and hydrogen gas. The water level on the secondary side was rising because more auxiliary feedwater was coming than was leaving as steam. At 4 h 42 min, auxiliary feedwater was shut off.

2.4.7 Recovery Attempts (5 h 15 min to 1 month)

For the rest of the day, control room personnel struggled to regain stability in the plant. The principal problem was to ensure a reliable flow of water through the core.

2.4.7.1 Attempt to Collapse Vapor Bubble

The operators first tried to repressurize in order to collapse what they believed to be saturated steam bubbles in the reactor coolant system and establish natural circulation.

At 5 h 15 min, the PORV block valve was closed to initiate the repressurization. Two makeup pumps were running throughout the repressurization so that a feed and bleed situation existed. By 5 h 43 min, the primary system was fully repressurized. The pressure was maintained between 2000 and 2200 psig by cycling the PORV block valve.

Figure 2.4-13 shows the reactor coolant system condition at 6 h. Liquid was being released intermittently through the PORV block valve. Two makeup pumps (HPI pumps) were running, and core heat removal was by heatup of the injected water. Steam generator heat transfer was blocked by hydrogen.

In order to encourage natural circulation, operators raised the water level of steam generator A to 90%, using the condensate pump for feed. It became clear that even with a full steam generator and high pressure, natural circulation was not being established.

At 6 h 10 min, airborne radiation levels in the Unit 2 control room required evacuation of all but essential personnel. At 6 h 17 min, Unit 2 personnel put on masks to protect them against possible airborne radionuclides. At 6 h 27 min, nonessential personnel began moving to the Unit 1 control room. At 6 h 52 min, people leaving the Unit 2 control room failed to close the door properly, possibly compromising the recirculation ventilation system.

By 7 h, communications in Unit 2 control room were hampered by respirators. Some personnel removed their respirators for short periods.

The operators were reluctant to start a reactor coolant pump for fear of vibration-induced seal failure LOCA. They recognized they had bubbles in both loops. They believed the reactor core was covered and considered the possibility of uncovering it as each option was reviewed. The concern that the PORV should remain closed was reevaluated leading to a decision to use the PORV block valve for pressure reductions.

2.4.7.2 Attempt to Use Core Flood Tanks

With the failure of repressurization to collapse the bubble, concern arose over whether the core was covered and how long the borated water storage tank inventory would last. These uncertainties led to the next strategy, which was to depressurize the primary system sufficiently to inject water from the core flood tanks. Nitrogen gas maintained the pressure on the water in the core flood tanks slightly above 600 psig. Utility personnel reasoned that lower pressure would activate the core flood tanks, which would dump more water onto the core, assuring that it would be covered. Actually, if the reactor coolant pressure drops only slightly below 600 psig (as happened at TMI-2) only a small amount of water is injected before the core flood tank pressure equilibrates with that in the primary system. An amount of water approaching the full volume of the tanks would only be injected into the reactor vessel if the reactor coolant pressure dropped far below 600 psig, as in a large break LOCA.

At 11:38 a.m. (7 h 38 min), the PORV block valve was opened, allowing steam and gas once again to escape from the pressurizer. The reactor building pressure increased from 0.2 psig to 2.5 psig during this reactor coolant system depressurization.

Figure 2.4-14 shows the condition in the reactor coolant system at 8 h. The reactor coolant pressure had been reduced to about 1000 psig. During depressurization, hydrogen was released through the PORV into the reactor building.

At 8 h 41 min, the reactor coolant pressure reached 600 psig, and the core flood check valves opened. Little water was injected from the core flood tanks into the reactor vessel. Some control room personnel interpreted this to mean the core was covered; others concluded that the core had never been uncovered. At 9 h 10 min, plant personnel closed the PORV block valve, halting the depressurization.

2.4.7.3 Attempt to Use Decay Heat Removal, Hydrogen Burn

Members of the emergency command team soon decided to depressurize again in the hope of reaching a low enough pressure to permit use of the decay heat removal system.

At 9 h 50 min, operators again opened the PORV block valve. As the block valve was opened, there was an extremely sharp increase in reactor building pressure and temperature. As a result of the pressure spike, which is shown in Figure 2.4-15, the reactor building again isolated, engineered safeguards actuated, and the reactor building sprays came on. Figure 2.4-15 indicates a peak pressure of 28 psig, which is the setpoint for the actuation of reactor building sprays.

It is now known that the pressure spike occurred when hydrogen, which had been released while the PORV block valve was open, ignited and burned with oxygen in the reactor building atmosphere. Ignition apparently occurred simultaneously with the opening of the PORV block valve at 9 h 50 min. The reactor building sprays quickly brought the pressure and temperatures down. Six minutes after actuation, the sprays were shut off from the control room because there appeared to be no need for them.

Initially, the spike was dismissed as some type of instrument malfunction. Shortly afterward, however, at least some supervisors concluded that for several independent instruments to have been affected in the same way, there must have been a pressure pulse. It was not until late Thursday night, however, that control room personnel became generally aware of the pressure spike's meaning. Its meaning became common knowledge among the management early Friday morning.

Figure 2.4-16 shows the condition in the reactor coolant system at 10 h 30 min. Reactor coolant pressure had been reduced to about 400 psig, which was about the minimum achieved, and the pressurizer temperature had reached saturation. Liquid was maintained in the reactor coolant system during depressurization by continuous high pressure injection and some flow from the core flood tanks. The reactor coolant pressure never dropped below 320 psig or 250 °F, the pressure and temperature below which the decay heat removal system would have been allowed to operate. It is probably fortunate that the decay heat removal system could not be used. It was not designed to handle highly radioactive liquids, and failure of seals in the system could have resulted in leakage of such liquids directly to the auxiliary building.

At 11 h 8 min operators ended attempts to depressurize. Figure 2.4-17 shows the condition at 13 h. The system pressure was about 600 psig. Very little decay heat was being removed except by makeup water and by occasional opening of the PORV block valve. Gradual heatup was causing the reactor temperature and pressure to rise. Pressure control was being attempted by adjusting makeup flow and cycling the PORV block valve. Steam generator B was isolated. Hydrogen in the upper portions of the system was preventing any significant heat removal by steam generator A.

2.4.7.4 Forced Circulation Established

At 13 h 20 min, utility executives offsite ordered the emergency command team to repressurize the system again. The objective was to collapse enough steam to permit the restart of a loop A reactor coolant pump. This would establish forced circulation through the core and heat removal by steaming in loop A steam generator.

Figure 2.4-18 depicts the status of the reactor coolant system at 15 h (7 pm). The reactor coolant was repressurized to 2300 psig. Reactor coolant pumps are off, although steam generator A was steaming to the condenser providing some heat removal. Steam generator B was isolated. Natural circulation of reactor coolant through the steam generator was still blocked by the hydrogen gas at the top of the hot legs (the so-called candy canes).

There was some concern, as to whether a reactor coolant pump would operate under the conditions that existed. With voids in the reactor coolant, sustained running could damage the pump or blow out the seals. Therefore, the control room personnel decided to "bump" one of the pumps (run it for only a few seconds) and to observe current and flow while the pump was running.

The loss of two motor control centers (at the time of the hydrogen burn) meant that the ac oil lift pumps were out of service. It is not possible to start a reactor coolant pump unless the oil lift pump can be started. There is a standby dc oil lift pump, but it was necessary to send people to the auxiliary building to start it.

At 15 h 33 min, operators started reactor coolant pump 1A by manually bypassing some of the inhibiting circuitry. The pump was run for 10 s, with normal amperage and flow. Dramatic results were seen immediately. Reactor coolant pressure and temperature instantly dropped, but began to rise again as soon as the pump was stopped. Evidently, there was an immediate transfer of heat to the steam generator when the coolant circulated. There was also a rapid spike in the steam pressure and a drop in steam generator level.

At 15 h 50 min, based on their earlier success, the operators managed to start a pump 1A and keep it running. This forced water through the core region and steam generator A. By 16 h (8 pm) relatively stable conditions were achieved as depicted in Figure 2.4-19. Reactor coolant temperatures were at about 290°F. Pressurizer level was still full-scale. Reactor coolant pressure was about 1300 psig. Steam generator B was isolated and at about 97% water level. Makeup was normal. The pressurizer temperature was about 150°F, and operators were letting down in an attempt to remove the excess hydrogen.

2.4.7.5 Collapsing the Bubble

At 17 h 25 min (9:25 pm), the utility believed pressure could soon be reduced to a level at which the decay heat removal system could be used.

Apparently, no one at this time realized that a bubble still existed in the reactor coolant system. Starting of the reactor coolant pumps swept the remaining gas in the upper part of the system around with the water as discrete bubbles. The gas bubbles would tend to collect in the most quiescent part of the system - the upper head of the reactor vessel.

It is now known that the gas was largely hydrogen. Hydrogen is slightly soluble in water, and its solubility is greater at high pressure. An attempt to depressurize the system would cause some of the dissolved hydrogen to effervesce out of the water. As the pressure dropped, the bubble would grow in size and interfere with circulation of the reactor coolant.

In addition to growing in size, the bubble and the dissolved gas made it impossible to depressurize the reactor coolant system completely. Ordinarily, reactor coolant pressure is controlled by the size of the steam bubble in the upper part of the pressurizer. When this bubble contains only steam, spraying cold water into the top the pressurizer shrinks the bubble and reduces the pressure. When the bubble contains a gas like hydrogen, however, spraying does not reduce the size of the bubble as much, so there is less control over the pressure.

A related problem occurred in the letdown system. As explained, hydrogen gas comes out of solution when the pressure is reduced. The gas from the letdown water collected in the bleed tanks and makeup tank, increasing the pressure and making it necessary to vent the tanks often. The vented gas was not pure hydrogen; it contained small amounts of volatile radionuclides as well. There was limited space available for holding the gas released from the letdown flow. These two factors made the reduction of pressure an extremely slow process that took several days to accomplish.

Natural circulation in the reactor coolant system was finally established on April 27, almost a full month after the accident began.

2.4.8 Lessons Learned

As a result of the incident at TMI-2, many safety issues were identified and acted upon by members of the utility industry, plant design companies, operator training facilities, and regulatory committees. These actions led to improvements in the exchange of reactor safety information, control room instrumentation, the operator-machine interface, emergency plans, operator training, and distribution of regulatory authority. For a more complete discussion of the actions resulting from the TMI-2, see Section 1.4.

Table 2.4-1
Chronology of Major TMI-2 Accident Events

Elapsed Time h:min:s	Event or Condition
-0:00:01	Condensate pump 1A and condensate booster pumps trip.
0:00:00	Feedwater pumps trip, turbine trips.
0:00:03	PORV opens at 2255 psig.
0:00:08	Reactor trip (control rods dropped) at 2355 psig.
0:00:13	PORV failed to reclose at 2205 psig.
0:00:15	Indicated pressurizer level peaked at 256 inches and began a rapid decrease.
0:00:14	Auxiliary feedwater pumps achieved normal discharge pressure.
0:00:15	Steam generator levels indicate 74 inches (startup range).
0:00:30	PORV and pressurizer safety valve outlet temperatures alarmed high.
0:00:38	Steam generator A water level at 23.8 inches. Auxiliary feedwater valves open as level decreases below 30 inches and give dual indication on panel.
0:00:40	Steam generator B water level at 23.7 inches and decreasing.
0:00:41	Operator manually started one of the three makeup pumps (pump 1B).
0:00:54	Pressurizer level reached lowest level (158 inches) and started to rise.
≥0:01:00	NRC estimate of onset of steam void formation.
≥0:01:45	Steam generators A and B boiled dry.
0:02:01	High pressure injection initiated (1000 gpm) when reactor coolant pressure fell below 1600 psig setpoint.
0:03:12	Reactor coolant drain tank relief valve began opening intermittently.
0:03:13	Operators bypassed the high pressure injection system.
0:03:28	Pressurizer high level alarm.
0:04:38	Operator throttled high pressure injection isolation valves and stopped makeup pump 1C.
0:04:52	Second let-down cooler put in service to allow increased letdown.
0:05:00	Pressurizer level reached 377 inches and continued to rise.
0:05:15	An operator restarted condensate pump 1A.
>0:05:15	Operators tried to restart condensate booster pump 2B but it tripped.
0:05:30	Saturated conditions indicated. Indicated reactor coolant temperature (T_h=582°F) and pressure (1340 psig) reached saturation.
0:06:00	Pressurizer steam bubble lost.
0:07:29	Reactor building sump pump 2A started (140 gpm).

0:08:00	*Figure 2.4-5. Expansion/Saturation Due to LOFW/LOCA.*
0:08:18	Operator opened auxiliary feedwater block valves.
0:10:19	Second reactor building sump pump (2A) started.
0:10:48	High (5.65 ft) reactor building sump level alarm. Sump soon overflowed (6 ft).
0:11:43	Pressurizer level indication came back on scale and dropped rapidly (20 inches in 1 min) as reactor coolant loop temperatures continued to decrease from the heat being removed by the steam generators.
0:14:48	Reactor coolant drain tank rupture disk blows.
≥0:14:50	Reactor coolant pump alarms sound.
0:18:00	Waste exhaust monitors showed a small increases in radioactive iodine. Reactor building exhaust showed a tenfold increase in reading of radioactive emissions.
0:22:00	Abnormal out-of-core source-range neutron flux behavior.
0:24:58	PORV outlet temperature was 285.4°F. Safety valve outlet temperature was 270°F.
0:28:00	Operators have been dispatched to the auxiliary building to confirm pressurizer level indication and/or determine source of water that has filled pressurizer.
>0:30:00	Emergency diesel generators shut off.
~0:36:00	Auxiliary feedwater pump 2B turned off.
0:38:10	Reactor building sump pumps turned off.
~0:40:00	Increasing count rate continued on the source range neutron detector.
0:46:23	Letdown cooler monitor count rate began increasing. It would increase by a factor of 10 within the next 40 minutes.
~0:50:00	Operators called on-call operating engineer to the site.
1:00:00	*Figure 2.4-7. Reactor Coolant Voids Increasing.*
1:11:00	Operators initiate reactor building cooling.
1:13:40	Loop B reactor coolant pumps turned off. Loop A pumps kept on to retain pressurizer spray capability.
>1:14:00	Sample of reactor coolant indicates low boron concentration (700 ppm).
1:20:00	An operator had the computer print out the PORV (283 °F) and pressurizer safety valve (211 °F and 219°F) outlet temperatures.
1:27:00	Operators isolate steam generator B.
1:30:00	*Figure 2.4-8. Loop-B Stagnates After Pumps Shut Off.*
~1:30:00	Reactor coolant sample indicated 400-500 ppm boron and 4 μCi/ml.
1:40:40	Loop A reactor coolant pumps turned off.
1:42:30	Excore source-range detectors indicated increasing neutron flux levels. Emergency boration initiated.
1:51:00	Loop A and B hotleg (T_h) temperatures were increasing (eventually went off scale high - 620°F). Cold leg temperatures were decreasing.

2:00:00 *Figure 2.4-9. Further Voiding After Loop-A Pumps Shut Off.*

2:00:00 Conference call.

2:14:23 Reactor building air sample particulate radiation monitor went off scale.

2:18:00 Fifteen to twenty people in control room at this time.

2:19:00 PORV block valve closed, loss of coolant halted.

2:20:00 Vessel water level had dropped to about midcore.

2:29:00 Hotleg temperature indications passed the high end of the instrument scale, 620°F.

2:30:00 1 R/h reported in makeup tank area of auxiliary building.

2:38:23 Letdown cooler A radiation monitor went off-scale high.

2:39:23 Two samples indicated the boron concentration in the reactor coolant was 400 ppm. Emergency boration was started to avoid a reactor restart.

2:47:00 Alarm typewriter indication showed self-powered neutron detectors responding to high temperature down to 4' level of the core. 90% of the core exit thermocouples >700°F.

2:48:00 *Figure 2.4-10. Hydrogen Generation.*

2:50:00 Start of melting, downward relocation, and crust formation.

2:54:00 Reactor coolant pump 2B was restarted and operated for 17 min.

2:56:00 Site emergency declared.

2:57:00 Fifty to sixty people are in control room; attempting to resolve the crisis.

3:00:00 *Figure 2.4-11. Effects of Loop-B Pump Restart.*

3:12:00 PORV block valve opened to control reactor coolant pressure.

3:20:00 Engineered safeguards actuated, makeup pump 1C started, HPI flow increased.

3:21:00 Excore neutron instrumentation indicated a sharp decrease (reflood).
Reactor building dome radiation monitor read 8 R/h.

3:23:23 General emergency declared.

3:29:00 PORV block valve reclosed.

3:30:00 *Figure 2.4-12 Vessel Refilled.*

3:32:00 The makeup tank radiation level was at about 3 R/h, and the auxiliary building basement was reported flooded with airborne radioactivity. Spent-fuel demineralizer monitor read 250-900 mr/h. Source range monitor count rate shows increase by a factor of three.

3:37:00 Operators tripped makeup pump 1C.

3:42:00 PORV block valve again opened.

3:44:00 Molten pour.

3:55:39 Reactor building automatically isolated on high (>4 psig) pressure.
Makeup pump 1C started automatically.

>4:00:00 Over the next 90 minutes, core exit thermocouple readings were manually obtained ranging from 217 to 2580°F.

4:18:00	Makeup pumps 1A and 1C tripped. Operator attempted to restart pump 1A. Switch was then placed in "Pull to Lock."
4:20:00	Reactor building dome radiation monitor records 600 R/h.
4:22:00	Makeup pump 1B was started.
4:26:00	Sustained high pressure injection after this time.
~4:30:00	Condensate system completely shut down. Problems with the condensate system were continuing. The condenser had been steadily losing vacuum. It was necessary to maintain steam to the main turbine seals in order to operate the condenser at a vacuum. When main steam is not available, seal steam is provided by the oil-fired auxiliary boiler. The auxiliary boiler broke down, so that seal steam could not be maintained. It was, therefore, necessary to shut down the condensate system completely.
4:40:00	Reactor building dome radiation monitor records 1000 R/h.
4:42:00	Auxiliary feedwater was turned off. Only a small amount of heat could be removed by the steam generator because the upper part of the primary system was filled by a mixture of steam and hydrogen gas. The water level on the secondary side was rising because more auxiliary feedwater was coming than was leaving as steam. At 4 h 42 min, auxiliary feedwater was shut off.
~5:00:00	Reactor building dome radiation monitor reaches 6000 R/h.
5:15:00	Initial repressurization began, PORV block valve shut.
5:29:00	Emergency diesel fuel racks reset.
5:35:00	NRC Region 1 inspector reports no consideration of offsite evacuation, since utility reports no significant leakage, and there has been no significant off-site radioactivity yet.
5:43:00	By cycling the PORV block valve, reactor coolant pressure was maintained in the 1865-2150 psig range during the next 2 hours.
6:00:00	*Figure 2.4-13. Repressurized, Attempting to Collapse Vapor Bubble.*
6:04:00	Commenced filling steam generator A (to 97%) using condensate pumps.
6:10:00	Airborne radiation levels in Unit 2 control room require evacuation of all but essential personnel.
6:17:00	Unit 2 personnel put on masks to protect against possible radiation.
6:27:00	Everyone, except essential personnel, started moving to Unit 1 control room.
6:52:00	People leaving the Unit 2 control room fail to close the door properly, possibly compromising the recirculation ventilation system.
7:00:00	Communications in Unit 2 control room were hampered by respirators. Communications problems led some personnel to remove respirators for short periods.
7:00:00	A tour of the auxiliary building found 10 R/h at the radiation waste panel, water standing on the floor in areas with floor drains, and the auxiliary building sumps full.
7:08:00	Auxiliary feedwater pump 2A was started. Level in steam generator A reached 100% (operating range).
7:38:54	Depressurization initiated to actuate core flood system.
7:40:00	Region 1 inspector reports that utility believes there will be no radioactive release to the surrounding area.

8:00:00	*Figure 2.4-14. Depressurizing, Releasing H_2.*
8:30:00	The power-operated emergency main steam dump valve was closed at the request of corporate management.
8:41:00	Core flood tanks initiate, little flow.
9:04:00	Makeup pump 1C was shut off (concerned with borated water storage tank inventory).
9:10:00	Initial depressurization halted.
9:50:00	*Figure 2.4-15. Second Depressurization Initiated, Hydrogen Burn.* High pressure injection actuated. Reactor building sprays actuated.
9:50:30	Makeup pump 1C was stopped.
9:57:00	Reactor building spray pumps were stopped.
10:26:15	Loop A T_h<620°F. Stays on scale 10 minutes.
10:30:00	*Figure 2.4-16 Reactor Coolant Pressure Near Minimum (400 psig).*
11:06:00	Pressurizer level decreased to 180" in the next 18 minutes. Loop A temperature was increasing.
11:08:00	Second depressurization attempt ends.
13:00:00	*Figure 2.4-17. Steam Generators Blocked By Hydrogen.*
≥13:00:00	About 13 hours after turbine trip, the auxiliary boiler was brought back into operation. Steam for the turbine seals was now available and it was possible to hold a vacuum on the condenser. Two condenser vacuum pumps were started. It was the operator's belief that the main condenser would soon be available.
13:20:00	Repressurization began.
14:35:00	NRC Region 1 inspector reported that there still appeared to be a bubble in loop B.
15:00:00	*Figure 2.4-18. Repressurized, Flow Blocked by Hydrogen.*
15:33:00	Operator started reactor coolant pump 1A started, ran it for 10 s, then tripped it.
15:45:00	The station superintendent directed operators to start a reactor coolant pump.
15:50:00	Operator started reactor coolant pump 1A and let it run continuously.
16:00:00	*Figure 2.4-19. Forced Circulation Re-established.*

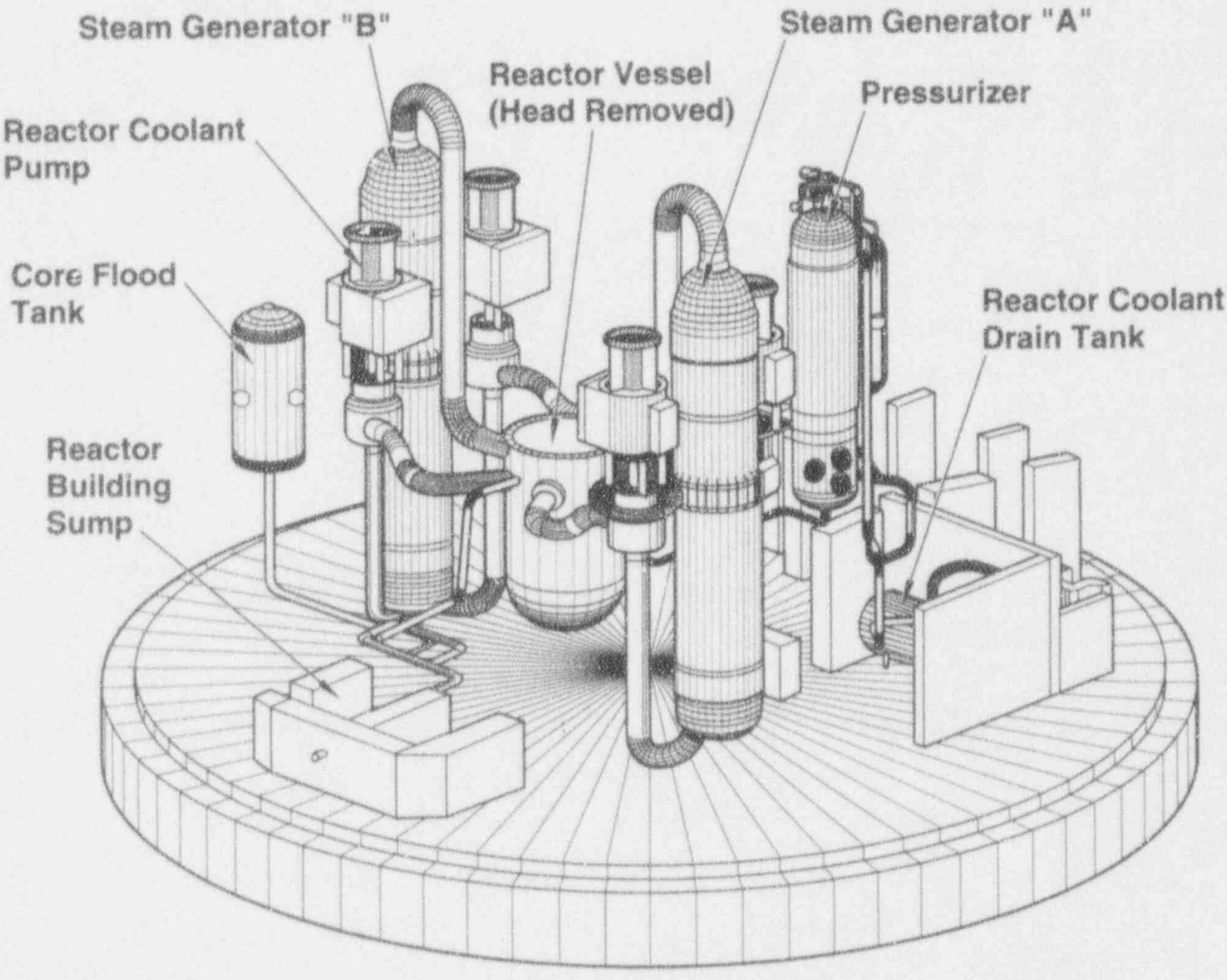


Figure 2.4-1 Arrangement of the primary reactor coolant system and related support system for the Three Mile Island, Unit 2 [TMI-2] Reactor. [Courtesy of R. Schauss and Construction Systems Associates.]

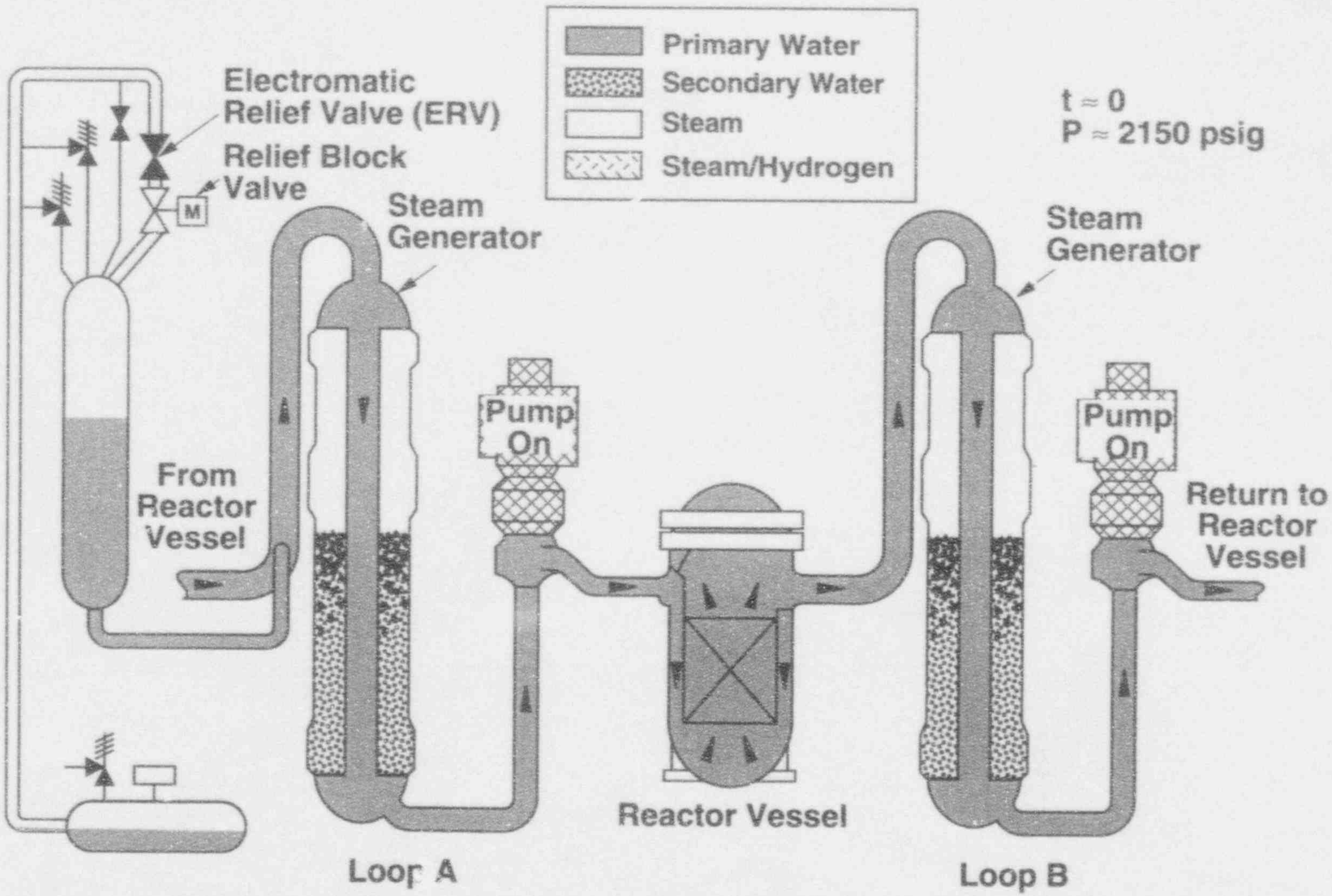


Figure 2.4-2 TMI-2 scenario: Initial condition - standby operation at 97% power.

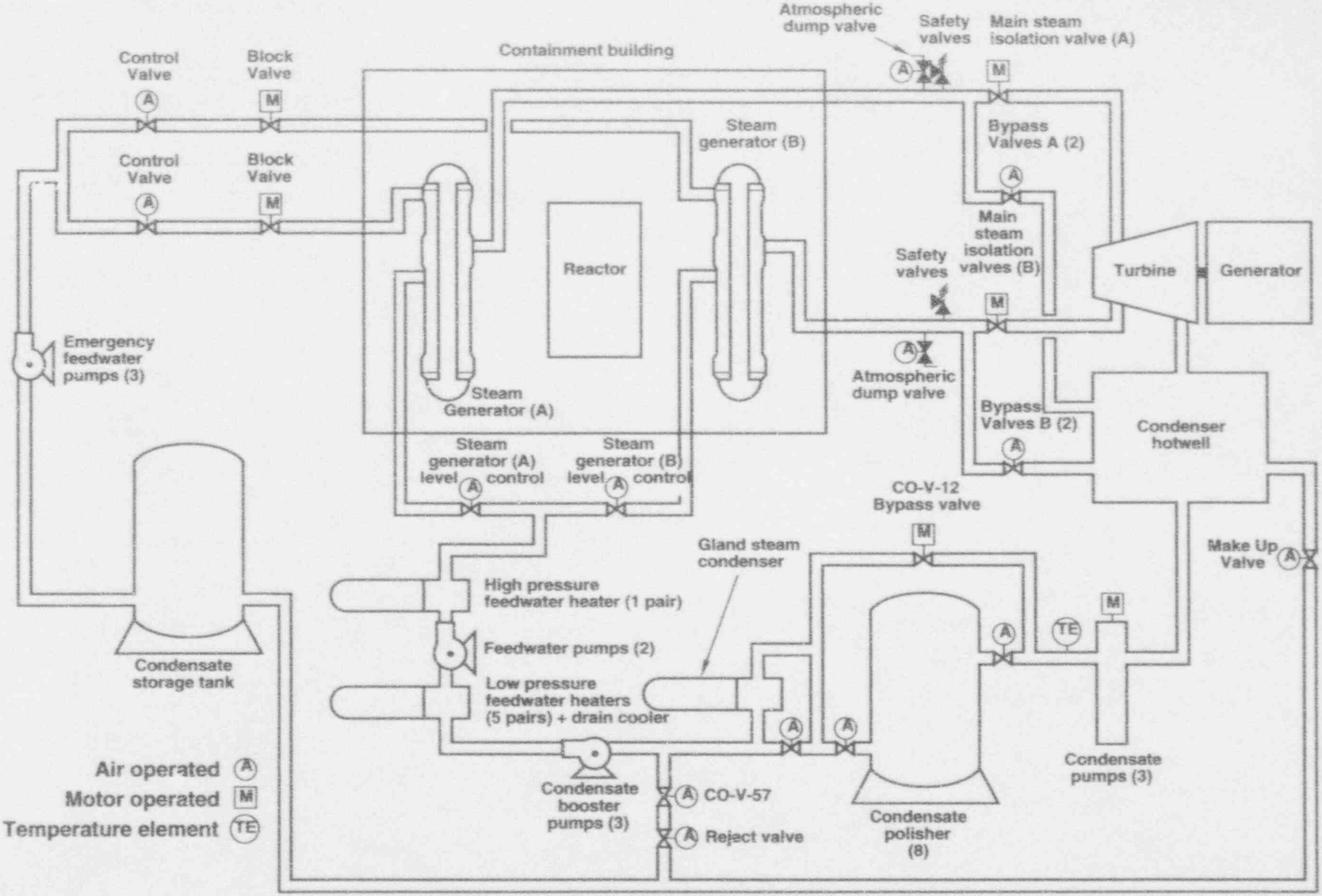


Figure 2.4-3 Condensate and Feedwater Systems.

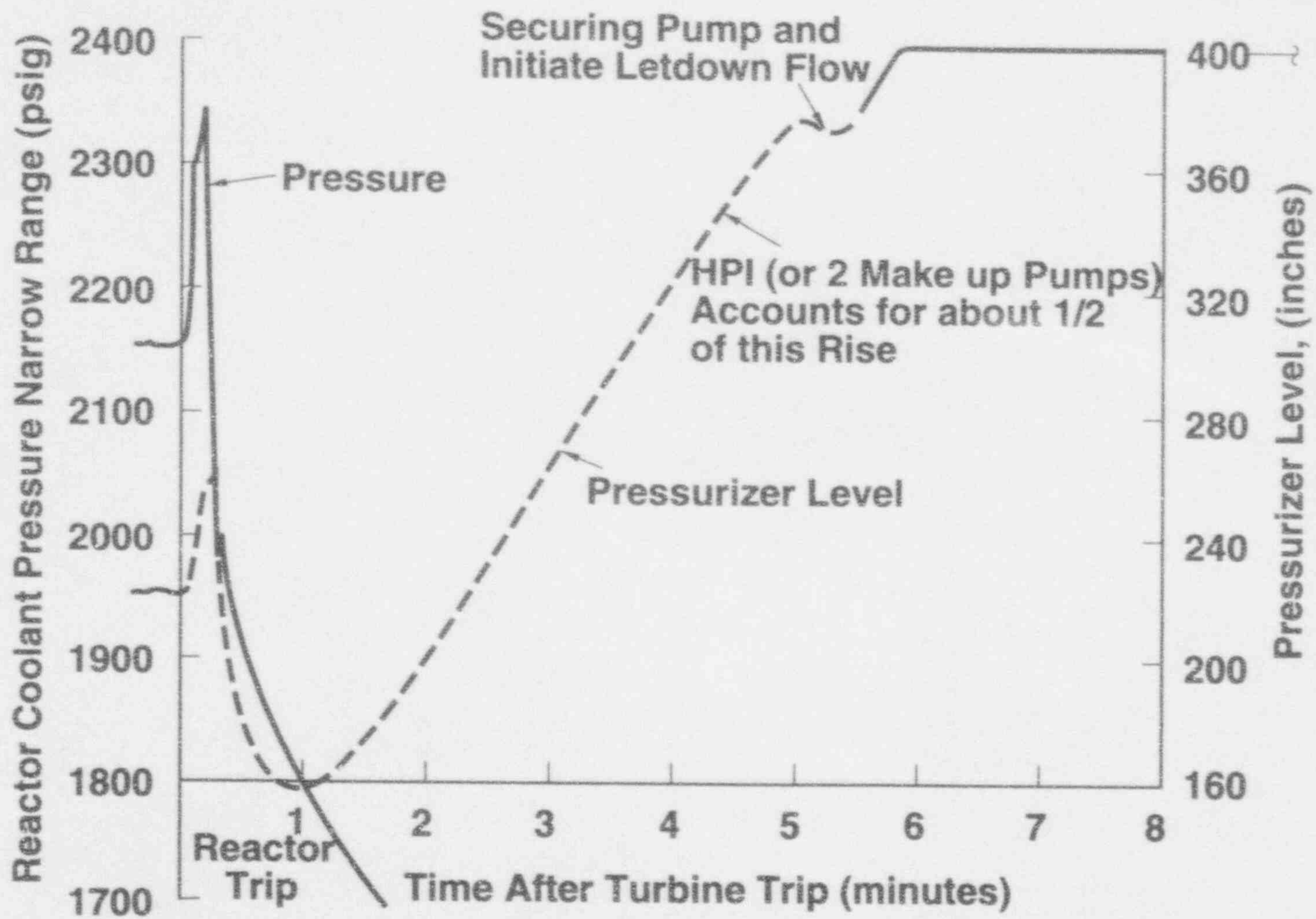


Figure 2.4-4 TMI-2 Scenario: reactor coolant pressure and pressurizer level vs. time

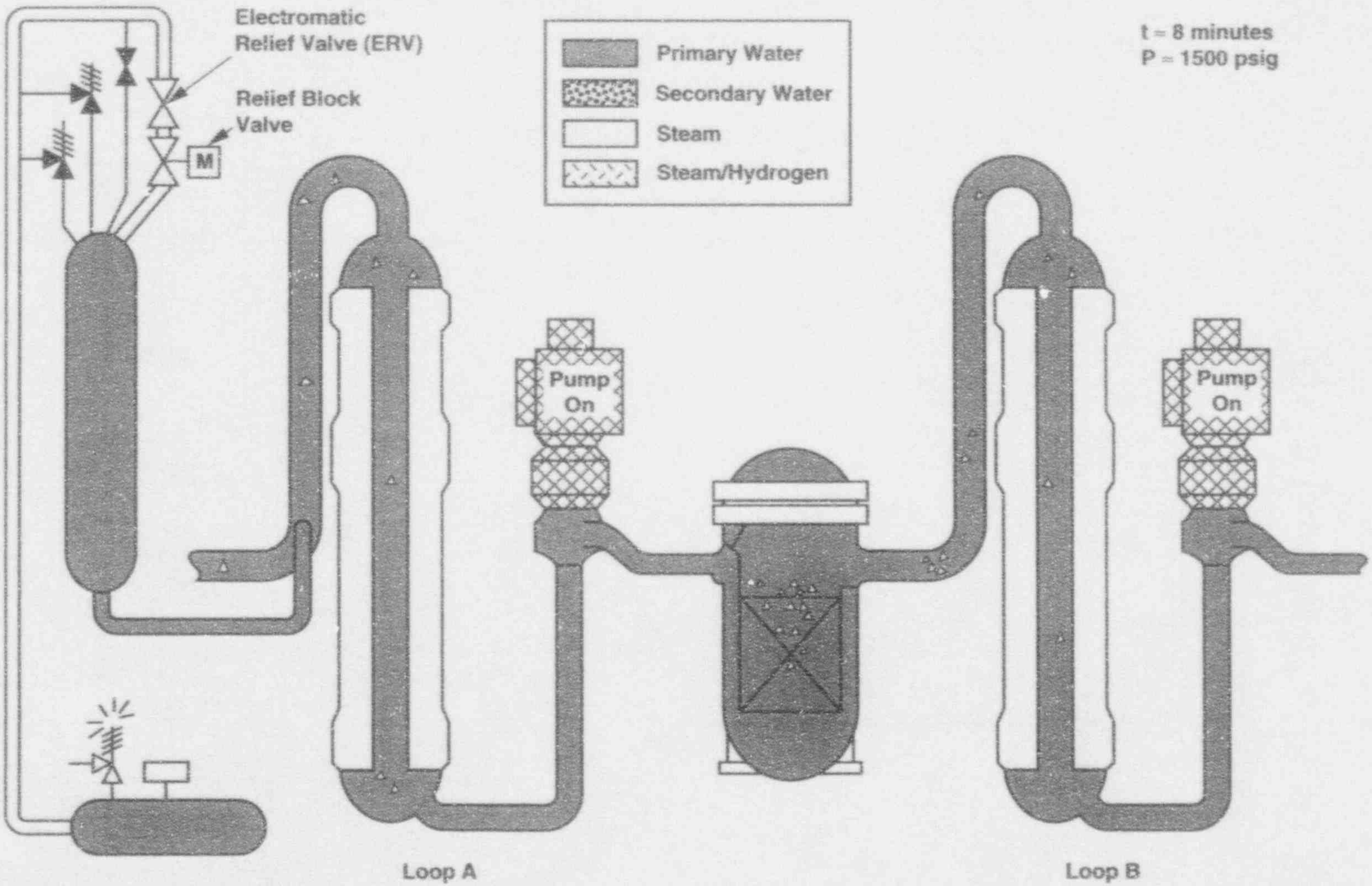
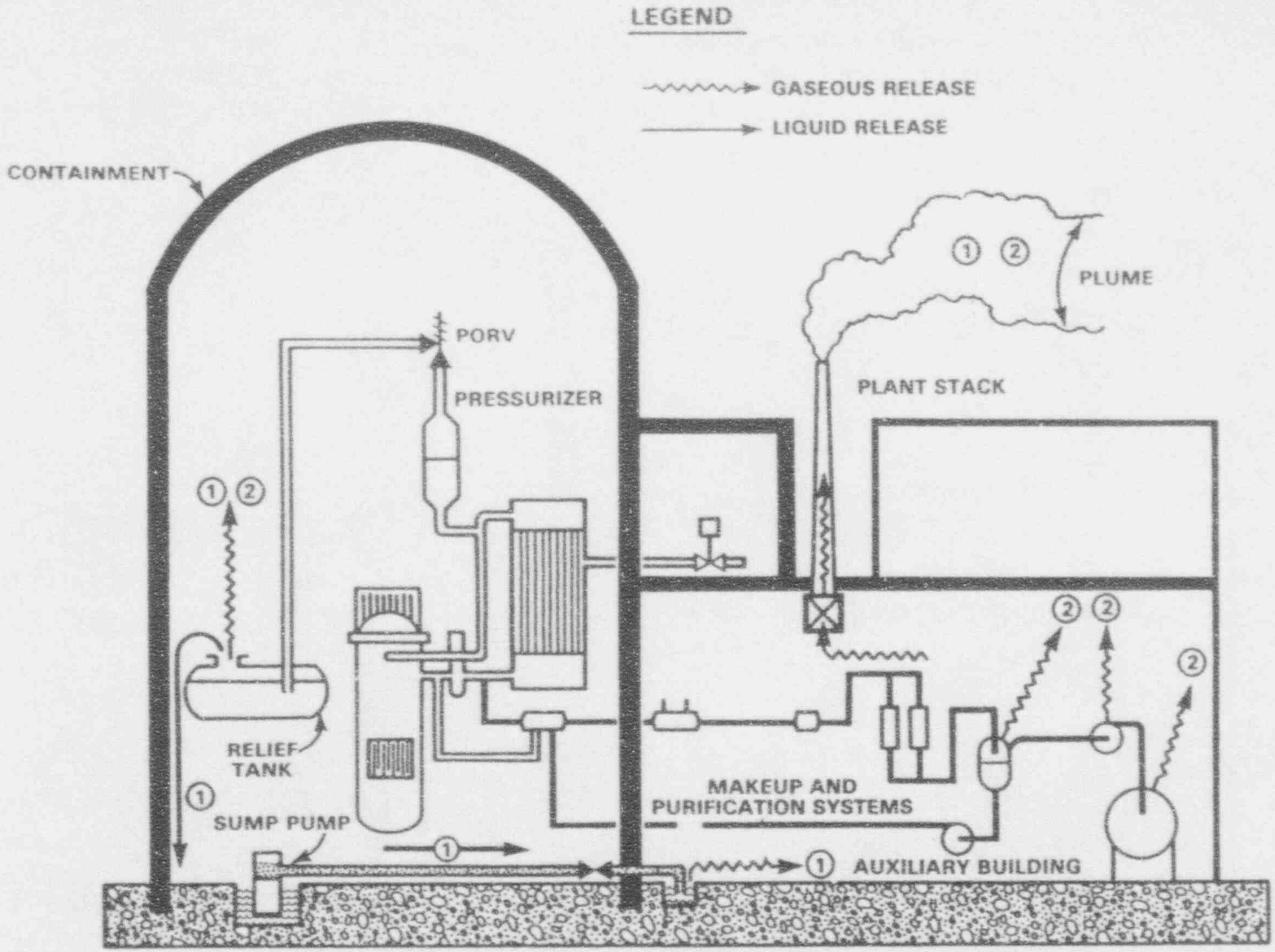


Figure 2.4-5 TMI-2 scenario: System nearly liquid solid. Liquid expanding with increasing temperature.



1. Early (first 38 min) before core damage, normal coolant only, sump pump operation.
2. After core damage, leakage from makeup and purification system was the source of most of the release.

Figure 2.4-6 TMI accident radioisotope release pathways

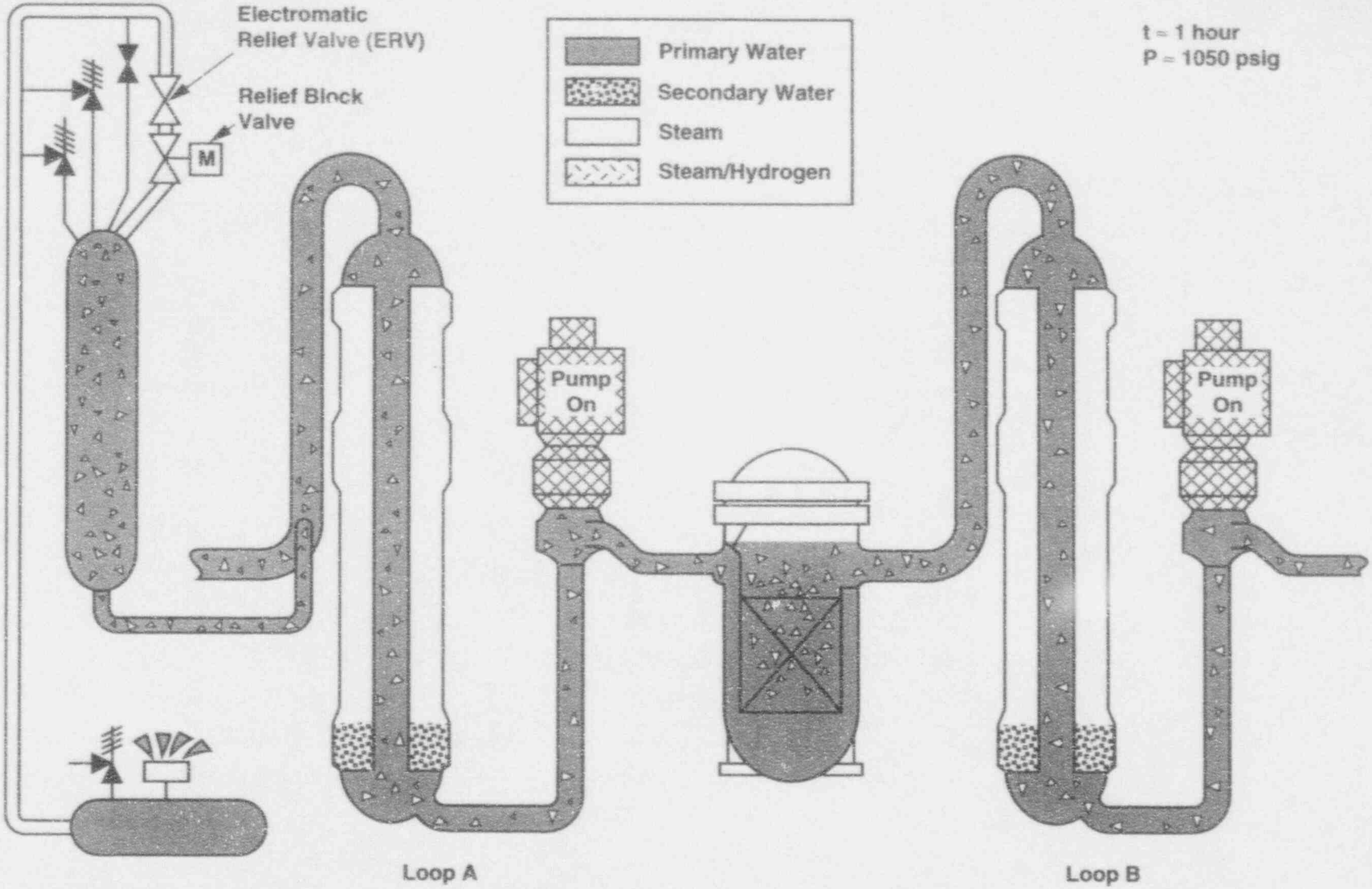


Figure 2.4-7 TMI-2 scenarios: Primary system pressure and temperatures nearly constant following secondary steam condition. Primary voids increasing.

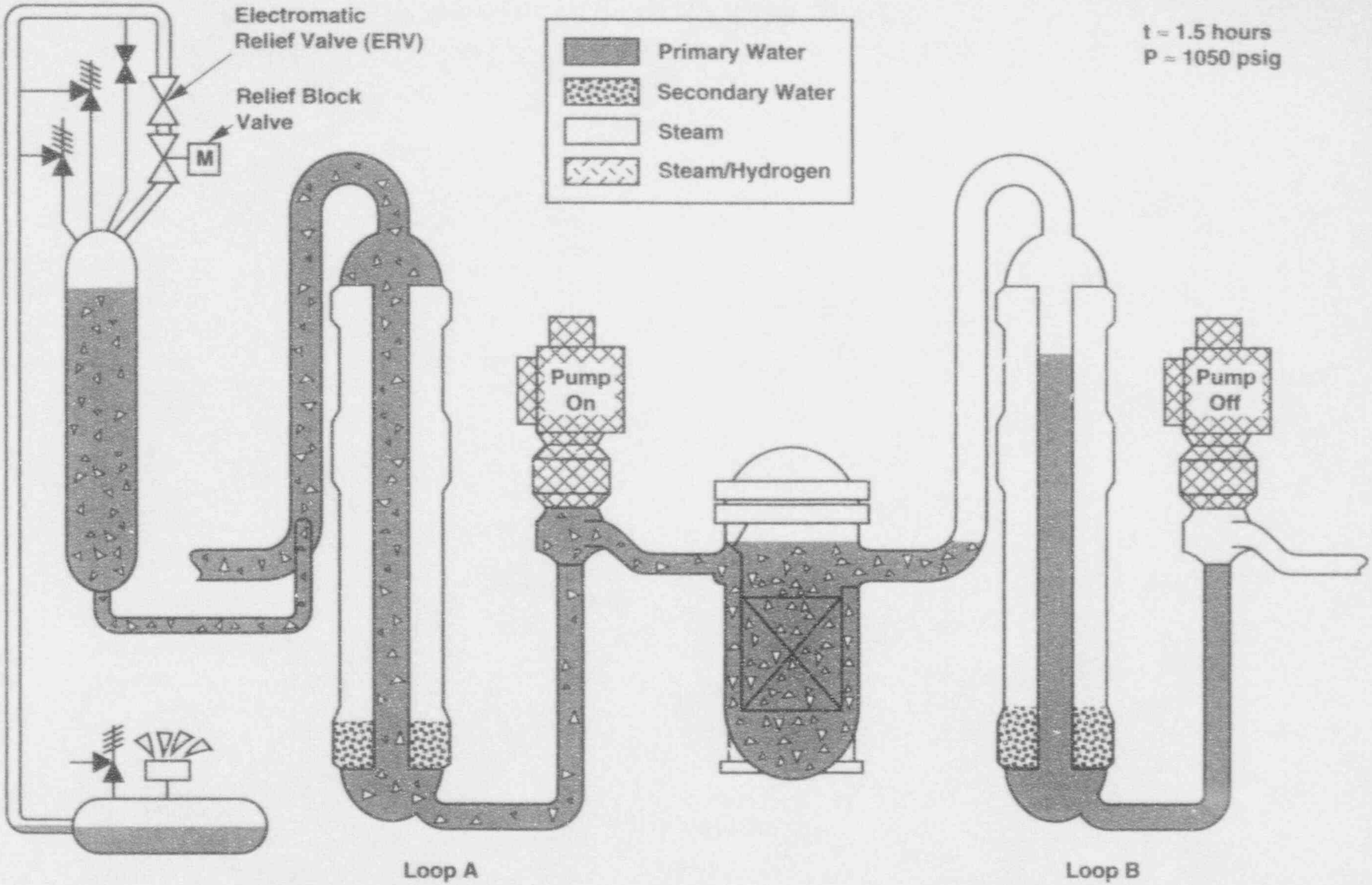


Figure 2.4-8 TMI-2 Scenario: Loop A pumps operating. Loop B stagnant after shutdown of Loop B pumps. Primary voids increasing.

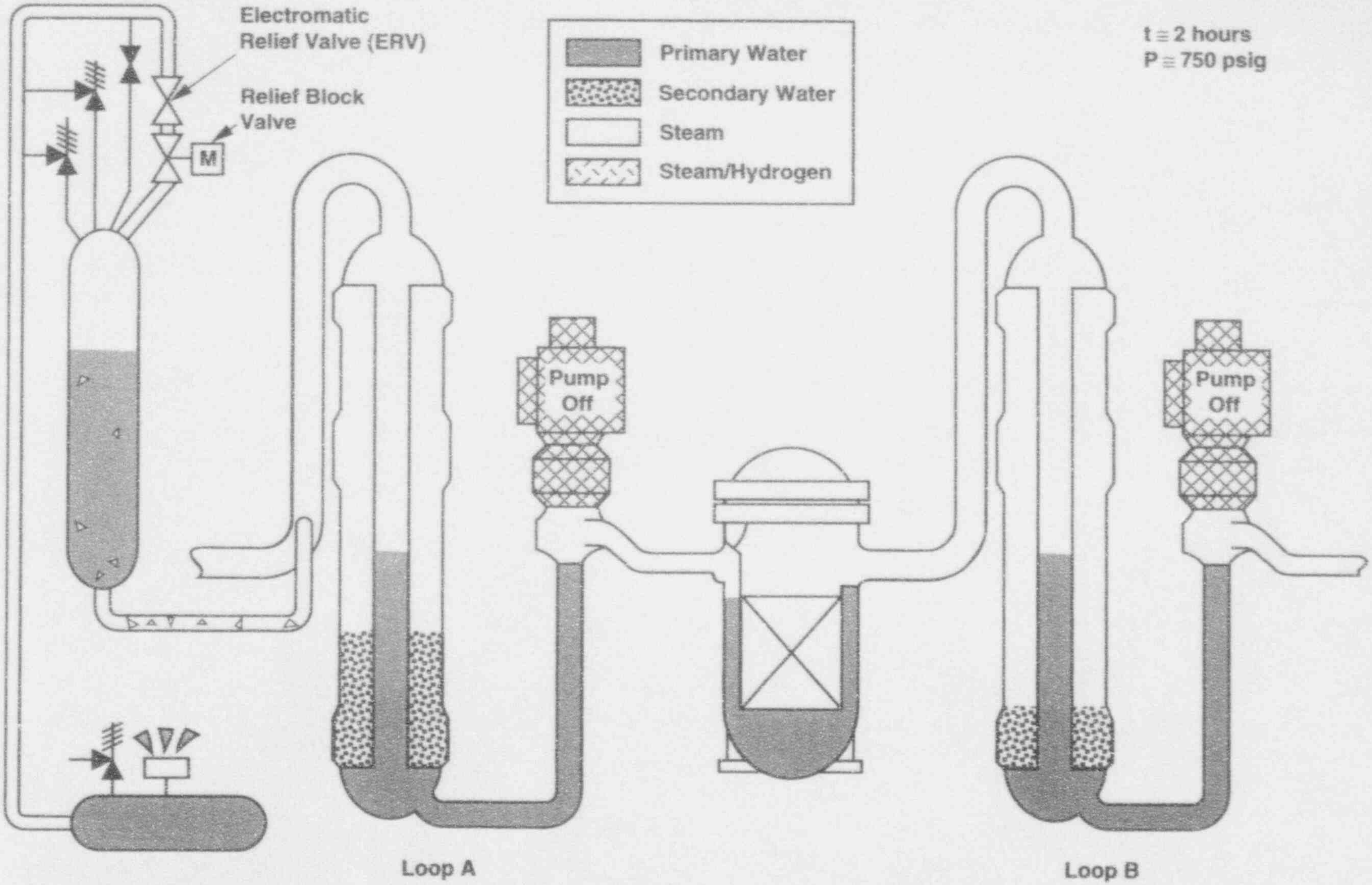


Figure 2.4-9 TMI-2 scenario: All pumps off. Reactor core drying out and heating up. Superheated steam flowing to pressurizer and to one steam generator and condensing.

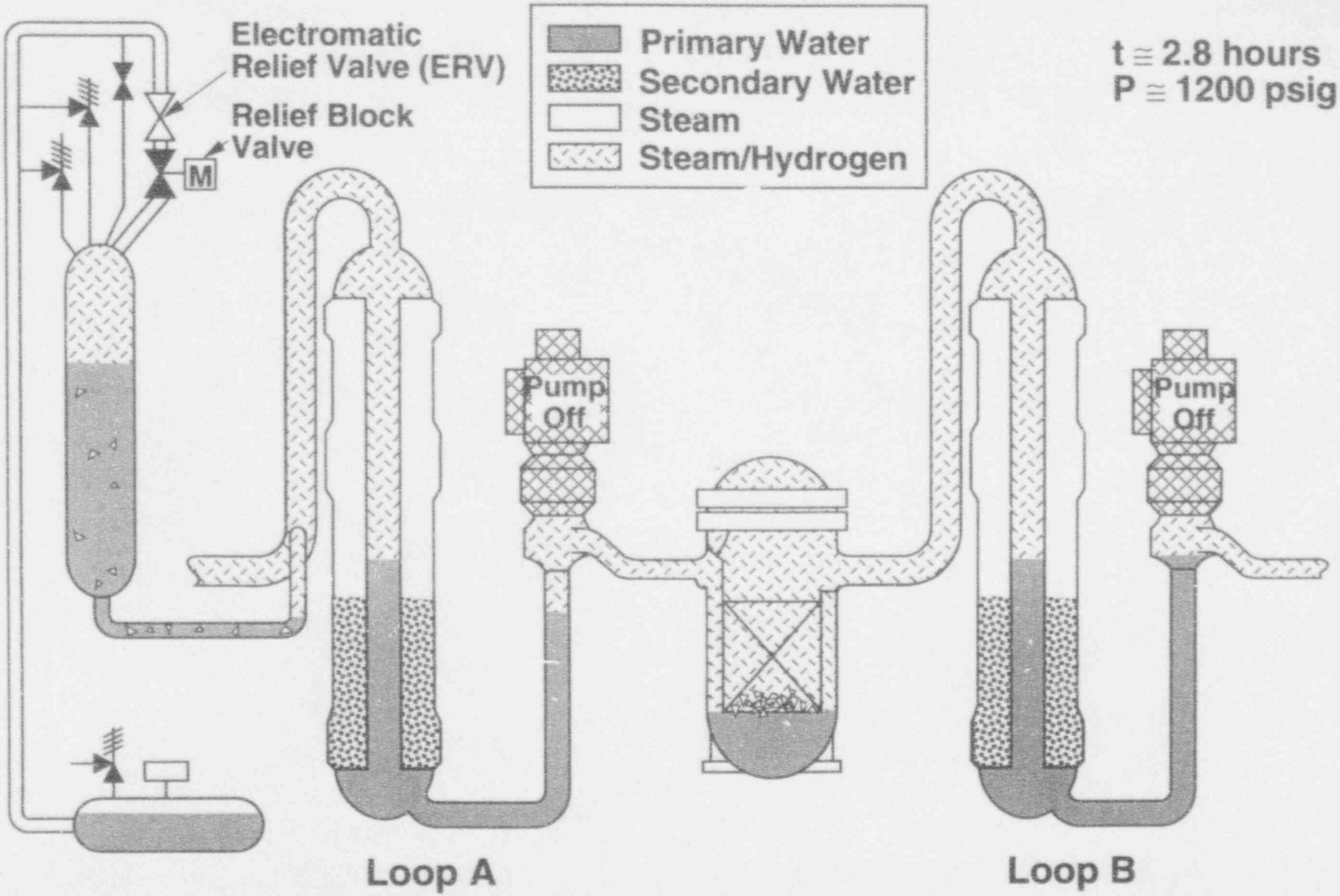


Figure 2.4-10 TMI-2 scenario: Core dryout and heatup continuing. Hydrogen generation by steam zirconium reaction in hotter regions.

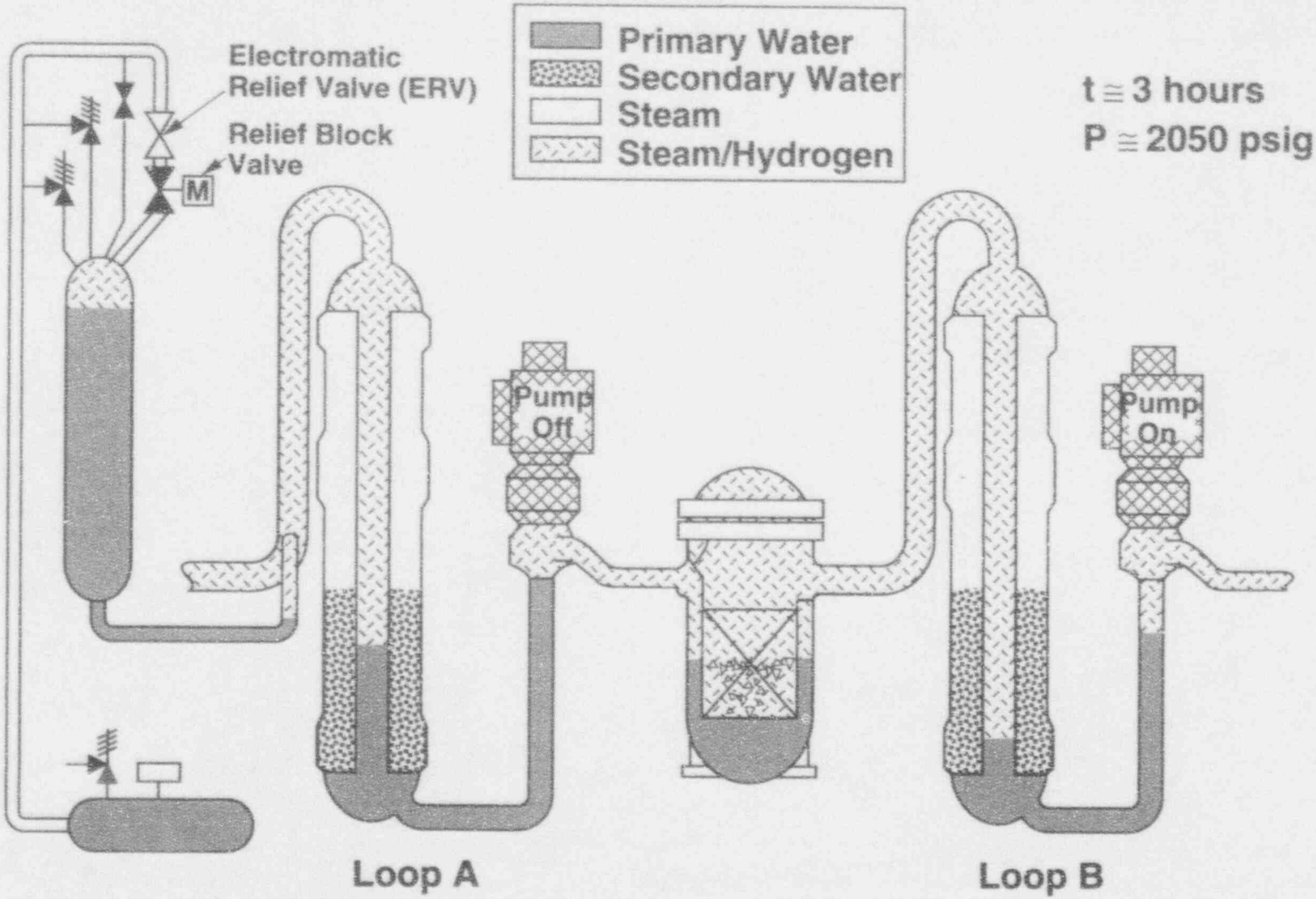


Figure 2.4-11 TMI-2 scenario: Core partially quenched by fluid during Loop B pump start. Heatup resumes.

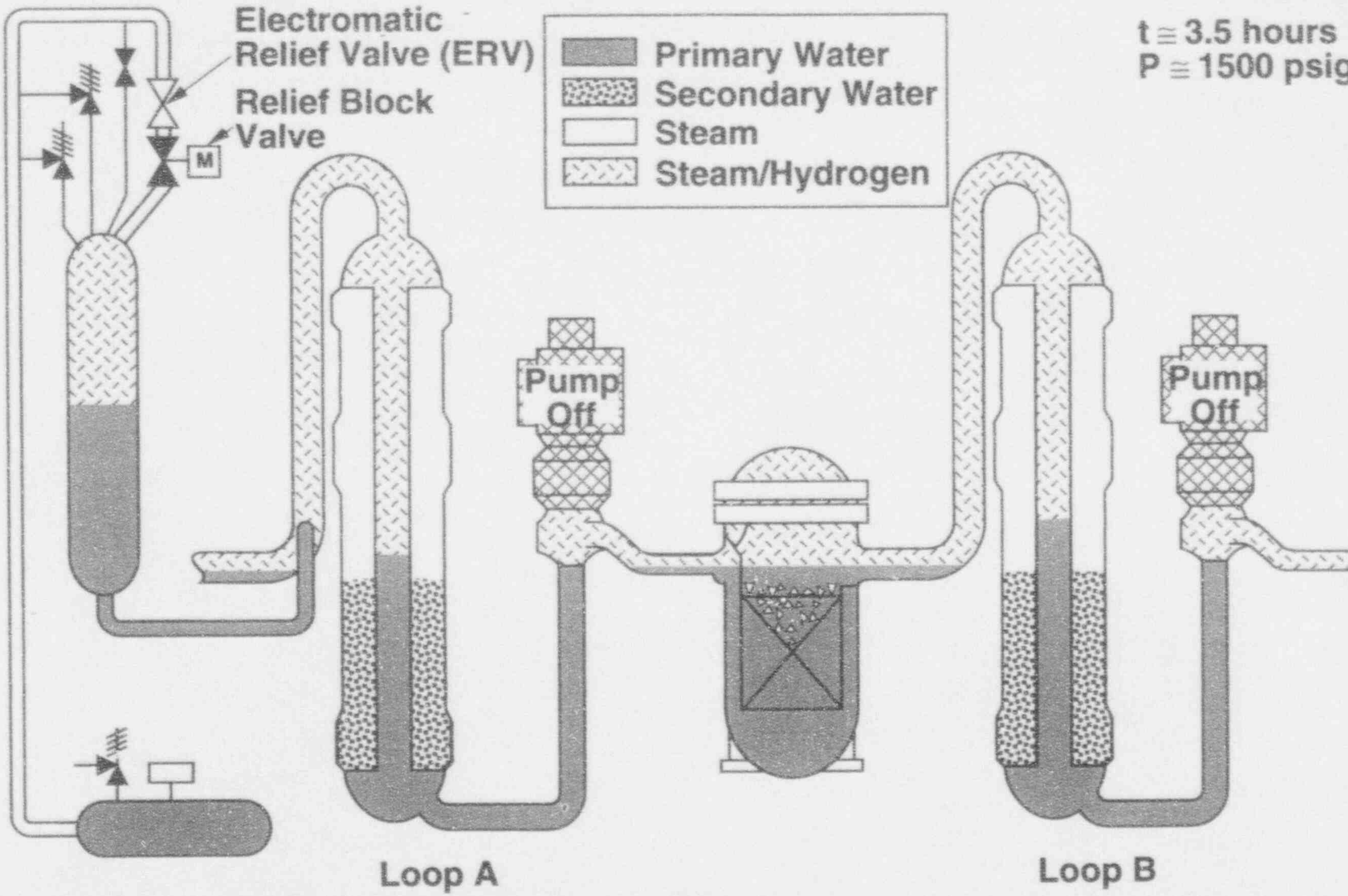


Figure 2.4-12 TMI-2 reactor vessel refilled by manual initiation of safety injection. Core temperatures decreasing.

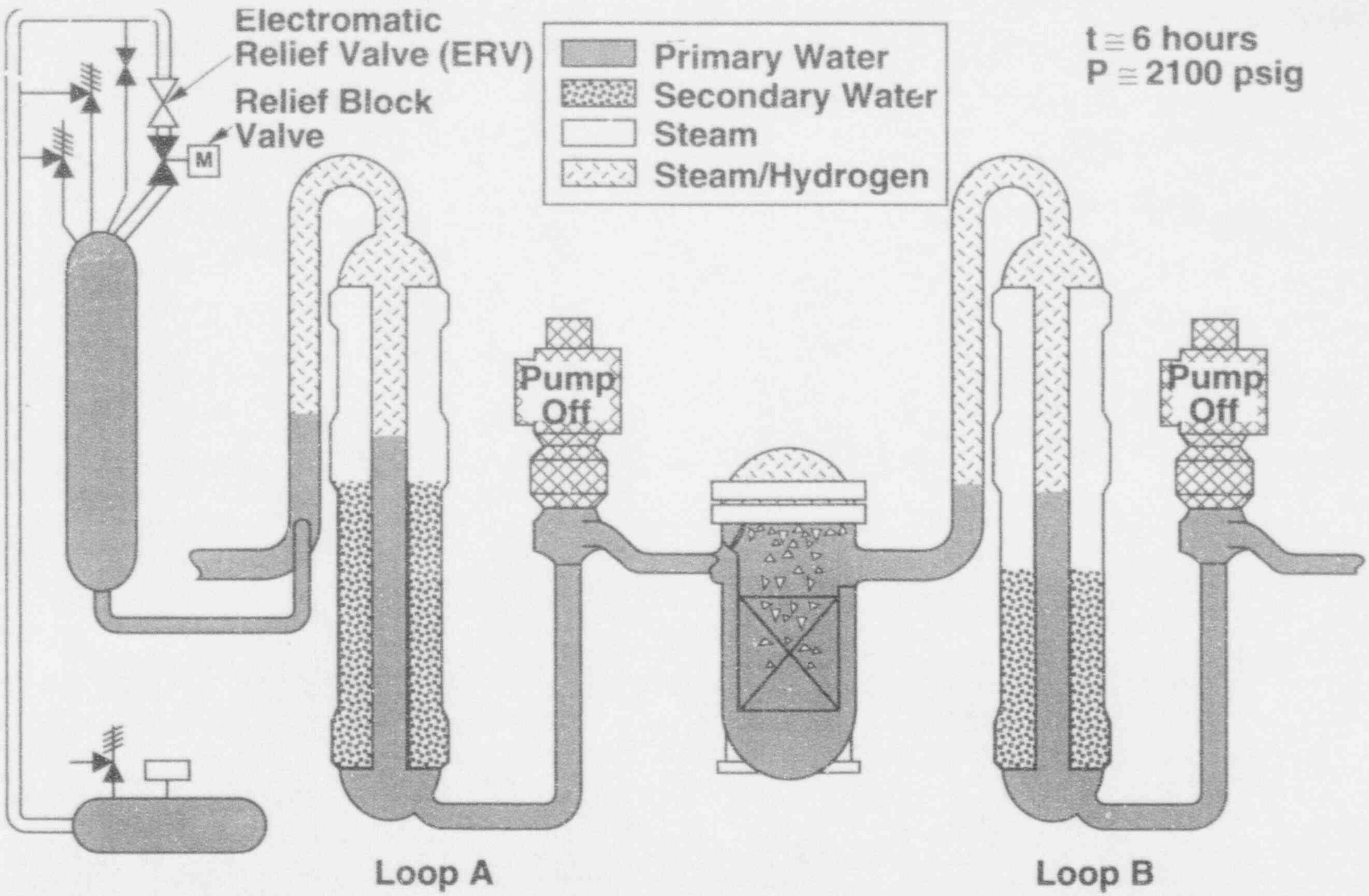


Figure 2.4-13 TMI-2 scenario: System pressurized by high-pressure injection system intermittent liquid release through top of pressurizer. Heat removal by heatup of injected water. Steam generator heat transfer blocked by hydrogen.

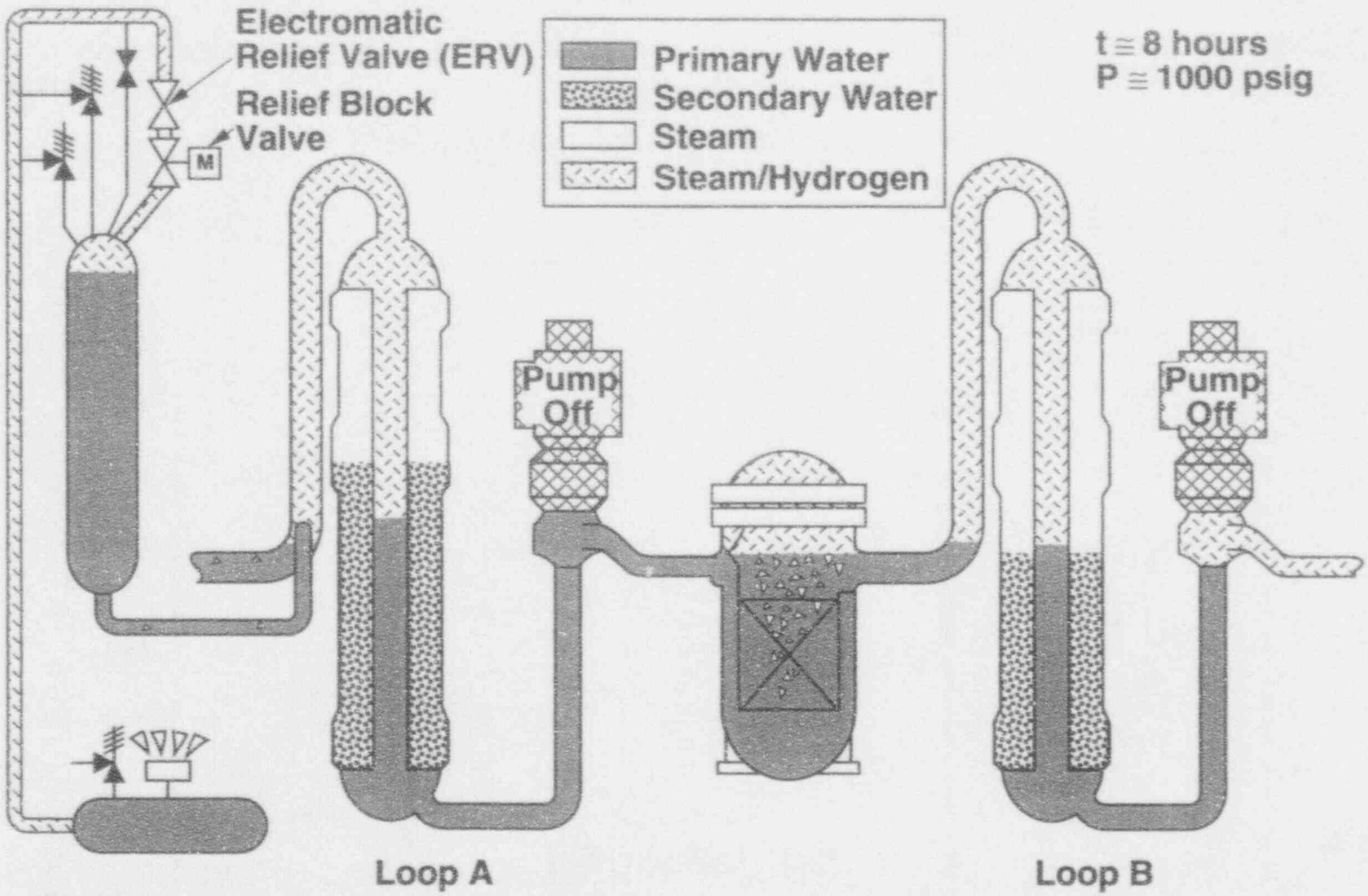


Figure 2.4-14 TMI-2 scenario: Primary system depressurizing and releasing hydrogen through the pressurizer into the containment

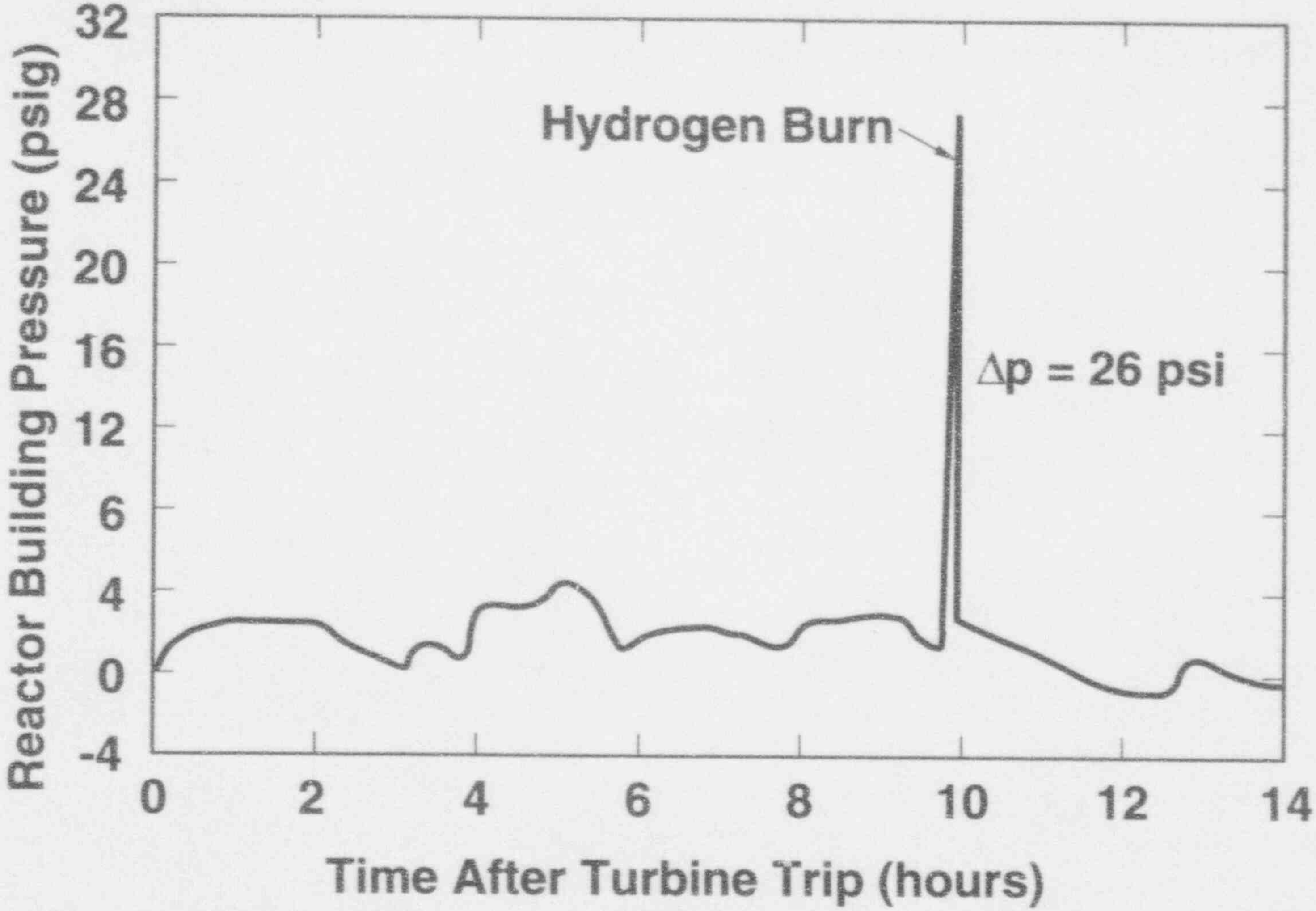


Figure 2.4-15 TMI-2 containment pressure versus time

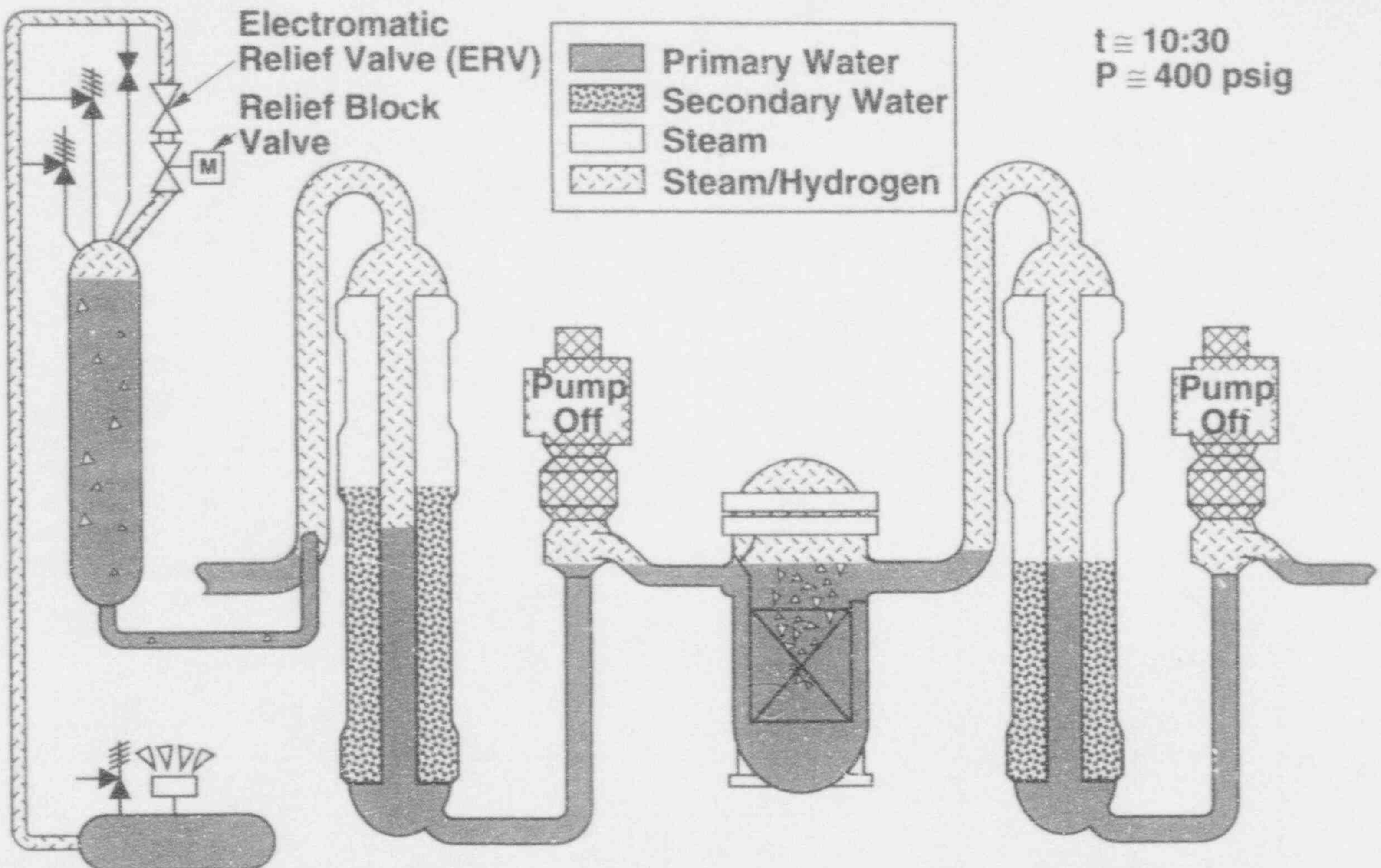


Figure 2.4-16 TMI-2 primary system pressure reaches a minimum as pressurizer temperature returns to saturated conditions. Liquid in system maintained during depressurization by high-pressure injection and core flood tanks.

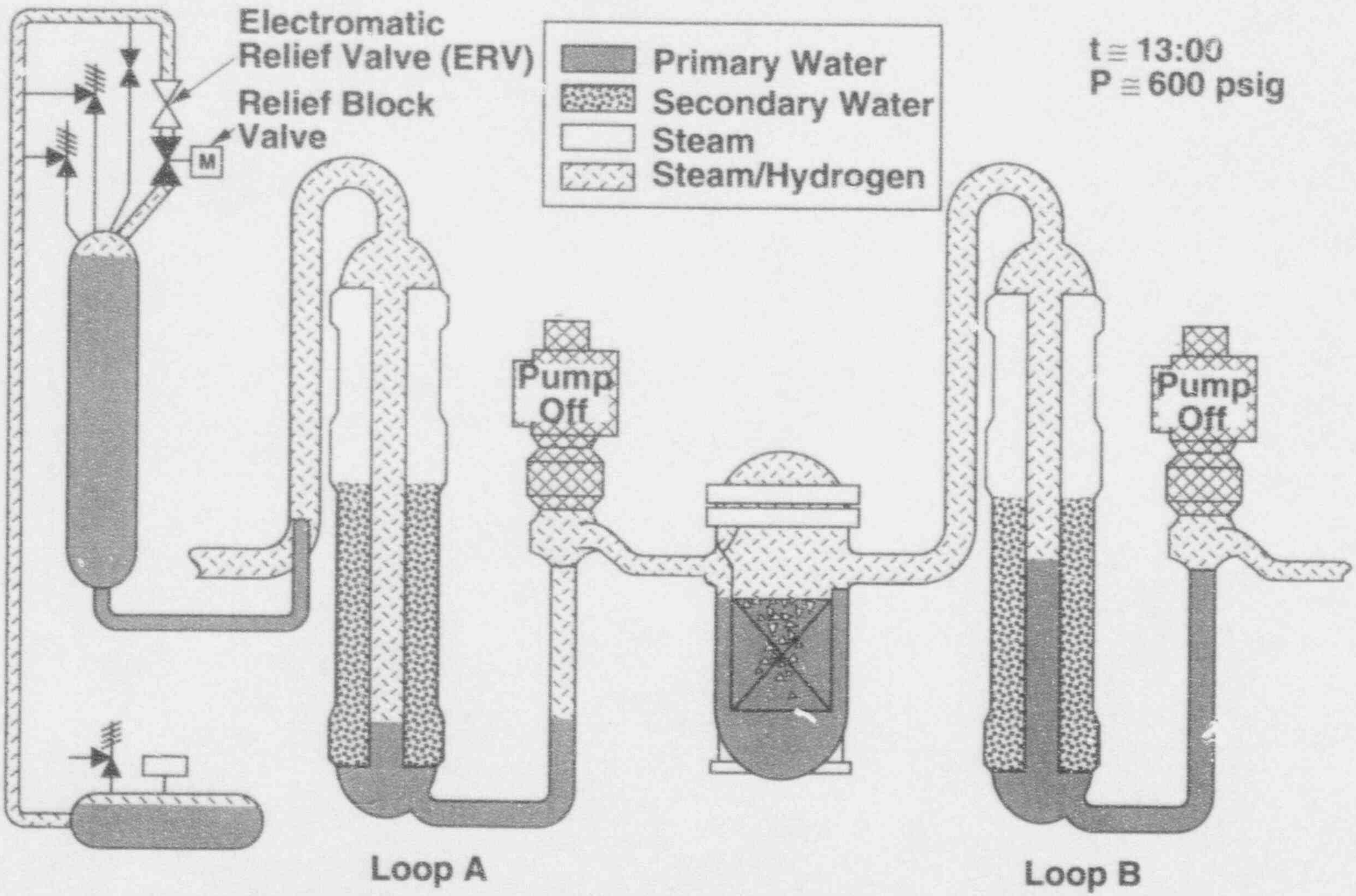


Figure 2.4-17 TMI-2 scenario: Steam generators blocked by hydrogen. Reactor vessel level decreasing. Primary system pressure increasing. Minimal make-up flow.

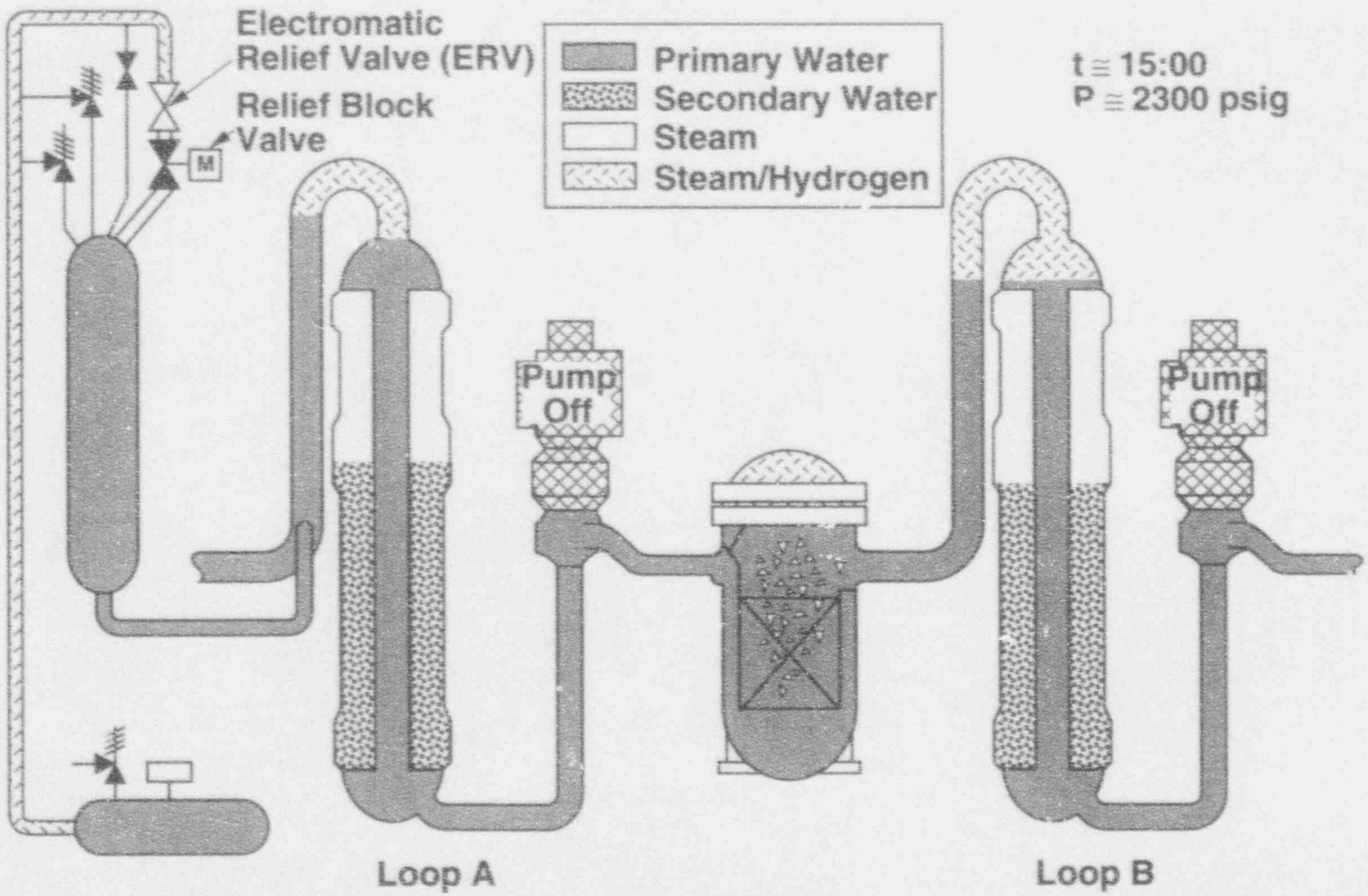


Figure 2.4-18 TMI-2 scenario: System repressurized by high-pressure injection. Natural circulation to steam generators blocked by hydrogen.

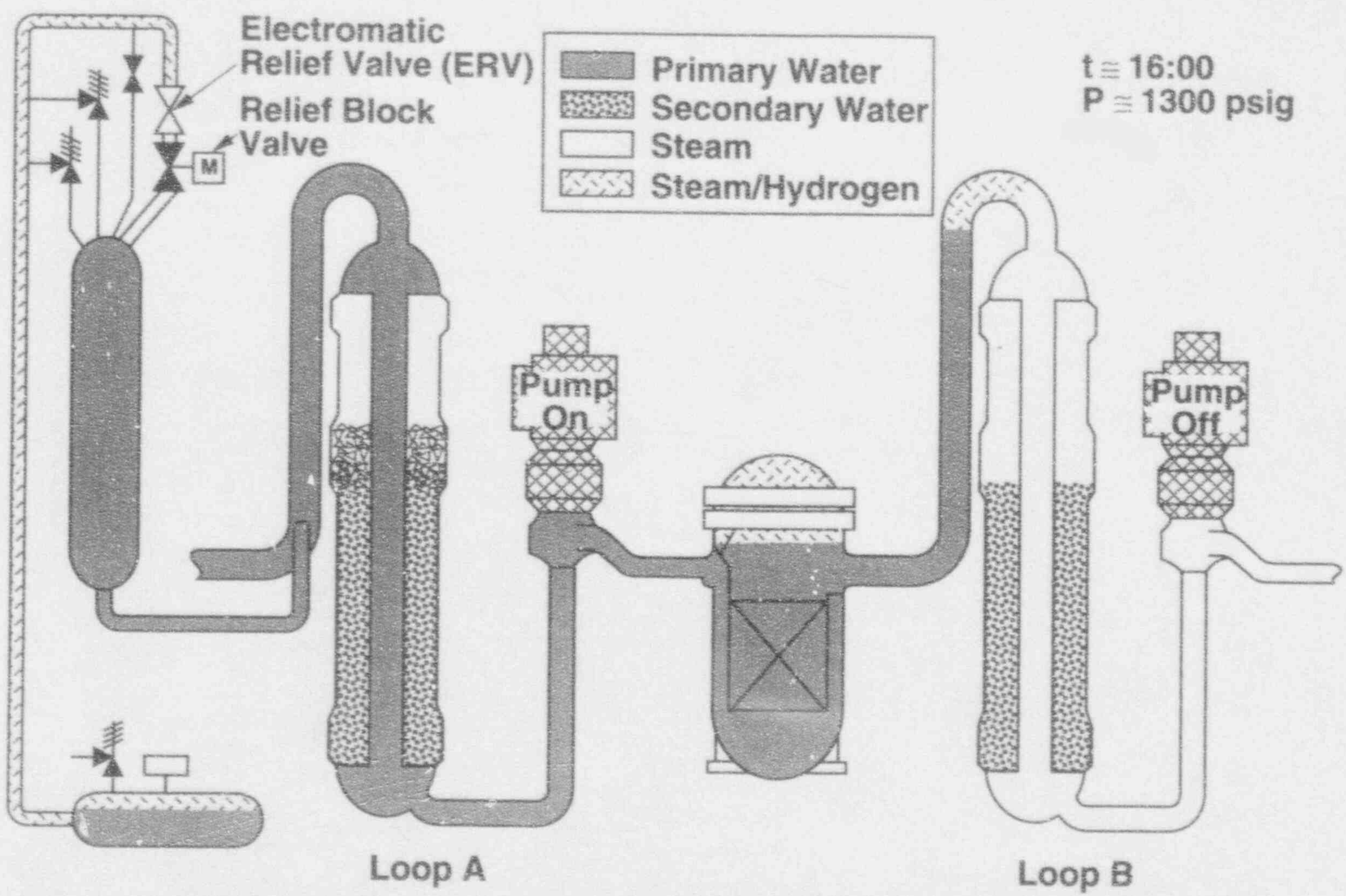


Figure 2.4-19 TMI-2 scenario: Forced circulation reestablished in Loop A with heat removal via Loop A steam generator

References for Section 2.4

1. NUREG-0600, "Investigation Into The March 28, 1979 Three Mile Island Accident by Office of Inspection and Enforcement," Investigative Report No. 50-320/79-10, August 1979.

2. E. Rubinstein and J. F. Mason, "An Analysis of Three Mile Island," *IEEE Spectrum*, November 1979.

3. M. Rogovin, G. T. Frampton, et al, *Three Mile Island, A Report to the Commissioners and to the Public*, NUREG/CR-1250 Volume II Part 2, January 1980.

4. NUREG-0585, *TMI-2 Lessons Learned Task Force Final Report*, 1980.

5. *NRC Action Plan Developed as a Result of the TMI-2 Accident*, NUREG-0669, May 1980.

6. R. A. Knief, "The Accident at Three Mile Island Unit 2," Chapter 15 of *Nuclear Energy Technology - Theory and Practice of Commercial Nuclear Power*, Hemisphere Publishing, 1991.

2.5 Chernobyl

The worst nuclear power plant accident occurred at the Chernobyl-4 plant in the Soviet Union. A remarkable series of events began on April 25, 1986 and continued over several days, resulting in more than 30 deaths and 237 injuries from radiation exposure, as well as massive contamination of wide geographical areas. The radiation released was measurable over much of the globe. A combination of human errors, design errors, and complacency contributed to the accident. In many ways, the attitude toward nuclear safety in the Soviet Union was similar to the pre-TMI attitude in the United States. This section provides a brief overview of the Chernobyl reactor design, a description of the sequence of events leading to the accident, and a discussion of the relevance of the accident to U.S. plants.

2.5.1 Chernobyl-4 Design Features

The Chernobyl-type reactors have undergone many design and operation changes since the accident at Chernobyl-4. The discussion below portrays the design as it existed at the time of the accident and does not reflect the many changes that have since occurred.

The Chernobyl site in located in the Ukraine and contains four RBMK reactors. As shown in Figure 2.5-1, the RBMK design is a graphite-moderated, light water cooled, pressure tube reactor.[1,2] The RBMK-1000 design generates approximately 1000 MW_e. The reactor contains 1661 vertical pressure tubes containing slightly enriched uranium dioxide fuel elements. The fuel tubes are made of a zirconium alloy and contain water at a pressure of about 1000 psig (7.1 Mpa). The water acts as a coolant, but unlike U.S. reactors, is not the primary moderator of neutrons.

The graphite moderator is 39 ft (12 m) in diameter and 23 ft (7 m) high. The fuel tubes pass up through the moderator assembly. Cooling water flows upward through the core with steam collected and driven through two turbines to generate electricity. Eight pumps return the water to the core. One of the most significant problems of the Chernobyl-4 core design was a positive void coefficient of reactivity. As boiling in the core increased, the power level increased. There were also problems with the reactivity control systems. 180 control rods are inserted from the top to control the reactor. To further exacerbate the reactivity problem, the control rods moved slowly and under some situations the control rods did not immediately introduce negative reactivity in the early phases of insertion.

The RBMKs do not employ a U.S. style containment building; however, they are not totally without containment. The graphite moderator is enclosed in a steel container filled with inert gases to prevent graphite fires. The steel container is further surrounded by a concrete structure on all sides but the top. Much of the primary system piping is contained in small concrete enclosures intended to deal with small loss of coolant accidents.

2.5.2 The Chernobyl Experiment

The Chernobyl accident began on April 25 with an experiment.[1] The experiment was intended to demonstrate that, in the event of a turbogenerator disconnection and the loss of offsite power, the inertia of the turbine rotor could be used to help maintain emergency power while the standby diesel generators were started. This in turn could relieve the diesel generators of the rapid startup requirements and associated stresses on the equipment. While such tests are not unknown, the procedures for the test were very poor, there was a desire to complete the tests quickly, and the operators lacked a complete understanding of the hazards involved.

Virtually no additional safety measures were taken during the test. The safety procedures indicated that all switching operations were to have the permission of the plant shift foreman and that during an emergency the staff were to follow plant instructions. (There were no specific instructions for these conditions.) This situation was in spite of the fact that the experiment called for deactivation of the Emergency Core Cooling System, so that it would not automatically actuate as the circulation pumps ran down.

2.5.3 The Sequence of Events

The material in this section was taken primarily from a September 11, 1986 special issue of Nuclear News.[1] This special issue contains an analysis of the accident by Valery Legasov of the Soviet Union as presented to an International Atomic Energy Agency conference in Vienna. Legasov presented a candid view of the accident, including many side comments. He noted, for example, that there would have been pressure on the operators to complete the tests as they shutdown on this occasion, because the next planned maintenance period would be more than a year away. He also said that, in hindsight, it can be seen that technical means could easily have been used to prevent the operators from overriding safety protection systems and otherwise violating procedures. Failure to provide adequate protection for such human error represented "a tremendous psychological mistake" on the part of the designers of the RBMK reactor.

The run up to the accident started at 1:00 a.m. on April 25, with the reduction of reactor power over the next five minutes from 100 percent (3200 MWt) to half that much. Then the unwanted turbogenerator was shut down. The plant systems that had been connected to this turbogenerator, including four of the main circulation pumps and two feedwater pumps, were switched to the grid busbars of the turbogenerator that was still on line.

At 2:00 pm, the ECCS was isolated to prevent it from kicking in automatically. The start of the test, however, was then postponed at the request of the local electricity dispatcher. As a result, the plant was maintained in the unauthorized state with no ECCS for the next nine hours, although this particular violation did not in actuality play any important part in what followed. Still, the delay may have aggravated operator impatience over the test, and contributed to the "mindset" that led plant personnel to ignore procedures and block safety systems in their effort to get the plant to the proper power level for the test.

At 11:10 pm, the load demand was lifted, and preparation for the test resumed with power reduced to the required level, 700-1000 MWt. The automatic control system that operates on groups of control rods in 12 zones of the core, to stabilize power density distribution, was switched off, in keeping with a low-power operation requirement. At higher power levels, these zonal rods also regulate the average power automatically. When the local controllers are switched off, automatic controllers working on a signal of the average power of the whole core come into play, but it appears that the operators did not synchronize this automatic system quickly enough to the required power setpoint. There was an overshoot in the power reduction, and the level fell below 30 MWt.

By 1:00 am, on April 26, the operators were able to stabilize the power back at 200 MWt, but this was as high as they could get it due to the xenon poison buildup that had started during the excursion to lower power and was still continuing. To drag the reactor up to 200 MWt, the operators had pulled far too many of the manual control rods out of the reactor, and the neutron flux distribution in the core was such that the reactivity worth of those rods that would be effective in the first few centimeters of travel back into the core was limited to the equivalent of six to eight fully inserted rods.

According to the rules, the operating margin of reactivity should not be allowed to go below 30 rod equivalents without special authorization from the chief engineer of the power station. Legasov said that if the margin ever falls below 15 rod equivalents, "nobody in the whole world--not even the Prime Minister--can authorize continued operation of the reactor." But the operators were so intent on getting the reactor up to an acceptable power level for the test--another attitude attributed to the mindset--that they ignored the touchy side of the reactor.

Thus, the operators at Chernobyl-4 decided to press on, and at 1:03 and 1:07 a.m., they started the sixth and seventh main circulation pumps in immediate preparation for the tests. Since the reactor power, and consequently the hydraulic resistance of the core and the recirculation circuit, were substantially lower than planned, the full eight pumps produced a massive coolant flow through the reactor, 245,000 to 255,000 gpm (56,000 to 58,000 m^3/hr). At some individual pumps, the flow was up to 35,000 gpm (8000 m^3/hr), compared with a normal operating level of 30,000 gpm (7000 m^3/hr). This was another violation, because of the danger that pump breakdown and vibration could be caused by cavitation at the pumps. But the most serious consequence of the increased flow was the creation of the coolant conditions very close to saturation, with the possibility that a small temperature increase could cause extensive flashing to steam. The steam pressure and the water level in the steam separation drums had also dropped below emergency levels--but, as part of the continuing attempt to keep the reactor running long enough for the test to be started, the operators also blocked the resulting signals of the low levels to the emergency protection system.

At 1:19 a.m., the feedwater supply was increased--to as much as four times its initial value--in an attempt to restore the water level in the steam separation drums. This reduced both the reactor coolant inlet temperature and fuel channel steam production, with consequent negative reactivity effects. Within 30 seconds the automatic control rods had fully withdrawn in response to the negative reactivity, and the operators attempted to withdraw the manual rods as well. But the operators again overcompensated, and the automatic rods began to move back in.

At 1:22 a.m., the reactor parameters were approximately stable, and the decision was made to start the actual turbine test. But in case they wanted to repeat the test again quickly, the operators blocked the emergency protection signals from the turbine stop valve, which they were about to close, so that it would not trip the reactor. Also, just before they shut off the steam to the turbine, they sharply reduced the feedwater flow back to the initial level required for the test conditions. This boosted the coolant inlet temperature, creating a transient situation that could not be addressed because safety systems were cut off.

At 1:22:30 a.m., the operators obtained a printout from the fast reactivity evaluation program, giving them the position of all the rods and showing that the operating reactivity margin had fallen to a level that required immediate shutdown of the reactor. But they delayed long enough to start the test. There was clearly a failure to appreciate the basic reactor physics of the system, which had rendered the control rods relatively worthless. The neutron flux distribution in the core had been pulled into such a distorted shape that the majority of the rods would have go to well into the core before they would encounter sufficient neutron flux for their absorption to be effective.

At 1:23:04 a.m., the turbine stop valve was closed. With the isolation of the turbine, four of the primary circulation pumps started to run down--another transient situation for which the automatic responses had been cut off.

Shortly after the beginning of the test, the reactor power began to rise sharply. The bulk of the coolant was very close to the saturation point at which it would flash to steam, because the operators had earlier run an excessive level of coolant flow with all eight pumps on during low power reactor operation. The RBMK reactor, with its positive void coefficient, responds to any such formation of steam with an increase in reactivity and power, and further increases in temperature and steam production--producing a runaway condition.

At 1:23:40 a.m., the scram button--which would drive all control rods into the core--was pushed. Legasov told the Vienna meeting that there seemed to be some ambiguity about the motivation for this action, as unearthed during subsequent questioning by investigators of the fatally ill shift foreman, who had given the order--he may have been belatedly responding to the printout of reactivity margin; he could have been responding to the sharp rise in reactor power; or he may simply have believed that the test had now run long enough to allow him to shut down the reactor.

After a few seconds a number of shocks were felt in the control room, and the operator saw that the control rods had not reached their lower stops. He therefore deactivated the rods to let them fall by gravity.

At about 1:24 a.m., observers outside the plant reported two explosions, one after the other; burning lumps of material and sparks shot into the air above the reactor and some fell onto the roof of the turbine hall and started a fire.

In his presentation of Table 2.5-1, which delineates the operator violations, at the Vienna meeting, Legasov said that if any one of the first five violations had not been committed, the accident would not have happened.

Inside the Reactor

The mechanism of the accident, particularly in the last few seconds before the explosion that literally blew the top off the reactor, was the subject of intense interest for one of the working groups at the meeting. By the end of the week, the consensus of international experts was that the accident mechanism as described in the Soviet report--a prompt critical reactivity excursion and a steam explosion--was a wholly plausible explanation for what happened. There is still a need for more detailed understanding of the mechanism, and some doubts linger on the cause of a second explosion that was reported to have taken three or four seconds after the first.

The prompt critical excursion took the power first to around 530 MWt at 1:23:40, and only the Doppler effect of the fuel heating up to an estimated 3000°C pulled it back down briefly. The continuing reduction of water flow through the fuel channels during the power excursion led to intensive steam production, the destruction of the fuel, a rapid surge of coolant boiling (with the particles of destroyed fuel entering the boiling water), a rapid and destructive increase of pressure in the fuel channels, and finally the explosion that destroyed the reactor.

At precisely the moment of fuel disruption, which was believed to occur when the energy density in the fuel exceeded 540 BTU/lbm (1260 J/g), there was an abrupt fall of the coolant flow as check valves on the main circulation pumps closed in response to the increased pressure in the core. This loss of flow was also recorded by the data-logging system. The flow from the pumps would have been partially restored after the rupture of the fuel channels, but the water was now directed into a mass of damaged zirconium and hot graphite. The ensuing reaction would have produced large amounts of hydrogen and carbon monoxide, which--upon contact with air above the reactor--could have caused the second explosion.

2.5.4 Implications for U.S. Plants

U.S. reactors employ very different designs than Chernobyl-4. First, all U.S. power reactors have negative reactivity coefficients in virtually every situation, and control rods in U.S. plants provide fast negative reactivity insertion. Further, disabling of safety systems in violation of technical specifications is not expected to knowingly occur. The level of safety-related training is much higher than that attained at Chernobyl prior to the event. Significantly, all U.S. power reactors also employ large strong containment structures as we will discuss in Module 4. Such a structure might not have been effective against the enormous energy releases of Chernobyl, but would be effective in many other accidents.

One U.S. reactor, the N Reactor at Hanford, Washington, was shut down following Chernobyl. The design of the N Reactor included pressure tubes and graphite moderation, but was different in many respects. However, the reduced need for the plutonium that it produced coupled with adverse publicity and safety concerns led to the ultimate shutdown and mothballing of the reactor.

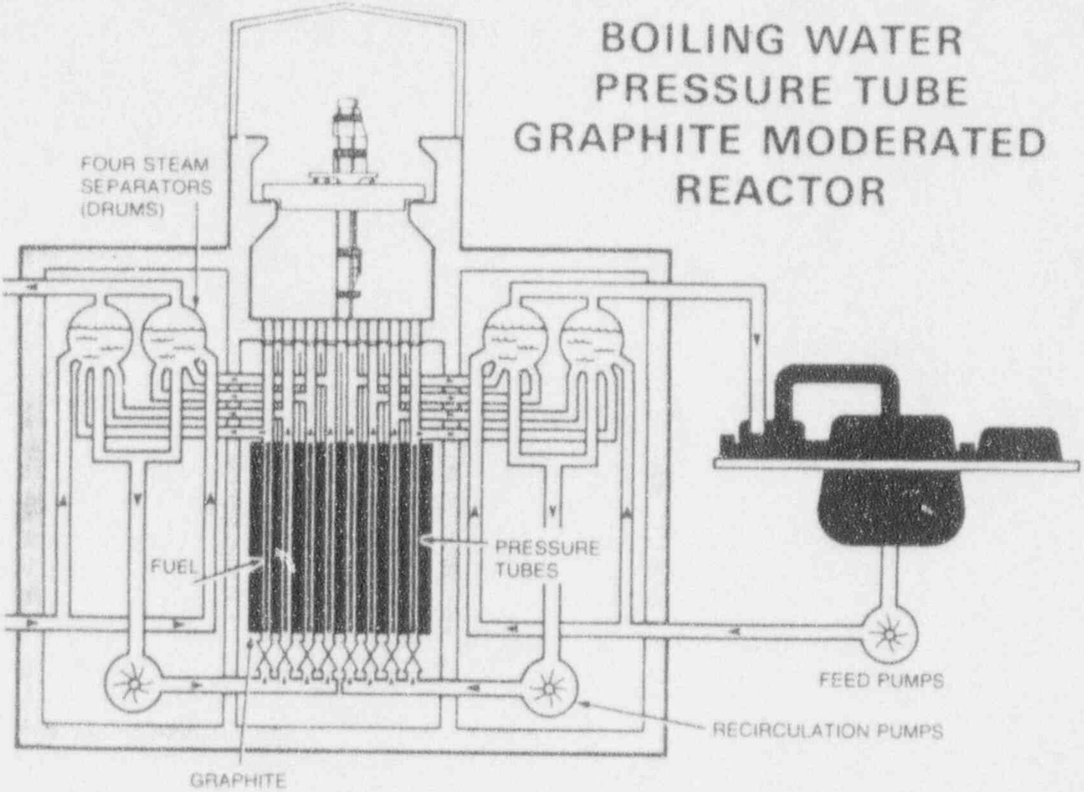
In Module 5, we will discuss the health effects and other consequences of serious reactor accidents. However, it is worthwhile to consider whether accidents as devastating as the one at Chernobyl could occur here. While the specific accident could not occur due to the different reactor physics involved, risk assessments for U.S. reactors have identified events in which containment fails and very large radiation releases occur. Accidents are possible that could result in a greater number of early fatalities if the radiation release and weather conditions were less favorable than at Chernobyl. In particular, the fire lofted much of the radionuclides high into the atmosphere so that offsite residents closest to the plant survived the release. Thus, while such accidents are not considered likely, we should avoid the mindset that "it can't happen here."

Table 2.5-1
The Most Dangerous Violations of Operating Procedures at Chernobyl-4*

	Violation	Motivation	Consequence
1.	Reducing operational reactivity margin below permissible limit	Attempt to overcome xenon poisoning	Emergency protection system was ineffective
2.	Power level below that specified in test program	Error in switching off local auto-control	Reactor difficult to control
3.	All circulating pumps on with some exceeding authorized discharge	Meeting test requirements	Coolant temperature close to saturation
4.	Blocking shutdown signal from both turbogenerators	To be able to repeat tests if necessary	Loss of automatic shutdown possibility
5.	Blocking water level and steam pressure trips from drum-separator	To perform test despite unstable reactor	Protection system based on heat parameters lost
6.	Switching off emergency core cooling system	To avoid spurious triggering of ECCS	Loss of possibility to reduce scale of accident

*From the Soviet Union summary of its report to the IAEA.

Figure 2.5-1
Boiling Water Pressure Tube Graphite Moderated Reactor[1]



Schematic diagram of the RBMK-1000, a heterogeneous water-graphite channel-type reactor (source: Soviet report to IAEA)

[1]Reprinted by special permission from the International Atomic Energy Agency.

References for Section 2.5

1. Nuclear News - *Special Report, American Nuclear Society*, La Grange Park, Illinois, September 11, 1986.

2. Nuclear News - *Special Report, American Nuclear Society*, La Grange Park, Illinois, June 1986.

2.6 Severe Accident Frequencies and NUREG-1150 Perspectives

The first five sections of Module 2 have discussed how severe accidents can occur at nuclear power plants. This section introduces the analysis methods used to identify the particular accidents that are possible and their likelihoods. The discussions are supplemented by insights from the NUREG-1150 risk assessments.[1] The consequences of severe accidents are only mentioned briefly in this section, but are discussed in more detail in later modules. While this course is not primarily intended as course in analysis methods, it is important to understand the basic concepts discussed in this section. Increasingly, as discussed in Section 2.7, safety issues are being resolved, policies are being set, and decisions are being made based at least partially on estimates of core damage frequency and other risk measures. Responsible participation in these processes requires a basic understanding of the estimation methods and their limitations. More in-depth training in these methods is available in other NRC courses.[2]

2.6.1 Risk Concepts and Terminology

Colloquially, risk is defined as danger, hazard, peril--exposure to death, injury, loss, or some other negative consequence. Thus, risk implies an unrealized potential for harm. If the danger is actually realized, then it is no longer risk but actual death, injury, loss, or other harmful consequence.

To quantify a risk, the likelihood of actually experiencing a given set of consequences must be estimated. While many definitions of risk have been proposed, the following definition is consistent with such estimates:

> *Risk* is the frequency with which a given set of consequences would be expected to occur.

Typically, units of risk are yr^{-1} reflecting the likelihood of experiencing the given consequence per calendar year. Risk can be estimated for either an individual or a selected population. For example, if the consequence in question is death due to cancer, the total U.S. cancer risk is simply the total number of people per year dying of cancer. The individual risk of cancer death can be estimated by dividing the total number of U.S. cancer deaths recorded last year by the estimated U.S population. The resulting risk to an individual is approximately $2x10^{-3}$ per year; that is, on the average, an individual in the U.S. has a one in 500 chance per year of dying from cancer. Of course, the risk for particular groups of individuals within the overall population is different from this average value.

One measure of the risk of accidents at nuclear power plants is *core damage frequency*:

> The *core damage frequency* is the probability per year of reactor operation (reactor year) of experiencing a core damage accident.

For this risk, the consequence in question is a core damage accident. The criteria for the onset of core damage must be specified as part of the risk assessment. The NRC's recent NUREG-1150 risk assessment assumes that the onset of core damage for BWRs occurs when the water level is less than 2 feet above the bottom of the active fuel and reflooding of the core is not imminently expected.[1] For PWRs, NUREG-1150 assumes that the onset of core damage occurs upon uncovery of the top of the active fuel (and without imminent coolant recovery). The difference between the two plant types is a result of the fact that BWRs can be steam cooled after the water level falls below the top of the active fuel while PWRs cannot be cooled as efficiently in this manner. Estimates of core damage frequencies for various U.S. nuclear power plants range from approximately 10^{-3} to 10^{-6} per reactor year.

The term *severe accident* is often used interchangeably with the term *core damage accident*. However, as defined in Section 2.2, a *severe accident* is generally taken to be one in which the extent of fuel damage includes gross failure of the cladding and release of radionuclides from the fuel.

Potential health and economic consequences of nuclear power plant accidents include early fatalities, early injuries, latent cancers, population doses, various health effects, and onsite and offsite costs. For such consequence measures, application of the preceding definition of risk becomes more complicated, because frequencies must be estimated for accidents with varying degrees of severity. For example, the frequency of transportation accidents involving 100 or more early fatalities is substantially lower than the frequency of transportation accidents involving only 1 fatality. In risk assessments, frequencies of accidents with all possible consequence levels are estimated. It is desirable to combine the risks associated with high, moderate, and low consequence accidents into an overall risk measure. For this purpose, the concept of actuarial or consequence-weighted risk is used.

> The *consequence-weighted risk* associated with an accident is the product of the accident's frequency and its consequence.

The total consequence-weighted risk is the sum of the consequence weighted risks of the individual accidents. The process of calculating consequence-weighted risk is illustrated in Table 2.6-1 for a hypothetical plant that has only four possible accidents. Consequence-weighted risk is so widely used in probabilistic risk assessments that the modifier consequence-weighted (or actuarial) is usually dropped, and the total consequence-weighted risk is simply called the plant risk.

Some recent risk results and insights are discussed later in this section. First, the probabilistic risk assessment process is discussed.

Probabilistic risk assessment (PRA) is the systematic process of

1. identifying accidents that could endanger the public health and safety,
2. estimating the frequencies of such accidents, and
3. estimating the consequences of such accidents.

In other words, PRA addresses three basic questions:

1. What is possible?
2. How likely is it?
3. What are the consequences?

PRA methods are extremely powerful because they provide a systematic process for identifying vulnerabilities. Most PRAs lead directly to safety improvements by eliminating previously undiscovered vulnerabilities. These safety improvements are often made at the utility's initiative without the need for regulatory action. Therefore, while some of the remaining discussion in this section describes the limitations of PRA methods, the reader should note that the overall benefits of the methods far outweigh those limitations.

PRAs can be performed for non-nuclear as well as for nuclear facilities. In this course only the risks of nuclear power plant accidents are treated. Traditionally, nuclear power plant PRAs have been conducted at one of three levels. Figure 2.6-1 illustrates the activities and/or products associated with each level.[1]

The Level 1 PRA identifies potential accident initiators and models possible sequences of events that could occur as the plant responds to these initiators. To identify the potential accidents and quantify their frequency of occurrence, event trees and fault trees (Section 2.6.4) are developed and quantified using historical data on initiating event frequencies, component and system failures, and human errors. Accident sequences leading to core damage are identified and their frequencies (together with the total core damage frequency) are estimated. Although the accident sequences of primary interest in a Level 1 PRA lead to core damage, all these accident sequences are not equivalent. Some are more severe than others in terms of potential plant damage and/or public health consequences. Therefore, all the Level 1 accident sequences are classified into plant damage states according to those factors which determine the potential severity of the consequences.

> A *plant damage state* is a group of accident sequences that has similar characteristics with respect to accident progression and containment engineered safety feature operability.

The plant damage states define the important initial and boundary conditions for the Level 2 accident progression and source term analyses.

The Level 2 PRA analyzes the thermal-hydraulic progression of the accident in the reactor coolant system, interfacing systems, the containment, and, where relevant, surrounding buildings. The release of radionuclides from the fuel, the reactor coolant system, containment and surrounding buildings is also modeled. These analyses yield estimates of the frequencies and magnitudes of potential radiological source terms.

> A *radiological source term* defines the radionuclide inventory that is released to the environment. Also included in the source term are the elevation, energy, and timing of the release.

The Level 3 PRA estimates the potential health and economic consequences associated with the source terms from the Level 2 PRA. Weather characteristics, plume dispersion, population concentrations, evacuation and sheltering are accounted for in such estimates. From the Level 3 PRA the consequence-weighted risks of early fatalities, latent cancers, and other health and economic consequences are estimated.

2.6.2 NUREG-1150

NUREG-1150, which was published in December 1990, documents the results of an extensive NRC-sponsored PRA.[1] The five nuclear power plants analyzed in NUREG-1150 are:

- Unit 1 of the Surry Power Station, a Westinghouse-designed three-loop reactor in a subatmospheric containment building, located near Williamsburg, Virginia.
- Unit 1 of the Zion Nuclear Power Plant, a Westinghouse-designed four-loop reactor in a large, dry containment building, located near Chicago, Illinois.
- Unit 1 of the Sequoyah Nuclear Power Plant, a Westinghouse-designed four-loop reactor in an ice condenser containment building, located near Chattanooga, Tennessee;
- Unit 2 of the Peach Bottom Atomic Power Station, a General Electric-designed BWR-4 reactor in a Mark I containment building, located near Lancaster, Pennsylvania;
- Unit 1 of the Grand Gulf Nuclear Station, a General Electric-designed BWR-6 reactor in

a Mark III containment building, located near Vicksburg, Mississippi.

A Level 3 PRA was performed for each of these plants. Variations in scope among the five studies will be discussed later. The NUREG-1150 study can be considered as a replacement to the Reactor Safety Study. As we proceed through the remainder of Section 2.6, the results and insights of NUREG-1150 will be presented within the context of current PRA methods.

2.6.3 Analysis of Initiating Events

The first step in performing a PRA is to identify possible initiating events and determine their frequencies. Section 2.2 described possible initiating events that could lead to core damage. Risk assessment methodologies have strengths and limitations that depend on the type of initiator considered. These strengths and limitations should be understood if PRA results are to be properly interpreted and employed in making regulatory or non-regulatory decisions.

Section 2.2 identified both traditional in-plant (internal) initiators, such as LOCAs, and external initiators, such as earthquakes and tornadoes. Internal initiators usually receive the most attention in PRAs, and their frequencies are generally less difficult to estimate than the frequencies of external initiators.[3] Internal initiators are based on both historical data and engineering analyses. Tables 2.2-1 and 2.2-2 presented lists of transient initiators for BWRs and PWRs. Table 2.6-2 presents those initiators along with some generic frequencies of occurrence. Generic frequencies are obtained by averaging over groups of plants and, thus, may not be accurate for a particular plant. Generic frequencies were used as a starting point in NUREG-1150. In Table 2.6-2 initiators requiring similar plant responses are grouped together. A set of internal initiating event groups and their frequencies for one of the NUREG-1150 plants is shown in Table 2.6-3. Initiating events not shown in this table, such as Reactor Vessel Rupture, were screened out of the study, based on low probability. More detail concerning the information in Tables 2.6-2 and 2.6-3 may be found in NUREG/CR-4550,[4] which is one of the supporting documents for NUREG-1150.

In addition to the traditional in-plant (internal) initiators discussed above, there are external initiators that can occur with variable magnitudes. Hazard analyses are performed to assess the likelihood of such events as functions of their magnitudes. Such analyses may indicate that the risk contribution of some initiators is clearly negligible. For example, the frequency of aircraft-impact damage to any one of the vulnerable structures whose failure could lead to core melt is often found to be much lower (e.g., by a factor of 100) than the frequency of other large external events, such as earthquakes. (If the consequences of severe accidents induced by aircraft impact are comparable to those for severe accidents induced by more likely external events, then detailed assessments of aircraft-impact accidents may be unnecessary.) Some unique characteristics of particular initiators are discussed in more detail below.

2.6.3.1 Internal Fires

Fire in a nuclear power plant can initiate potential core damage accidents by rendering vital plant equipment inoperable. For example, the Browns Ferry fire, which is discussed in Section 2.3, damaged electrical cables and other components, thus disabling systems that would normally be used to cool the core. The term internal fire is used to denote any fire originating within the plant (including outdoor equipment such as high voltage transformers). Causes can include equipment malfunctions and human errors. Fire initiating event frequencies are based on the historical frequency of occurrence of fires and the locations and quantities of combustible materials. The characteristics of the combustible material will determine the rate at which the fire can spread and propagate heat and smoke to undesired locations.

It is important to note that fires can be significant contributors to plant risk despite regulations, such as 10 CFR 50, Appendix R. Regulations can significantly reduce risk, but can not eliminate it entirely. Compliance with Appendix R can not prevent all fires from occurring; nor can it prevent all possible combinations of equipment failures and human errors, given a fire.

2.6.3.2 Seismic Events

Although the Reactor Safety Study concluded in 1975 that seismic events represented a very minor contributor to accident risk from a nuclear reactor, ensuing developments have led to a strong case that the seismic contributions to risk from LWRs are appreciable. The difficulty in predicting seismic risks lies in predicting the frequency with which seismic events of various magnitudes occur. Section 2.2 pointed out the significance of different earthquake levels and their impact on needed plant response.

The probabilistic expression of the frequency and magnitude of seismic events is known as the seismic hazard curve and is usually expressed in terms of the annual frequency of exceedance (the probability per year of a seismic event at least as large as a stated ground acceleration). Data on the frequencies of small seismic events in seismically active regions is easy to obtain, but data is sparse for very large seismic events. The recorded earthquake history in the Eastern U.S. goes back only about 200 years.

Estimates of ground accelerations for such earthquakes must be based on observations of existing fault lengths (both active and inactive) and relationships between fault lengths and earthquake magnitudes. This results in significant uncertainty in the frequency of high magnitude (once in 100 to 100,000 years) seismic events. Furthermore, there is currently some controversy as to the interpretation of recorded earthquake motions in the Eastern U.S. The uncertainties in the hazard curve are represented by developing a family of curves with a probability assigned to each curve such that the summation of probabilities over the family of curves is unity. Figures 2.6-2 and 2.6-3 present two markedly different families of hazard curves for the Peach Bottom site.[1] This controversy is the subject of ongoing research and may take many years to resolve.

2.6.3.3 Weather-Related Events

Severe weather such as hurricanes, tornadoes, high winds, and floods can cause the loss of offsite power or, if they exceed plant design bases, cause damage to safety-related structures and equipment. Frequencies of severe weather initiators are difficult to estimate, because it is hard to predict how severe the weather could get at any plant location with a frequency of once in 100 to 100,000 years. In fact, significant climatic changes have occurred during such time spans, so even if one could examine accurate weather data for the past 100,000 years, there would still be significant uncertainty as to whether the probabilities developed from that data would be truly applicable to the next fifty or so years.

Fortunately, the most severe weather is often very localized, so it is possible to examine the worst known storm near the reactor facility and use geometrical arguments to determine an estimate of the probability that the reactor site itself might be affected. Normally, a bounding analysis of that probability is sufficient to screen out most severe weather events from further consideration. The loss of offsite power as a result of severe weather is generally included in the overall loss of offsite power frequency (included in the internal events analysis). If any particular severe weather events can not be screened out based on low frequency, then analyses of plant response are performed during the accident sequence development phase of the PRA.

2.6.3.4 Other Naturally Occurring External Events

A number of other naturally occurring phenomena could conceivably cause damage to a nuclear power plant and initiate a core damage accident. These include volcanic activity, lightning, avalanche, landslide, fog, drought, forest fire, sand storm, high tide, seiche, tsunami, low lake or river level, meteor impact, and soil shifting. Most of these events either are not applicable to a particular site, are predictable, develop very slowly (and, hence, provide much time for corrective actions), or can be analyzed using "worst case" bounding analyses to demonstrate they pose negligible risks. Those that can not be dismissed should be included in the accident sequence analysis.

2.6.3.5 Human-Caused External Initiators

As discussed in Section 2.2, external events include not only naturally occurring phenomena, but also unintentional human-caused events, such as pipeline and transportation accidents. Like many of the naturally occurring external events, many of these events either are not applicable to a particular site, are predictable, develop very slowly (and, hence, provide much time for corrective actions), or can be analyzed using "worst case" bounding analyses to demonstrate they pose negligible risks. These types of events are inherently better understood than the naturally occurring external events because there is a theoretical upper bound to the magnitude of the human-caused initiating event (e.g., it is difficult to postulate the magnitude of the most severe credible earthquake, but the type and severity of a nearby industrial or transportation accident is limited by the types of industries and transportation facilities that exist near the reactor site). Furthermore, there is a large body of information available about these types of accidents that is directly applicable to the facilities near the reactor site. Those that cannot be handled through bounding analyses should be included in the accident sequence analysis.

2.6.3.6 Accidents at Low Power and Shutdown

Section 2.2 described many of the important features of accidents occurring at low power and shutdown. Many of the initiating events that can occur at full power can also occur at low power and shutdown. The frequencies of some events, such as earthquakes or loss of offsite power, are not affected by the particular operating mode of the plant. Other events, such as LOCAs, can occur at either full power or shutdown, but at different frequencies due to the different plant state (pipe breaks are less likely at shutdown due to lower reactor coolant pressure). Some full power events, such as a turbine trip, can not occur at shutdown, while other initiating events, such as loss of Residual Heat Removal or some types of maintenance errors, can only occur at shutdown. Overall, there tend to be more categories of initiating events to consider at low power and shutdown than at full power. Table 2.6-4 presents initiating event frequencies for the Grand Gulf plant while in Plant Operation State 5[5], which basically includes the Cold Shutdown Mode of Operation. These frequencies are per year of operation in POS 5.

2.6.3.7 Sabotage

Sabotage can involve a wide variety of different types of initiating events, depending upon the particular scenarios followed by the saboteurs. All of these threats, especially insider threats, are well-known to security analysts. However, because acts of sabotage are related to the human will to cause damage, they are extraordinarily complex to analyze from a probabilistic perspective.

Although it is generally accepted that the frequency of sabotage threats decreases as their severity increases, attempts to develop a sabotage "hazard curve" have been unsuccessful. Such a curve would have to account for political conditions both in the U.S. and internationally, interpersonal relationships of plant employees, their families and friends, and other intangible considerations. In short, it is not currently feasible to make useful and defensible estimates of public risks associated with sabotage of nuclear or non-nuclear facilities.

The current methodology for assessing the security of nuclear facilities involves demonstrating that a large set of postulated design basis threats to the facility can be repelled reliably. These design basis threats are analyzed without regard to their probability of occurrence, although they are selected based on current knowledge of real threats.

2.6.4 Accident Sequence Development

2.6.4.1 Accident Delineation

The identification of accidents leading to core damage is undertaken by the use of *event trees*. An event tree is developed for each initiating event or group of similar initiating events. The questions asked at the top of an event tree usually concern the success or failure of front line systems that may be used to prevent core damage. The accident initiator and the system success/failure questions are diagrammed sequentially in the order that they affect the course of the accident. The tree branches at points where the systems either succeed or fail in their functions.

Actual event trees can be very complex and involve hundreds of possible accident sequences; however, the event tree process can be illustrated by the simple example shown in Figure 2.6-4. Consider a LOCA initiated by a small pipe break (event S2). In such an accident, the front-line systems that should automatically respond to prevent core damage are the reactor protection system (RPS) and the High Pressure Injection System (HPI). Proper operation of these two systems constitutes a success path through the event tree because core damage would be prevented. There are, of course, other success paths. For example, if the RPS succeeds but HPI fails, core damage can still be prevented if both the Automatic Depressurization System (ADS) and the Low Pressure Injection System (LPS) function. Note that some illogical branches have been eliminated in Figure 2.6-4. For example, if high pressure injection and automatic depressurization both fail, then low pressure injection is not possible and does not affect the outcome.

The frequency associated with any particular outcome of the event tree is the product of the initiating event frequency and the successive, often dependent success or failure probabilities at each branch. For example, the risk of core damage due to an accident initiated by a small LOCA (S2) and compounded by failure of both High Pressure Injection (fHPI) and Automatic Depressurization (FADS) is

$$F_{S2} * [1-P_{fRPS|S2}] * P_{FHPI|S2,RPS} * P_{fADS|S2,RPS,fHPI}$$

Here

F_{S2} is the frequency of small LOCAs per reactor year,

$P_{fRPS|S2}$ is the probability RPS fails given an S2 initiator,

$P_{fHPI|S2,RPS}$ is the probability HPI fails given an S2 initiator and RPS success,

$P_{fADS|S2,RPS,fHPI}$ is the probability ADS fails given an S2 initiator, RPS success, and HPI failure.

For nuclear power plants, system failure probabilities are generally small, much smaller than unity; hence, success probabilities like ($1-p_{fRPSIS2}$) are essentially equal to one.

The fact that system failure probabilities are small is, of course, desirable; however, it also means that there is little data available to directly quantify the failure probabilities of such systems. Instead, a logical model for each system must be developed to express the system's failure probability as a function of the failure probabilities of its components and supporting systems. Such logical models are developed through the use of *fault trees*.

For a particular event called the top event (usually a failure of a system to perform some intended function), a fault tree is used to identify the combinations of base events (usually component failures or operator errors) that could lead to the top event. An example is shown in Figure 2.6-5, which is a fault tree for a hypothetical, one-pump injection system. The symbols used in fault trees originate from the logical operations **OR** (+) and **AND** (*). For the example, insufficient system flow could result from a failure to actuate the injection system **OR** from insufficient flow from the pump. The actuation failure requires both that the automatic actuation signal fail **AND** that the operator fail to actuate the system manually. Insufficient flow from the pump can be caused by any of the failure events listed under the corresponding **OR** gate. Note that one of these events, failure of power to the pump, is based on another fault tree for the power system, which is a support system for the injection system.

Figure 2.6-5 is a very simple example. Fault trees for actual nuclear power plant systems commonly involve hundreds of logic gates and hundreds of base events. Nevertheless, Figure 2.6-5 can be used to illustrate the process undertaken to solve fault trees and event trees. The first step is to find the minimal combinations of events that lead to system failure. These are called minimal cut sets for the system. For the example depicted in Figure 2.6-5, any of the failure events under the bottom **OR** gate would result in insufficient flow from the pump and hence system failure. System failure due to actuation failure requires both events under the **AND** gate on the left hand side. Hence, in Boolean logic notation, the injection system failure (ISF) is given by a sum over 6 cut sets:

$$ISF = ASF*OFA + VFO + POM + PFS + PFR + PFF$$

The first five cut sets on the right hand side are minimal cut sets because the base events they contain (taken alone or in combination with other failures) lead to core damage. The single event PFF in the last term on the right hand side, failure of power to the pump (PFF), is not a base event and would have to be expressed in terms of minimal cut sets for the power system. Of course, some of the "base events" in the above expression, in particular event ASF, could have been modeled in more detail. After determining the minimal cut sets for each of the front line systems depicted on an accident event tree, the logical expression for any path through the event tree is simply the logical **AND** of all system failures along the path. Computer codes are used to perform such logical substitutions. Repeated events and duplicate cut sets are subsumed in this process, and low probability cut sets may be deleted. The results of the solution process are the minimal cut sets associated with each path leading to core damage.

2.6.4.2 Special Analysis Topics

As noted in Section 2.2.3, most core damage accidents involve multiple failures. Fault trees provide a systematic approach for identifying many of these failures. Most multiple independent failures and explicitly dependent failures, such as support system dependencies and shared equipment dependencies (see Section 2.2.3.2), are readily identified. However, some types of events that can lead to multiple failures are not straightforward to model and require special treatment in order to determine their frequencies. The following subsections address some of those failure types.

Common Cause Failures

Common cause failures are described in Section 2.2.3.4 as simultaneous failures of multiple components due to some underlying common cause, such as design errors or environmental factors. Common cause events can be placed directly on fault trees for analysis. Engineering judgment is used to determine which common cause events are important enough to include. It is not possible to include all conceivable combinations of common cause events due to the number of components involved. For example, the number of combinations of motor-operated valves in a plant that could fail from a common cause is almost endless. Standard practice is to consider common cause combinations across multiple trains of single systems, but with a few exceptions not across multiple systems.

Plant specific data for common cause phenomena are scarce; therefore, industry wide data and compilations of generic data must be used to quantify common cause failure probabilities. One method of common cause probability estimation involves the use of so-called beta factors that are estimated from such industry wide data. A beta factor is the conditional probability of a component failure given that a similar component has failed. Typical values for beta factors range between 0.01 and 0.1, depending upon the type of component involved.

Consider a simple example involving two identical components in different trains of a two train system. If the independent failure probability of each component is 0.01, then the probability of both components failing simultaneously is 10^{-4}. However, if the common cause beta factor for components of this type is 0.1, then the probability of both components failing due to a common cause is 10^{-3}, which is an order of magnitude higher than the independent failure probability. Normally, the common cause failure rate for multiple components will be significantly higher than the independent failure rate, and common cause failures are usually significant in the final PRA results.

Human Factors, Heroic Acts, Errors of Commission

Human factors analyses are incorporated into current, state-of-the-art PRA studies to model the failure of operators to follow written procedures under normal-operating and accident conditions. These acts can be included in fault trees or incorporated into the cut set results. Probabilities for these events are relatively easy to determine, although there is significant uncertainty. Also, the effects of such failures can be identified by tracing the reactor systems and examining the written procedures. As discussed in Section 2.2.3.3, it is infinitely more difficult, however, to model cases where the operators "think for themselves" and/or intentionally violate written procedures by undertaking actions that they believe will aid in achieving a desired plant condition. Such acts may indeed improve the situation (see discussion of Davis Besse loss of feedwater event in Appendix 2A) in which case they are defined in PRAs as *heroic acts*. Frequently, however, such independent acts initiate or exacerbate accidents, in which case they are called *errors of commission*. Both the Three Mile Island (Section 2.4) and Chernobyl (Section 2.5) nuclear accidents were exacerbated by such errors of commission. No PRA would have considered the possibility that a licensed reactor operator would actually turn the emergency core cooling system off during a loss of coolant accident, yet that occurred at Three Mile Island. Similarly, operators are not expected to disable large numbers of safety related systems in violation of technical specifications, yet this was done at Chernobyl. Thus, human errors of commission may be very significant to actual risks, yet at present there is no comprehensive method by which such actions can be examined as part of a probabilistic risk assessment.

2.6.5 NUREG-1150 Internal Event Frequencies

The internal-event core damage frequency distributions from NUREG-1150 are included as Figure 2.6-6.[1] The bars in Figure 2.6-6 show the 90 percent uncertainty ranges along with the mean and median values. The interpretation of these uncertainty bars will be discussed further in Section 2.6.9.

Figure 2.6-6 reflects core damage frequencies that are relatively low. Except for a particular sequence involving component cooling water at Zion (and which is being fixed), there are no serious vulnerabilities that yield unusually high risk. This is due in part to good design and operating procedures. It is also due to the fact that these plants have been studied before and previously identified vulnerabilities have been fixed. Plants undergoing a PRA for the first time may yield higher core damage frequencies than the NUREG-1150 plants.

2.6.5.1 Dominant Contributors to Core Damage Frequency

The various accident sequences that contribute to the core damage frequency can be grouped by common factors into categories. NUREG-1150 uses the accident categories depicted in Figures 2.6-7 and 2.6-8: station blackout, anticipated transients without scram, other transients, reactor coolant pump seal LOCAs, interfacing system LOCAs, and other LOCAs. The selection of such categories is not unique, but merely a convenient way to group the results.

The existence of a highly dominant accident sequence does not of itself imply that a safety problem exists. For example, if a plant has an extremely low estimated core damage frequency, the existence of a single dominant accident sequence would have little significance. Similarly, if a plant was modified to eliminate the dominant accident sequence, another accident sequence or group of accident sequences would become dominant.

Nevertheless, the identification of dominant accident sequences and the failures that contribute to those sequences provide understanding of why the core damage frequency is high or low relative to other plants and desired goals. This qualitative understanding of the core damage frequency is necessary to make practical use of the PRA results and improve the plants, if necessary.

2.6.5.2 BWR versus PWR Plants

It is evident from Figure 2.6-6 that the BWRs in NUREG-1150 have core damage frequencies that are lower than those of the three PWRs. It would be inappropriate to conclude that all BWRs have lower core damage frequencies than PWRs; however, it is instructive to consider reasons for the NUREG-1150 result.

The LOCA sequences, which often dominate the PWR core damage frequencies, are minor contributors for the BWRs. This is not surprising because BWRs have many more systems than PWRs for injecting water into the reactor coolant system. For many transients, the same argument holds. BWRs have many more systems that can provide decay heat removal and makeup for transients that lead to loss of water inventory due to stuck-open relief valves or primary system leakage.

BWRs have historically been considered more subject than PWRs to ATWS events. This is partly due to the fact that some ATWS events in BWRs involve an insertion of positive reactivity. However, Figures 2.6-7 and 2.6-8 indicate that ATWS frequencies for the two BWRs are comparable to those for the three PWRs. There are several reasons for this. First, plant procedures for dealing with ATWS events have been modified over the past several years, and operator training specifically for these events has improved significantly. Second, the ability to model and analyze ATWS events have improved and indicate lower core power levels during ATWS accidents than predicted in the past. Further, these calculations indicate that low-pressure injection systems can be used without resulting in significant power oscillations. Note that for both BWRs and PWRs the frequency of reactor protection system failures remains highly uncertain. Therefore, all comparisons concerning ATWS accidents should be made with caution.

Station blackout accidents contribute a high percentage of the core damage frequency for the BWRs. However, when viewed on an absolute scale, station blackout has a higher frequency at the PWRs than at the BWRs. To some extent this is due to design differences between BWRs and PWRs. For example, in station blackout accidents, PWRs are potentially vulnerable to reactor coolant pump seal LOCAs following loss of seal cooling, leading to loss of inventory with no method for providing makeup. BWRs, on the other hand, have at least one injection system that does not require ac power. While such BWR and PWR design features influence the core damage frequencies associated with station blackout, the electric power system design, which is largely independent of the plant type, is probably more important. The station blackout frequency is low at Peach Bottom because of the presence of four diesels that can be shared between units and a maintenance program that led to an order of magnitude reduction in the diesel generator failure rates. Grand Gulf has essentially three trains of emergency ac power for one unit, with one of the trains being both diverse and independent from the other two. These characteristics of the electric power system design tend to dominate any differences in the NSSS design. Therefore, a BWR with a below average electric power system reliability could be expected to have a higher station blackout-induced core damage frequency than a PWR with an above average electric power system.

Along with electric power, NUREG-1150 analyses indicate that for both BWRs and PWRs other support systems, such as service water, are also quite important. Because support systems vary considerably among plants, caution must be exercised when making statements about generic classes of plants, such as PWRs versus BWRs. Once significant plant-specific vulnerabilities are removed, support-system-driven sequences will probably dominate the core damage frequencies of both types of plants. Both types of plants have sufficient redundancy and diversity so as to make multiple independent failures unlikely. Support system failures introduce dependencies among the systems and thus can become dominant.

2.6.5.3 Boiling Water Reactor Observations

As shown in Figure 2.6-6, the internal-event core damage frequencies for Peach Bottom and Grand Gulf are extremely low. Therefore, even though dominant accident sequences and contributing failure events can be identified, these items should not be considered as safety problems for the two plants. In fact, these dominating factors should not be overemphasized because, for core damage frequencies below 1E-05, it is possible that other events outside the scope of these internal-event analyses are the ones that actually dominate. In the cases of these two plants, the real perspectives come not from understanding why particular sequences dominate, but rather why all types of sequences considered in NUREG-1150 have low frequencies for these plants.

Previously it was noted that LOCA sequences can be expected to have low frequencies at BWRs because of the numerous systems available to provide coolant injection. While low for both plants, the frequency of LOCAs is higher for Peach Bottom than for Grand Gulf. This is primarily because Grand Gulf is a BWR-6 design with a motor-driven high-pressure core spray system, rather than a steam-driven high-pressure coolant injection system as is Peach Bottom. Motor-driven systems are typically more reliable than steam-driven systems and, more importantly, can operate over the entire range of pressures experienced in a LOCA sequence.

It is evident from Figure 2.6-7 and 2.6-8 that station blackout plays a major role in the internal-event core damage frequencies for Peach Bottom and Grand Gulf. Each of these plants has features that tend to reduce the station blackout frequency, some of which would not be present at other BWRs.

Grand Gulf, like all BWR-6 plants, is equipped with an extra diesel generator dedicated to the high-pressure core spray system. While effectively providing a third train of redundant emergency ac power for decay heat removal, the extra diesel also provides diversity, based on a different diesel design and plant location relative to the other two diesels. This results in a low probability of common-cause failures affecting all three diesel generators. The net effect is a highly reliable emergency ac power capability. In those unlikely cases where all three diesel generators fail, Grand Gulf relies on a steam-driven coolant injection system that can function until the station batteries are depleted. At Grand Gulf the batteries are sized to last for many hours prior to depletion so that there is a high probability of recovering ac power prior to core damage. In addition, there is a diesel-driven firewater system available that can be used to provide coolant injection in some sequences involving the loss of ac power.

Peach Bottom is an older model BWR that does not have a diverse diesel generator for the high-pressure core spray system. However, other factors contribute to a low station blackout frequency at Peach Bottom. Peach Bottom is a two-unit site, with four diesel generators available. Any one of the four diesels can provide sufficient capacity to power both units in the event of a loss of offsite power, given that appropriate crossties or load swapping between Units 2 and 3 are used. This high level of redundancy is somewhat offset by a less redundant service water system that provides cooling to the diesel generators. Subtleties in the design are such that if a certain combination of diesel generators fails, the service water system will fail, causing the other diesels to fail. In addition, station dc power is needed to start the diesels. (Some emergency diesel generator systems, such as those at Surry, have a separate dedicated dc power system just for starting purposes.) In spite of these factors, the redundancy in the Peach Bottom emergency ac power system is considerable.

While there is redundancy in the ac power system design at Peach Bottom, a more significant factor is a high-quality diesel generator maintenance program. Plant-specific data analysis determined that the diesel generators at Peach Bottom were an order of magnitude more reliable than at an average plant.

Finally, Peach Bottom, like Grand Gulf, has station batteries that are sized to last several hours in the event that the diesel generators do fail. With two steam-driven systems to provide coolant injection and several hours to recover ac power prior to battery depletion, the station blackout frequency is further reduced.

Unlike most PWRs, the response of containment is often a key in determining the core damage frequency for BWRs. For example, at Peach Bottom, there are a number of ways in which containment conditions can affect coolant injection systems. High pressure in containment can lead to closure of primary system relief valves, thus failing low-pressure injection systems, and can also lead to failure of steam-driven high-pressure injection systems due to high turbine exhaust backpressure. High suppression pool temperatures can also lead to the failure of systems that are recirculating water from the suppression pool to the reactor coolant system. If the containment ultimately fails, certain systems can fail because of the loss of net positive suction head in the suppression pool, and also the reactor building is subjected to a harsh steam environment that can lead to failure of equipment located there.

Despite the concerns described in the previous paragraph, the core damage frequency for Peach Bottom is relatively low, compared to the PWRs. There are two major reasons for this. First, Peach Bottom has the ability to vent the wetwell through a 6-inch diameter steel pipe, thus reducing the containment pressure without subjecting the reactor building to steam. While this vent cannot be used to mitigate ATWS and station blackout sequences, it is valuable in reducing the frequency of many other sequences. The second important feature at Peach Bottom is the presence of the control rod drive cooling system, which is not affected by either high pressure in containment or containment failure. Other plants of the BWR-4 and BWR-5 designs are potentially vulnerable to containment-related problems. As a result, the NRC has negotiated changes to containment venting for BWR-4 plants. These changes are discussed further in Module 4.

The Grand Gulf design is generally much less susceptible to containment-related problems than Peach Bottom. The containment design and equipment locations are such that containment rupture will not result in discharge of steam into the building containing the safety systems. Further, the high-pressure core spray system is designed to function with a saturated suppression pool so that it is not affected by containment failure. Finally, there are other systems that can provide coolant injection using water sources other than the suppression pool. Thus, containment failure is relatively benign as far as system operation is concerned, and there is no obvious need for containment venting.

2.6.5.4 Pressurized Water Reactor Observations

The three PWRs examined in NUREG-1150 reflect much more variety in terms of dominant accident sequences than the BWRs. While the sequence frequencies are generally low, it is useful to understand why the variations among the plants occurred.

For LOCA sequences, the frequency is significantly lower at Surry than at the other two PWRs. A major portion of this difference is directly tied to the additional redundancy available in the injection systems. In addition to the normal high-pressure injection capability, Surry can crosstie to the other unit at the site for an additional source of high-pressure injection. This reduces the core damage frequency due to LOCAs and also certain groups of transients involving stuck-open relief valves.

In addition, at Sequoyah there is a particularly noteworthy emergency core cooling interaction with containment engineered safety features in loss-of-coolant accidents. In this (ice condenser) containment design, the containment sprays are automatically actuated at a very low pressure setpoint, which would be exceeded for virtually all small LOCA events. This spray actuation, if not terminated by the operator, can lead to a rapid depletion of the refueling water storage tank at Sequoyah. Thus, an early need to switch to recirculation cooling may occur. Portions of this switchover process are manual at Sequoyah and, because of the timing and possible stressful conditions, lead to a significant human error probability. Thus, LOCA-type sequences are the dominant accident sequence type at Sequoyah.

Station blackout-type sequences have relatively similar frequencies at all three PWRs. Station blackout sequences can have very different characteristics at PWRs than at BWRs. One of the most important findings of NUREG-1150 is the importance of reactor coolant pump seal failures. During station blackout, all cooling to the seals is lost and there is a significant probability that they will ultimately fail, leading to an induced LOCA and loss of inventory. Because PWRs do not have systems capable of providing coolant makeup without ac power, core damage will result if power is not restored. The seal LOCA reduces the time available to restore power and thus increases the station blackout-induced core damage frequency. New seals have been proposed for Westinghouse PWRs and could reduce the core damage frequency if implemented, although they might also increase the likelihood that any resulting accidents would occur at high pressure, which has implications for the accident progression analysis.

Apart from the generic reactor coolant pump seal question, station blackout frequencies at PWRs are determined by the plant-specific electric power system design and the design of other support systems. Battery depletion times for the three PWRs were projected to be shorter than for the two BWRs. A particular characteristic of the Surry plant is a gravity-fed service water system with a canal that may drain during station blackout, thus failing containment heat removal. When power is restored, the canal must be refilled before containment heat removal can be restored.

The dominant accident sequence type at Zion is not a station blackout, but it has many similar characteristics. Component cooling water is needed for operation of the charging pumps and high-pressure safety injection pumps at Zion. Loss of component cooling water (or loss of service water, which will also render component cooling water inoperable) will result in loss of these high-pressure systems. This in turn leads to a loss of reactor coolant pump seal injection. Simultaneously, loss of component cooling water will also result in loss of cooling to the thermal barrier heat exchangers for the reactor coolant pump seals. Thus, the reactor coolant pump seals will lose both forms of cooling. As with station blackout, loss of component cooling water or service water can both cause a small LOCA (by seal failure) and disable the systems needed to mitigate it. The importance of this scenario is increased further by the fact that the component cooling water system at Zion, although it uses redundant pumps and valves, delivers its flow through a common header. The licensee for the Zion plant has made procedural changes and is also considering both the use of new seal materials and the installation of modifications to the cooling water systems.

ATWS frequencies are generally low at all three of the PWRs. This is due to the assessed reliability of the shutdown systems and the likelihood that only slow-acting, low-power-level events will result. While of low frequency, it is worth noting that interfacing-system LOCA (V) and steam generator tube rupture (SGTR) events do contribute significantly to risk for the PWRs. This is because they involve a direct path for fission products to bypass containment. There are large uncertainties in the analyses of these two accident types, but these events can be important to risk even at frequencies that may be one or two orders of magnitude lower than other sequence types.

During the past few years, most Westinghouse PWRs have developed procedures for using feed and bleed cooling and secondary system blowdown to cope with loss of all feedwater. These procedures have led to substantial reductions in the frequencies of transient core damage sequences involving the loss of main and auxiliary feedwater. Appropriate credit for these actions was given in these analyses. However, there are plant-specific features that will affect the success rate of such actions. For example, the loss of certain power sources (possibly only one bus) or other support systems can fail power-operated relief valves (PORVs) or atmospheric dump valves or their block valves at some plants, precluding the use of feed and bleed or secondary system blowdown. Plants with PORVs that tend to leak may operate for significant periods of time with the block valves closed, thus making feed and bleed less reliable. On the other hand, if certain power failures are such that open block valves cannot be closed, then they cannot be used to mitigate stuck-open PORVs. Thus, both the system design and plant operating practices can be important to the reliability assessment of actions such as feed and bleed cooling.

2.6.6 External Events and Fire Analyses

External events and fires require additional steps in both the initiating event and accident sequence analysis portions of a PRA. A key reason for the differences is that the initiating events can have variable magnitude. As indicated in Figure 2.6-9, the basic steps in the analysis of risks from variable magnitude initiating event like earthquakes, are (1) hazard analysis, (2) plant-system and structure response analysis, (3) evaluation of the fragility and vulnerability of components (structures, piping, and equipment), (4) accident sequence development, and (5) consequence analysis. Section 2.6.3 discussed the development of hazard curves, and consequence analysis is discussed in Module 5. The other steps are discussed briefly below.

In the response analysis, the response of plant systems and structures for a specified hazard input level is calculated. The response of interest is often the structural response at selected structural, piping, and equipment locations. For earthquakes, the response parameters could be spectral acceleration, moment, and deflection. For extreme winds, they could be force or moment on a structural element and deflection. For fires, thermal response and smoke accumulation are of interest.

The fragility of a component is the conditional failure frequency for a given value of a response parameter. The first step in generating fragility curves is a clear definition of what constitutes failure for each component. This failure criterion is calculated by an analysis of the parameter of interest, such as a structural or thermal failure threshold. Uncertainties in the component-fragility are represented by developing a family of fragility curves for each component. The sum of the probabilities assigned over a family of fragility curves is unity.

Accident-sequence development was discussed in Section 2.6.4. The major differences in this step for external events as contrasted with traditional internal events are the addition of external event-caused failures to the fault trees and the increased likelihood of multiple failures of safety systems due to correlations between component responses and between component capacities. There are additional considerations when determining core damage frequencies associated with fires. These considerations include the availability and effectiveness of automatic and manual fire suppression, and the locations of vital equipment with respect to potential fires. Coincident failures of fire protection systems and other systems are also considered. Only a small fraction of the fires that could occur in a nuclear power plant would be expected to lead to core damage.

2.6.7 External Events in NUREG-1150

The frequency of core damage initiated by external events has been analyzed for two of the plants in NUREG-1150, Surry and Peach Bottom. The analysis examined a broad range of external events (e.g., lightning, aircraft impact, tornadoes, and volcanic activity). Most of these events were assessed to be insignificant contributors by means of bounding analyses. However, seismic events and fires were found to be potentially major contributors and thus were analyzed in detail.

Figures 2.6-10 and 2.6-11 show the results of the core damage frequency analysis for seismic- and fire-initiated accidents, as well as internally initiated accidents, for Surry and Peach Bottom, respectively. Examination of these figures shows that the core damage frequency distributions of the external events are comparable to those of the internal events. It is evident that the external events are significant in the total safety profile of these plants.

2.6.7.1 NUREG-1150 Seismic Analysis Observations

The analysis of the seismically induced core damage frequency begins with the estimation of the seismic hazard, that is, the likelihood of exceeding different earthquake ground-motion levels at the plant site. As discussed in Section 2.2, the sciences of geology and seismology have not yet produced a model or group of models upon which all experts agree. NUREG-1150 used seismic hazard curves for Peach Bottom and Surry that were part of an NRC-funded Lawrence Livermore National Laboratory project that resulted in seismic hazard curves for all nuclear power plant sites east of the Rocky Mountains.[6] For purposes of completeness and comparison, the seismically induced core damage frequencies were also calculated based upon a separate set of seismic hazard curves developed by the Electric Power Research Institute (EPRI).[7] Both sets of results are presented in Figures 2.6-10 through 2.6-13.

As can be seen in Figures 2.6-12 and 2.6-13, the shapes of the seismically induced core damage probability distributions are considerably different from those of the internally initiated and fire-initiated events. In particular, the 5th to 95th percentile range is much larger for the seismic events. In addition, as can be seen in Figures 2.6-10 and 2.6-11, the wide disparity between the mean and the median and the location of the mean relatively high in the distribution indicate a wide distribution with a tail at the high end but peaked much lower down. This is a result of the uncertainty in the seismic hazard curve.

It can be clearly seen that the difference between the mean and median is an important distinction. The mean is the parameter quoted most often, but the bulk of the distribution is well below the mean. Thus, although the mean is the "center of gravity" of the distribution (when viewed on a linear rather than logarithmic scale), it is not very representative of the distribution as a whole. Instead, it is the lower values that are more probable. The higher values are estimated to have low probability, but, because of their great distance from the bulk of the distribution, the mean is "pulled up" to a relatively high value. In a case such as this, it is particularly evident that the entire distribution, not just a single parameter such as the mean or the median, must be considered when discussing the results of the analysis.

2.6.7.1.1 Surry Seismic Analysis

The core damage frequency probability distributions, as calculated using the Livermore and EPRI methods, have a large degree of overlap, and the differences between the means and medians of the two resulting distributions are not very meaningful because of the large widths of the two distributions.

As shown in Figure 2.6-14, the breakdown of the Surry seismic analysis into principal contributors is reasonably similar to the results of other seismic PRAs for other PWRs. The total core damage frequency is dominated by loss of offsite power transients resulting from seismically induced failures of the ceramic insulators in the switchyard. This dominant contribution of ceramic insulator failures has been found in virtually all seismic PRAs to date.

A site-specific but significant contributor to the core damage frequency at Surry is failure of the anchorage welds of the 4kV buses. These buses play a vital role in providing emergency ac electrical power since offsite power as well as emergency onsite power passes through these buses. Although these welded anchorages have more than adequate capacity at the safe shutdown earthquake (SSE) level, they do not have sufficient margin to withstand (with high reliability) earthquakes in the range of four times the SSE, which are contributing to the overall seismic core damage frequency results.

Similarly, a substantial contribution is associated with failures of the diesel generators and associated load center anchorage failures. These anchorages also may not have sufficient capacity to withstand earthquakes at levels of four times the SSE.

Another area of generic interest is the contribution due to vertical flat-bottomed storage tanks (e.g., refueling water storage tanks and condensate storage tanks). Because of the nature of their configuration and field erection practices, such tanks have often been calculated to have relatively smaller margin over the SSE than most components in commercial nuclear power plants. Given that all PWRs in the United States use the refueling water storage tank as the primary source of emergency injection water (and usually the sole source until the recirculation phase of ECCS begins), failure of the refueling water storage tank can be expected to be a substantial contributor to the seismically induced core damage frequency.

2.6.7.1.2 Peach Bottom Seismic Analysis

As can be seen in Figure 2.6-14, the dominant contributor in the seismic core damage frequency analysis is a transient sequence brought about by loss of offsite power. The loss of offsite power is due to seismically induced failures of onsite ac power. Peach Bottom has four emergency diesel generators, all shared between the two units, and four station batteries per unit. Thus, there is a high degree of redundancy. However, all diesels require cooling provided by the emergency service water system, and failure to provide this cooling will result in failure of all four diesels.

There is a variety of seismically induced equipment failures that can fail the emergency service water system and result in a station blackout. These include failure of the emergency cooling tower, failures of the 4 kV buses (in the same manner as was found at Surry), and failures of the emergency service water pumps or the emergency diesel generators themselves. The various combinations of these failures result in a large number of potential failure modes and give rise to a relatively high frequency of core damage based on station blackout. None of these equipment failure probabilities is substantially greater than would be implied by the generic fragility data available. However, the high probability of exceedance of larger earthquakes (as prescribed by the hazard curves for this site) results in significant contributions of these components to the seismic risk.

2.6.7.2 NUREG-1150 Fire Analysis Observations

The core damage likelihood due to a fire in any particular area of the plant depends upon the frequency of ignition of a fire in the area, the amount and nature of combustible material in that area, and the nature and efficacy of the fire-suppression systems in that area. In NUREG-1150, fire analyses were performed for the Surry and Peach Bottom plants.

2.6.7.2.1. Surry Fire Analysis

Figure 2.6-15 shows the dominant contributors to core damage frequency resulting from the Surry fire analysis. The dominant contributor is a transient resulting in a reactor coolant pump seal LOCA, which can lead to core damage. The scenario consists of a fire in the emergency switchgear room that damages power of control cables for the high-pressure injection and component cooling water pumps. Credit was given for existing fire-suppression systems and for recovery by crossconnecting high-pressure injection from the other unit. The most significant physical location is the emergency switchgear room. In this room, cable trays for the two redundant power trains were run one on top of the other with approximately 8 inches of vertical separation in a number of plant areas, which gives rise to the common vulnerability of these two systems due to fire. In addition, the Halon fire-suppression system in this room is manually actuated.

The other principal contributor is a spuriously actuated pressurizer PORV. In this scenario, fire-related component damage in the control room includes control power for a number of safety systems. Full credit was given for independence of the remote shutdown panel from the control room except in the case of PORV block valves. Discussions with utility personnel indicated that control power for these valves was not independently routed.

2.6.7.2.2 Peach Bottom Fire Analysis

Figure 2.6-15 shows the mechanisms by which fire leads to core damage in the Peach Bottom analysis. Station blackout accidents are the dominant contributor, with substantial contributions also coming from fire-induced transients and losses of offsite power.

Control room fires are of considerable significance in the fire analysis of this plant. Fires in the control room were divided into two scenarios, one for fires initiating in the reactor core isolation cooling (RCIC) system cabinet and one for all others. Credit was given for automatic cycling of the RCIC system unless the fire initiated within its control panel. Because of the cabinet configuration within the control room, the fire was assumed not to spread and damage any components outside the cabinet where the fire initiated. The analysis gave credit for the possibility of quick extinguishing of the fire within the applicable cabinet since the control room is continuously occupied. However, should these efforts fail, even with high ventilation rates, these scenarios postulate forced abandonment of the control room due to smoke from the fire and subsequent plant control from the remote shutdown panel.

The cable spreading room below the control room is significant but not dominant in the fire analysis. The scenario of interest is a fire-induced transient coupled with fire-related failures of the control power for the high-pressure coolant injection system, the reactor core isolation cooling system, the automatic depressurization system, and the control rod drive hydraulic system. The analysis gave credit to the automatic CO_2 fire-suppression system in this area.

The remaining physical areas of significance are the emergency switchgear rooms. The fire-induced core damage frequency is dominated by fire damage to the emergency service water system in conjunction with random failures coupled with fire-induced loss of offsite power. In all eight emergency switchgear rooms (four shared between the two units), both trains of offsite power are routed. It was noted that in each of these areas there are breaker cubicles for the 4 kV switchgear with a penetration at the top that has many small cables routed through it. These penetrations were inadequately sealed, which would allow a fire to spread to cabling that was directly above the switchgear room. This cabling was a sufficient fuel source for the fire to cause a rapid formation of a hot gas layer that would then lead to a loss of offsite power. Since both offsite power and emergency service water systems are lost, a station blackout would occur.

2.6.7.2.3 General Observations on Fire Analysis

Figures 2.6-10 and 2.6-11 clearly indicate that fire-initiated core damage sequences are significant in the total probabilistic analysis of the two plants analyzed. These analyses include credit for the fire protection programs required by Appendix R to 10 CFR Part 50.[8]

Although the two plants are of completely different design, with completely different fire-initiated core damage scenarios, the possibility of fires in the emergency switchgear areas is important in both plants. The importance of the emergency switchgear room at Surry is particularly high because of the seal LOCA scenario. Further, the importance of the control room at Surry is comparable to that of the control room at Peach Bottom.

This is not surprising in view of the potential for simultaneous failure of several systems by fires in these areas. Thus, in the past such areas have generally received particular attention in fire protection programs. It should also be noted that the significance of various areas also depends upon the scenario that leads to core damage. For example, the importance of the emergency switchgear room at Surry could be altered (if desired) not only by more fire protection programs but also by changes in the probability of the reactor coolant pump seal failure.

2.6.8 Data Analysis and Accident Precursors

The validity of PRA results is determined in part by the quality of the data that is used in the quantification. Collection and analysis of data is therefore an important part of a reactor PRA. Data needed in order to perform a core damage frequency analysis include component failure rates, test and maintenance unavailabilities, initiating event frequencies, and human error rates. When possible, it is generally best to use plant-specific data that relate to the specific components and events of interest. Possible sources of plant-specific data include:

Licensee Event Reports (LERs)
Operator/Control Room Logs
Diesel Generator Start Logs
Maintenance Work Orders
Post-Trip Analysis Reports
NRC Gray Book
Interview with Plant Personnel
Other Plant Logs and Records

In many cases, there are insufficient data from a single plant to develop reliable estimates of failure rates and other parameters. In those cases, generic data from a larger group of plants are used. Tables 2.6-5 and 2.6-6 identify sources of generic data that can be used in PRA studies. A summary compilation of this generic data is contained in Chapter 8 of NUREG/CR-4550.[4]

As noted previously in Section 2.2, the NRC collects and evaluates some data for the purpose of identifying possible severe accident precursors. When the NRC determines that a particular event, usually identified in a Licensee Event Report (LER), is worth further investigation, the Accident Sequence Precursor (ASP) Program is used to evaluate the potential core damage frequency importance of the event. The ASP program uses a simplified set of event trees for the analysis, in essence performing a mini-PRA. The intent of the program is not a high degree of accuracy, but rather, relative insights and selection of events for further NRC study. In the analysis of an event, the probabilities of failure that actually occurred are set to 1.0 and additional failure that could have led to core damage are quantified to determine how close the particular event came to core damage. Table 2.6-7 shows the results of ASP analyses of several precursor events. For example, this table indicates that the Browns Ferry Fire came closer to core damage than most other precursors.

2.6.9 Uncertainties in Risk Estimates

Proper use of PRA results generally requires an understanding of the limitations and uncertainties associated with the results. The limitations and uncertainties vary for different types of events and failures. Since the Reactor Safety Study, risk analyses have examined in detail the potential for severe accidents to be initiated by operational failures like those considered for design-basis accidents in SAR Chapter 15. Consequently, the methodology and databases for treating such accidents are better developed than for initiators requiring hazard analyses. There is substantial agreement within the risk assessment community that PRAs can determine the most likely sequences of equipment failures and operator errors of omission (failures to follow procedures in response to equipment failures) that could lead to core damage.

There is less agreement, however, on the interpretation of the absolute magnitude of the calculated core damage frequencies and other risks obtained from such PRAs. This is due to the fact that, along with statistical uncertainties associated with data collection and analysis, there are scope and methodology limitations inherent in current state of the art PRAs. For example, PRA methods are inadequate for addressing human errors of commission (see subsection 2.4.4.2), design and construction errors or the influence of plant management. Further, PRA methods are only beginning to be applied to accidents initiated at low power and shutdown. Consequently, PRAs do not (and do not claim to) represent the total public risk from the analyzed plants.

To characterize uncertainty, analysts use a distribution of possible values and discuss each risk measure in terms of the mean, median, and various percentiles of its distribution. For example, the internal-event core damage frequencies from the NRC NUREG-1150 risk assessment of five plants are shown in Figure 2.6-6. The lower and upper extremities of the bars represent the 5th and 95th percentiles of the distributions, with the mean and median of each distribution also shown. Thus, the bars include the central 90 percent of the distribution. Figure 2.6-6 shows that the range between the 5th and 95th percentile covers from one to two orders of magnitude for each of the five core damage frequencies.

As a result of the uncertainties inherent in seismic hazard curves (see Section 2.6.3.2), many risk analysts feel that estimates of seismic risks are less robust than those calculated for internal events. In this regard, the NRC is not requiring the calculation of a seismic core damage frequency as part of its ongoing Individual Plant Examination (IPE) program. Alternatively, an assessment of the margin between the plant design and the plant SSE level may be made. This margin assessment process avoids the need of developing a seismic hazard curve, although specification of the earthquake level at which the margin is to be assessed is determined by agreement between the plant utility and the NRC, and may involve probabilistic considerations. Previous PRA studies have shown the seismic margin to be considerable in that the estimated frequency of seismically induced core damage is often more that a factor of ten lower than the estimated SSE frequency.

Comparing a risk estimated for one plant to that estimated for another plant or to some absolute limit or goal is not simply a matter of comparing two numbers. It is more appropriate to observe how much of the uncertainty distribution lies below a given value, which translates into a measure of the certainty that the core damage frequency is less than the given value. For example, if the 95th percentile of core damage frequency for a given plant was 1.0×10^{-4} per reactor year, there would be only a 5% chance that the plant's true core damage frequency would exceed 1.0×10^{-4} per reactor year. Similarly, when comparing risks calculated for two or more plants, it is not sufficient to simply compare the mean values of the uncertainty distributions. Instead, entire distributions must be compared. For example, from Figure 2.6-6, one can have relatively high confidence that the internal-event core damage frequency for Grand Gulf is lower than that of Sequoyah or Surry. Conversely, differences in core damage frequency between Surry and Sequoyah are not very significant.

Table 2.6-1. Consequence Weighted Risk

Accident Scenario	Estimated Frequency (accid/yr)	Estimated Consequence (deaths/accid)	Consequence-Weighted Risk (deaths/yr)
S_1	$2.0x10^{-5}$	1	$2.0x10^{-5}$
S_2	$0.2x10^{-5}$	3	$0.6x10^{-5}$
S_3	$0.6x10^{-5}$	7	$4.2x10^{-5}$
S_4	$0.3x10^{-5}$	5	$1.5x10^{-5}$
Total	$3.1x10^{-5}$		$8.3x10^{-5}$

Table 2.6-2. Transient Initiating Event Frequencies

Reactor/Group	Table 2.2-1 or 2.2-2 Event	Initiating Event		Frequency/ Reactor Year
BWR Groups				
LOSP	31.	LOSP		0.08
	32.	Loss of auxiliary power (transformer)		0.02
			Group Total	0.10
Loss of PCS	2.	Electric load rejection with turbine bypass failure		0.004
	4.	Turbine trip with turbine bypass valve failure		0.004
	5.	MSIV closure		0.27
	6.	Inadvertent closure of one MSIV		0.21
	7.	Partial MSIV closure		0.06
	8.	Loss of condenser vacuum		0.41
	9.	Pressure regulator fails open		0.08
	10.	Pressure regulator fails closed		0.10
	12.	Turbine bypass fails open		0.04
	13.	Turbine bypass or control valves increase pressure (closed)		0.42
	37.	Cause unknown		0.06
			Group Total	1.66
IORV	11.	IORV		0.14
PCS Available	1.	Electric load rejection		0.45
	3.	Turbine trip		0.87
	14.	Recirculation control failure, increasing flow		0.18
	15.	Recirculation control failure, decreasing flow		0.05
	16.	One recirculation pump trip		0.06
	17.	Recirculation pump trip (all)		0.03
	18.	Abnormal startup of idle recirculation pump		0.02
	19.	Recirculation pump seizure		0.004
	20.	FW--increasing flow at power		0.14
	21.	Loss of FW heater		0.02
	23.	Trip of one FW or condensate pump		0.20
	27.	Rod withdrawal at power		0.01
	29.	Inadvertent insertion of rods		0.06
	30.	Detected fault in RPS		0.05
	33.	Inadvertent startup of HPCI/HPCS		0.01
	34.	Scram from plant occurrences		0.58
	35.	Spurious trip via instrumentation, RPS fault		1.11
	36.	Manual scram, no out-of-tolerance condition		0.87
			Group Total	4.71
FW Lost but Condenser Available	22.	Loss of all FW flow		0.07
	24.	FW, low flow		0.49
			Group Total	0.56

Table 2.6-2. Transient Initiating Event Frequencies (Continued)

Reactor/Group	Table 2.2-1 or 2.2-2 Event	Initiating Event	Frequency/ Reactor Year
PWR Groups			
LOSP	35.	Loss of offsite power	0.15
Loss of PCS	9.	Inadvertent safety injection signal	0.05
	16.	Total loss of FW flow (all loops)	0.16
	18.	Closure of all MSIVs	0.04
	20.	Increase in FW flow (all loops)	0.02
	21.	FW flow instability--operator error	0.29
	22.	FW flow instability--miscellaneous mechanical cause	0.34
	24.	Loss of all condensate pumps	0.01
	25.	Loss of condenser vacuum	0.14
	30.	Loss of circulating water	0.05
		Group Total	1.10
PCS Available	1.	Loss of RCS flow (one loop)	0.28
	2.	Uncontrolled rod withdrawal	0.01
	3.	CRD mechanical problems and/or rod drop	0.50
	4.	Leakage for control rods	0.02
	5.	Leakage in primary system	0.05
	6.	Low pressurizer pressure	0.03
	7.	Pressurizer leakage	0.005
	8.	High pressurizer pressure	0.03
	10.	Containment pressure problems	0.005
	11.	CVCS malfunction--boron dilution	0.03
	12.	Pressure/temperature/power imbalance--rod position error	0.13
	13.	Startup of inactive coolant pump	0.002
	14.	Total loss of RCS flow	0.03
	15.	Loss or reduction in FW flow (one loop)	1.50
	17.	Full or partial closure of MSIV (one loop)	0.17
	19.	Increase in FW flow (one loop)	0.44
	23.	Loss of condensate pumps (one loop)	0.07
	26.	Steam generator leakage	0.03
	27.	Condensate leakage	0.04
	28.	Miscellaneous leakage in secondary system	0.09
	29.	Sudden opening of steam relief valves	0.02
	33.	Turbine trip, throttle valve closure, EHC problems	1.19
	34.	Generator trip or generator caused faults	0.46
	36.	Pressurizer spray failure	0.03
	38.	Spurious trips--cause unknown	0.08
	39.	Auto trip--no transient condition	1.49
	40.	Manual trip--no transient condition	0.47
		Group Total	7.20

Table 2.6-3. Example BWR Initiating Event Frequencies

Initiator Nomenclature	Description	Mean Frequency (per year)
T1	Loss of offsite power (LOSP) transient	0.079
T2	Transient with the Power Conversion System (PCS) unavailable	0.05
T3A	Transient with the PCS initially available	2.5
T3B	Transient involving loss of feedwater (LOFW) but with the steam side of the PCS initially available	0.06
T3C	Transient due to an Inadvertent Open Relief Valve (IORV) in the primary system	0.19
TAC/x	Transient caused by loss of safety AC Bus "x"	5.0E-3
TDC/x	Transient caused by loss of safety DC Bus "x"	5.0E-3
A	Large LOCA	1.0E-4
S1	Intermediate LOCA	3.0E-4
S2	Small LOCA	3.0E-3
S3	Small-small LOCA	3.0E-2
"V"	Interfacing system LOCA	<1E-8

Table 2.6-4 Initiating Events for POS 5

Initiating Event Nomenclature	Description	Mean Frequency per Year for POS 5
T_1	Loss of Offsite Power (LOSP) Transient	0.13
A	Large LOCA at Low Pressure	3.62E-05
A_{HY}	Large LOCA during Hydro Test (High Pressure)	1.25E-04
S_1	Intermediate LOCA at Low Pressure	3.62E-05
S_{1H}	Intermediate LOCA during Hydro Test (High Pressure)	1.25E-04
S_2	Small LOCA at Low Pressure	3.62E-05
S_{2H}	Small LOCA during Hydro Test (High Pressure)	1.25E-04
S_3	Small-small LOCA at Low Pressure	3.62E-05
S_{3H}	Small-small LOCA during Hydro Test (High Pressure)	1.25E-04
H_1	Diversion to Suppression Pool via RHR	6.1E-02
J_2	LOCA in connected system (RHR)	1.56E-02
E_{1B}	Isolation of SDC loop B only	5.7E-02
E_{1C}	Isolation of RWCU as DHR	1.57E-03
E_{1D}	Isolation of ADHRS only	5.7E-02
E_{1T}	Isolation of SDC common suction line	0.356
E_{1V}	Isolation of common suction line for ADHRS	0.356
E_{2B}	Loss of operating RHR shutdown system	6.5E-02
E_{2C}	Loss of RWCU as DHR	1.57E-03
E_{2D}	Loss of ADHRS only	6.5E-02
E_{2T}	Loss of SDC common suction line	3.8E-02
E_{2V}	Loss of common suction line for ADHRS	3.8E-02
T_{5A}	Loss of all Standby Service Water (SSW)	2.4E-02
T_{5B}	Loss of all Turbine Building Cooling Water	2.4E-02
T_{5C}	Loss of all Plant Service Water (includes Radial Well)	2.4E-02
T_{5D}	Loss of all Component Cooling Water	2.4E-02
T_{AB}	Loss of 1E 4160 V AC Bus B	1.66E-03
T_{DB}	Loss of 1E 125 V DC Bus B	6E-03
T_{IA}	Loss of Instrument Air	0.18

Table 2.6-4 Initiating Events for POS 5

Initiating Event Nomenclature	Description	Mean Frequency per Year for POS 5
T_{ORV}	Inadvertent Open Relief Valve at Shutdown	7.2E-02
T_{IOP}	Inadvertent Overpressurization (makeup greater than letdown)	1.57E-03
T_{IHP}	Inadvertent Pressurization via spurious HPCS actuation	1.4E-02
T_{IOF}	Inadvertent Overfill via LPCS or LPCI	2.2E-02
T_{RPT}	Loss of Recirculation Pump	7.2E-02
T_{LM}	Loss of Makeup	8E-03

* This value was taken from NUREG/CR-3862, EPRI Category 20 -- Feedwater - Increasing Flow at Power. Note that for POS 5, inadvertent overpressurization is essentially loss of RWCU.

⋆ This value was taken from NUREG/CR-3862, EPRI Category 24 -- Feedwater - Low Flow. Note that for POS 5, loss of makeup is essentially loss of CRD.

ADHRS	alternate decay heat removal system
CRD	control rod drive
DHR	decay heat removal
EPRI	electric power research institute
LOCA	loss of coolant accident
LOSP	loss of off-site power
LPCI	low pressure coolant injection
LPCS	low pressure core spray
RHR	residual heat removal
RWCU	reactor water cleanup
SDC	shut down cooling
SSW	stand-by service water

Table 2.6-5 Collections and Summaries of Actual Failure Events

Title	Source	Reference
1. Licensee Event Reports	USNRC	
2. Licensee Event Report Summaries Valves Pumps Electrical Power Circuit Breakers, Protective Relays Initiating Events Selected I&C Components Control Rods and Drive Mechanisms	Idaho National Engineering Laboratory	 NUREG/CR-1363 NUREG/CR-1205 NUREG/CR-1362 NUREG/CR-4212 NUREG/CR-3862 NUREG/CR-1740 NUREG/CR-1331
3. In-Plant Reliability Data Systems Pumps Valves Electrical Power Components (Diesels, Batteries, Chargers and Inverters)	Oak Ridge National Laboratory	 NUREG/CR-2886 NUREG/CR-3154 NUREG/CR-3831
4. Nuclear Plant Reliability Data System	Institute for Nuclear Power Operations	Quarterly Reports
5. Reactor Safety Study Section III - LER Data for 1972-1973	USNRC	WASH-1400
6. ATWS: A Reappraisal	Electric Power Research Institute	EPRI NP-2230
7. Loss of Offsite Power at Nuclear Power Plants	Electric Power Research Institute	EPRI NP-2301 NSAC-103
8. Diesel Generator Reliability at Nuclear Power Plants	Electric Power Research Institute	EPRI NP-2433
9. Classification and Analysis of Reactor Operating Experience Involving Dependent Events	Electric Power Research Institute	EPRI NP-3967
10. PORV Failure Reduction Methods	Combustion Engineering	CEN-145
11. Evaluation of Station Blackout Accidents at Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-44: Final Report	NRC	NUREG-1032

Table 2.6-6. Statistical Analyses and Generic Data Bases

Statistical Analyses

Title	Source	Reference

Probabilistic Safety Analysis of DC Power Requirements for Nuclear Power Plants	USNRC	NUREG-0666
Reliability Data Book	Swedish Nuclear Power Inspectorate	RSK 85-25
Statistical Analysis of Nuclear Power Plant Pump Failure Rate Variability-Preliminary Results	Los Alamos National Laboratory	NUREG/CR-3650

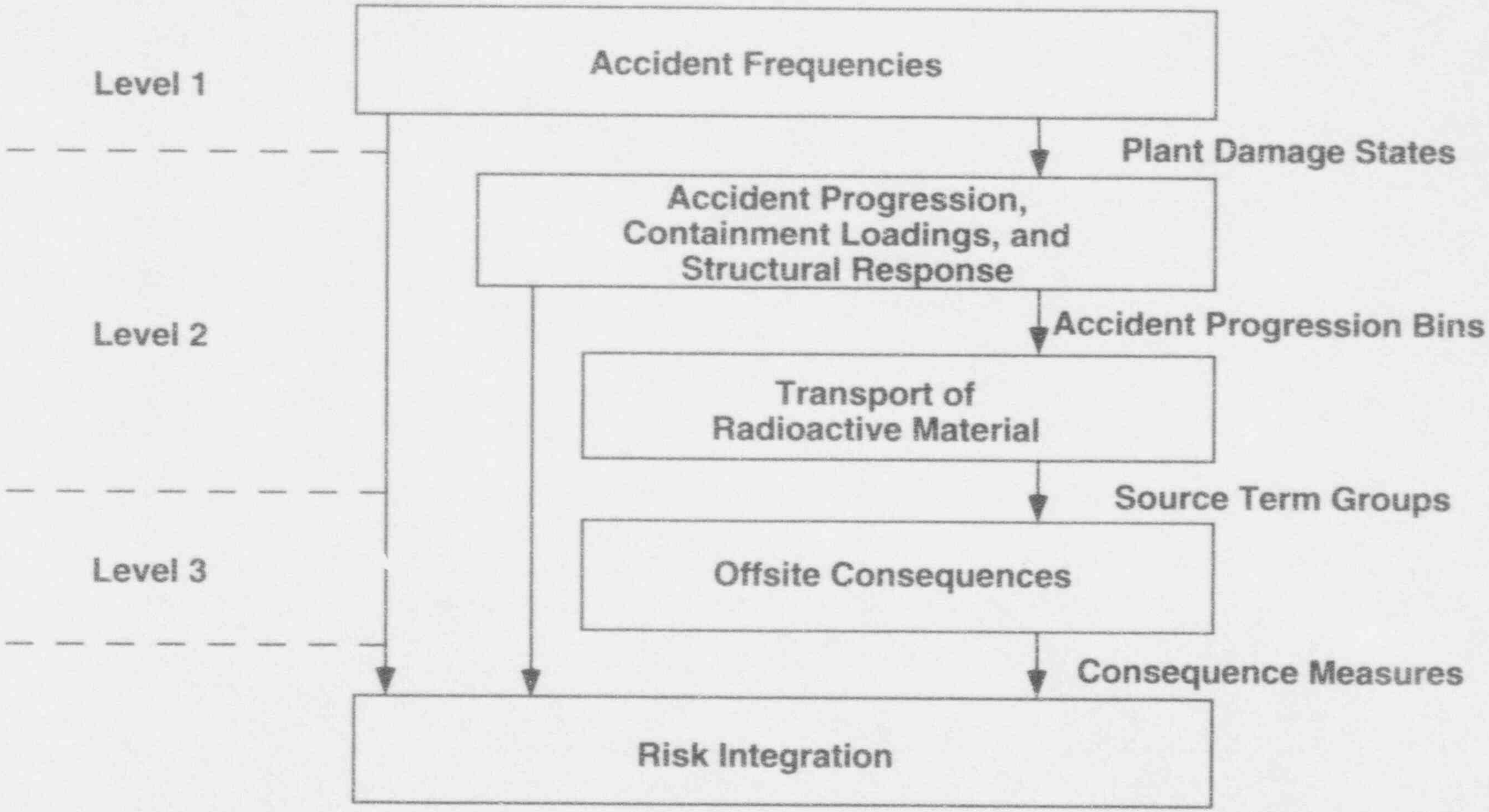
In addition, items 2, 3, 5, 7, 8, 9, and 10 of Table 2.4-4 present analyses of reported data.

Generic Failure Rate Data Bases

Title	Source	Reference
Reactor Safety Study	USNRC	WASH-1400
Interim Reliability and Evaluation Program (IREP) Procedures Guide	Sandia National Laboratories	NUREG/CR-2728
Reliability Data Book	Swedish Nuclear Power Inspectorate	RKS 85-25
Station Blackout Accident Analyses -TAP A-44	USNRC	NUREG/CR-3226

TABLE 2.6-7
PRECURSORS AND SEVERE ACCIDENTS

Date	Type	Event	Cond. Core Damage Probability	Reference
24-Mar-71	LOSP	LaCrosse loss of offsite power	$4x10^{-5}$	NUREG/CR-2497
19-Jan-74	LOSP	Haddam Neck loss of offsite power	$2x10^{-4}$	NUREG/CR-2497
22-Mar-75	Fire	Browns Ferry Fire	$1.5x10^{-1}$	NUREG/CR-2497
31-Aug-77	LOFW	Cooper loss of feedwater	$1x10^{-3}$	NUREG/CR-2497
10-Nov-77	Flooding	Surry 2 valve flooding	$6x10^{-7}$	NUREG/CR-2497
20-Mar-78	Other	Rancho Seco loss of nonnuclear instrumentation	$1x10^{-1}$	NUREG/CR-2497
06-Mar-79	Service Water	Brunswick loss of RHR service water	$2x10^{-5}$	NUREG/CR-2497
02-May-79	LOFW	Oyster Creek loss of feedwater flow	$2x10^{-3}$	NUREG/CR-2497
28-Jun-80	ATWS	Browns Ferry partial failure to scram	$9.8x10^{-4}$	NUREG/CR-3591
02-Nov-81	LOCA	Sequoyah loss of coolant	$9x10^{-4}$	NUREG/CR-2497
09-Jun-85	LOFW	Davis Besse loss of feedwater	$1.1x10^{-2}$	NUREG/CR-4674
20-Mar-90	Shutdown Transient	Vogtle 1 loss of shutdown cooling	$1x10^{-3}$	NUREG/CR-4674
13-Aug-91	Transient	Nine Mile Point 2	$1x10^{-5}$	Not Published



Note: Adapted from NUREG-1150

Figure 2.6-1 Three levels of probabilistic risk assessment

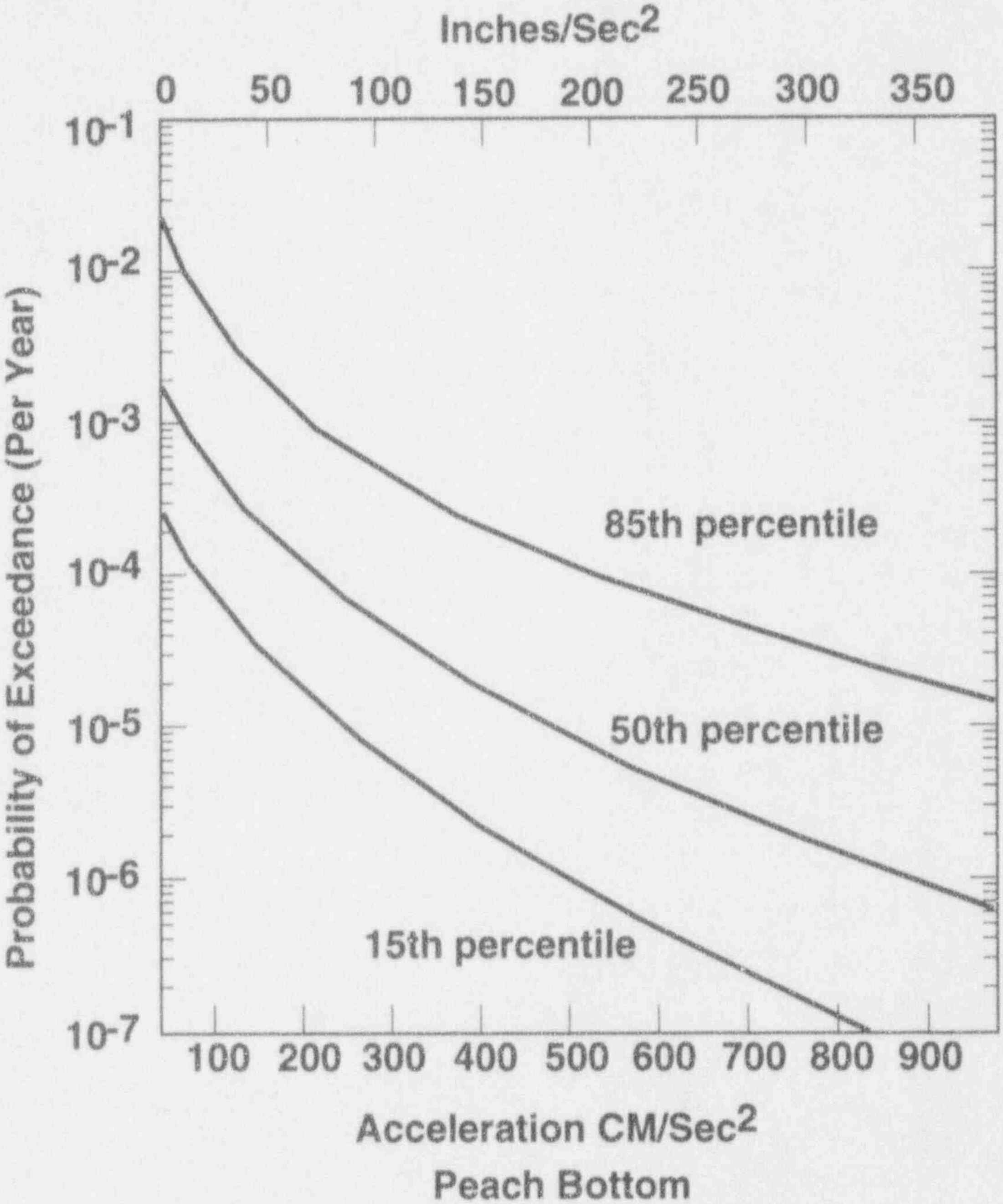


Figure 2.6-2 LLNL hazard curves for Peach Bottom site

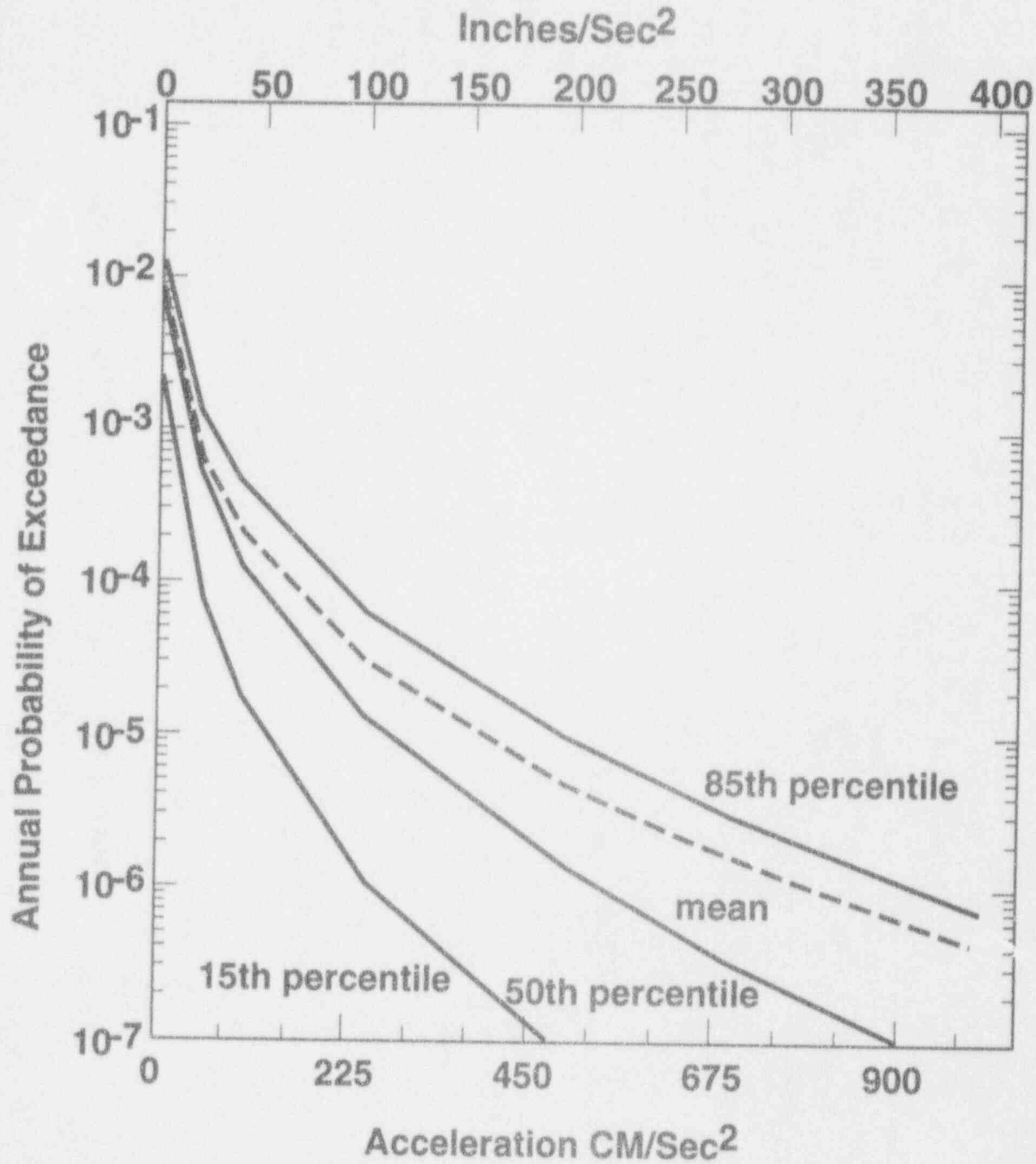


Figure 2.6-3 EPRI hazard curves for Peach Bottom site

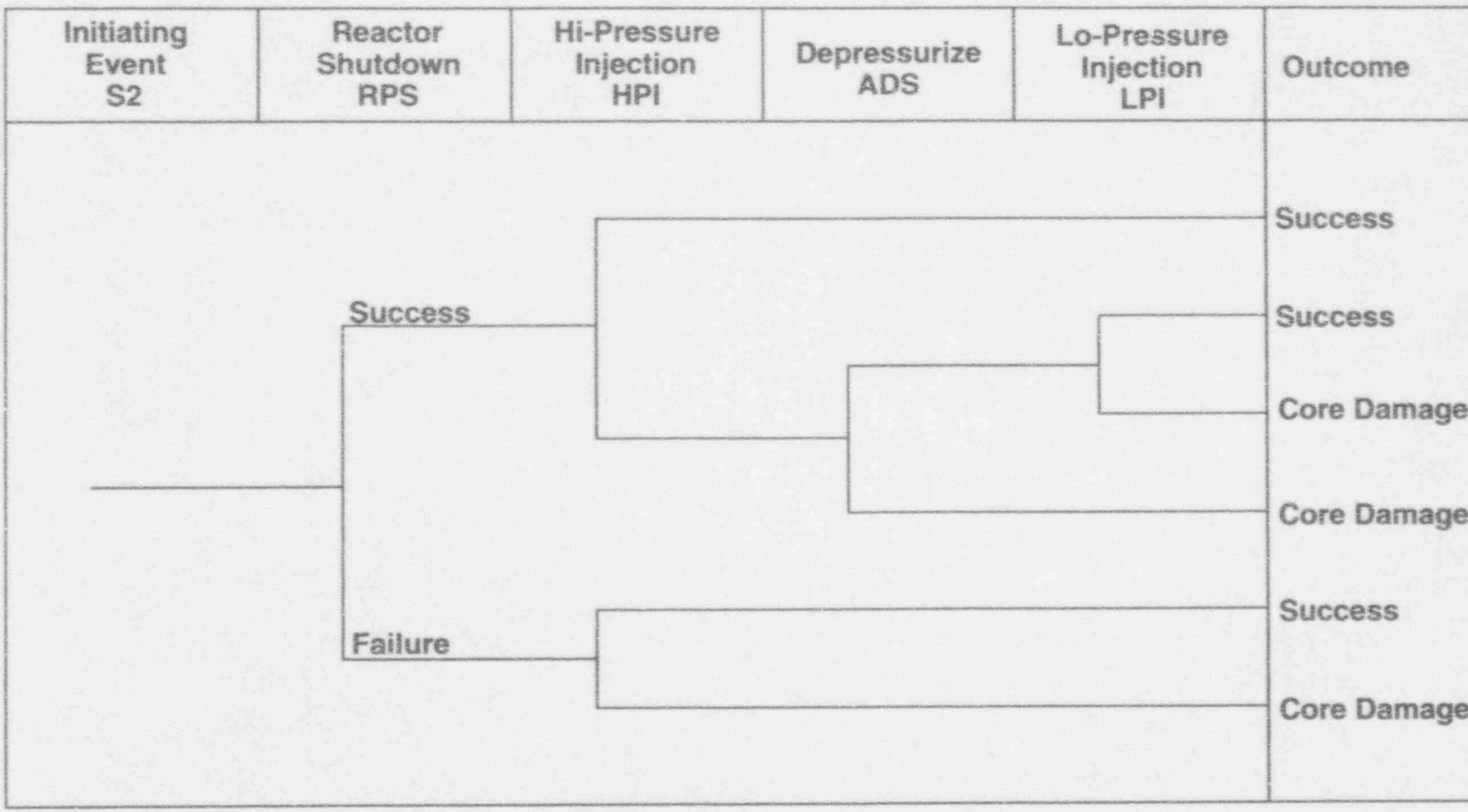


Figure 2.6-4 Example event tree

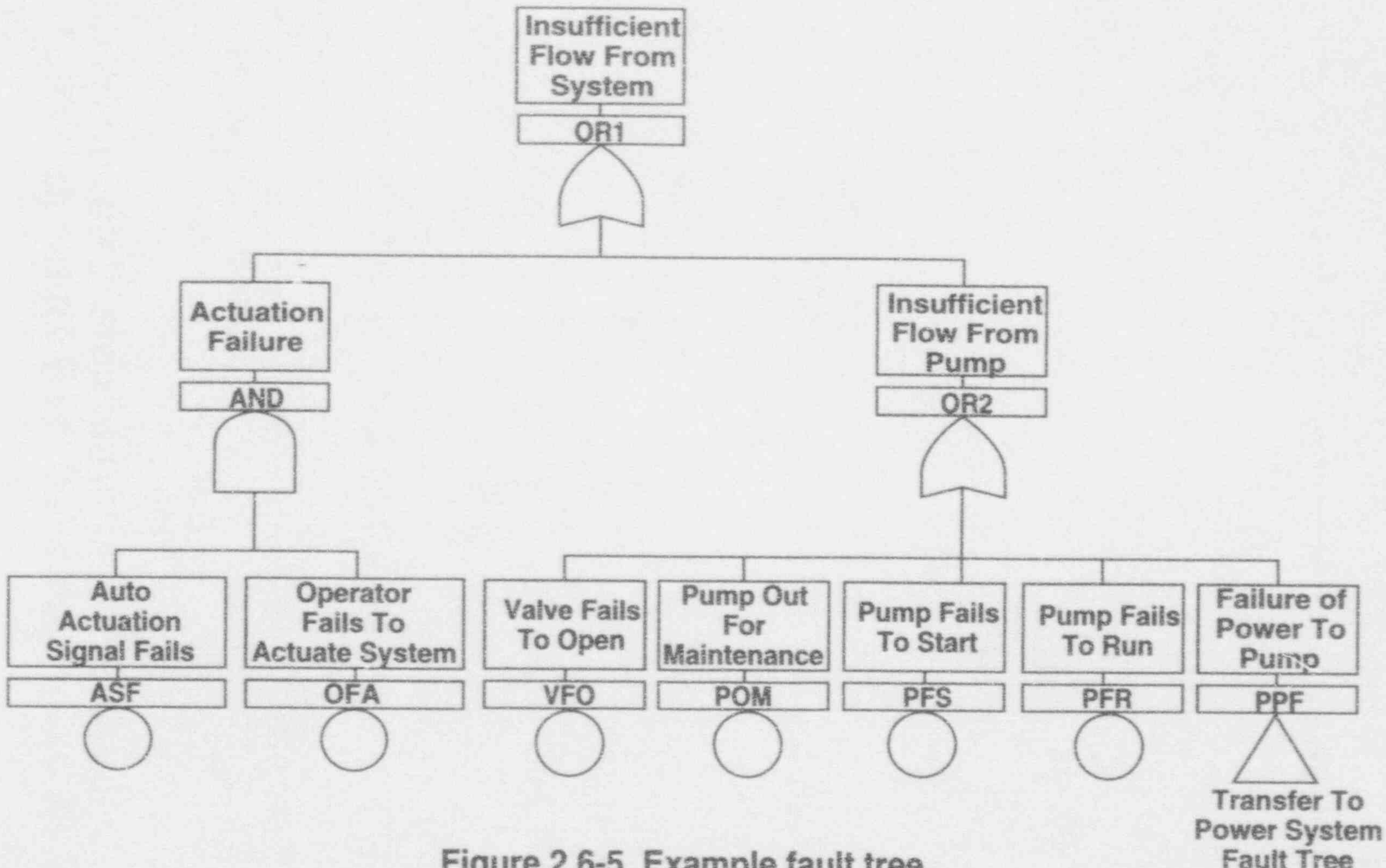


Figure 2.6-5 Example fault tree

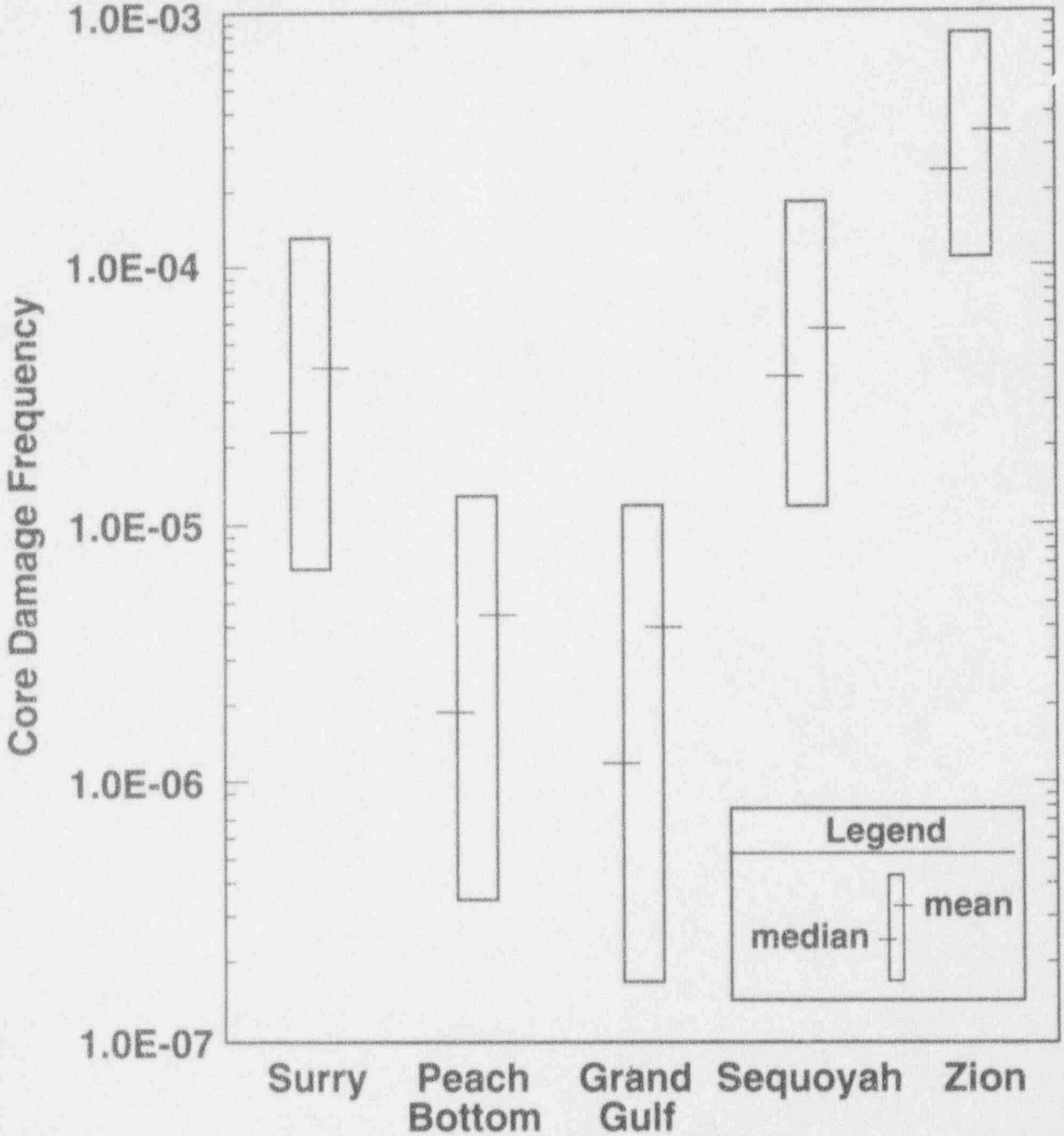


Figure 2.6-6 Internal core damage frequency ranges (5th to 95th percentiles)

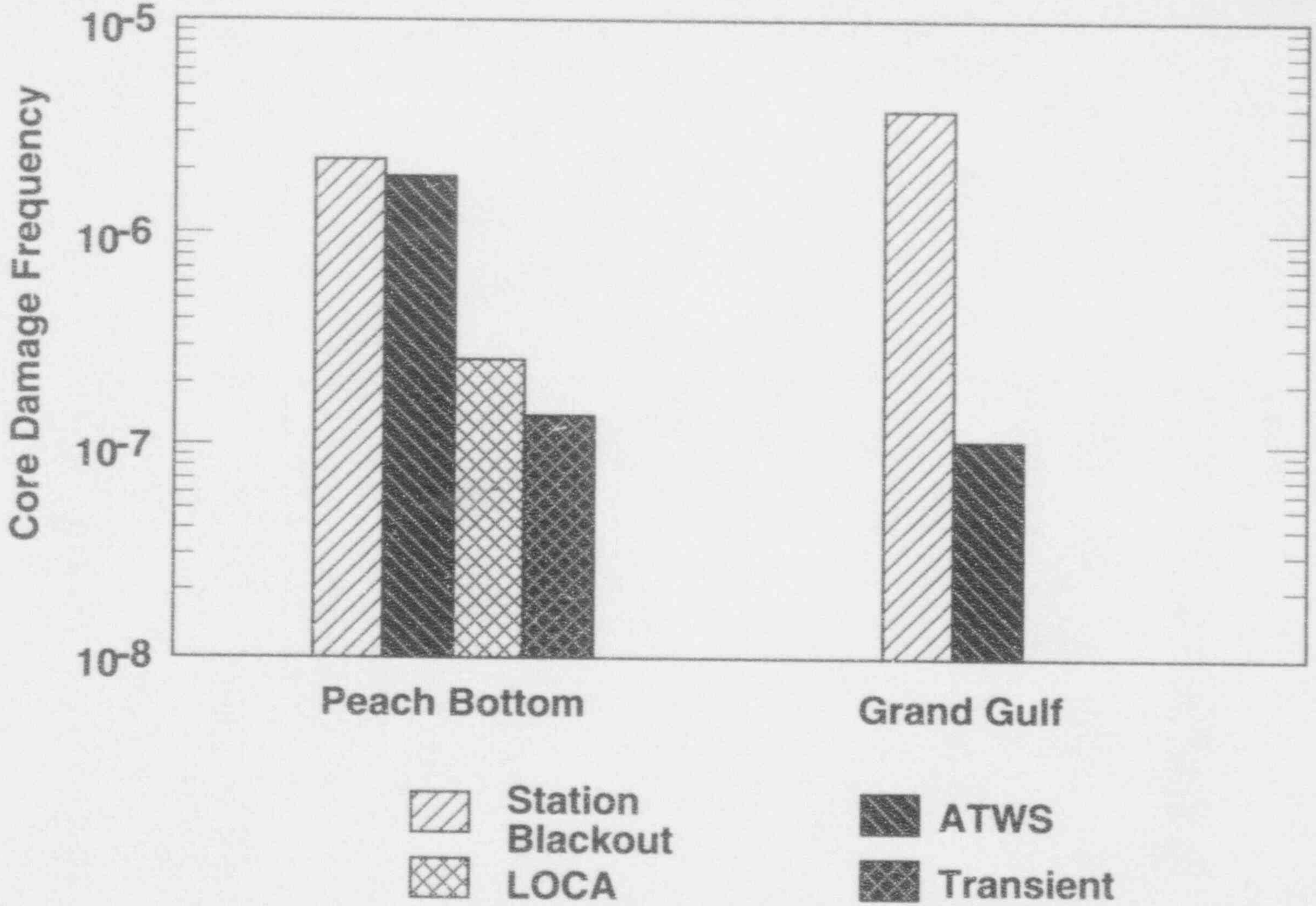


Figure 2.6-7 BWR principal contributors to internal core damage frequencies

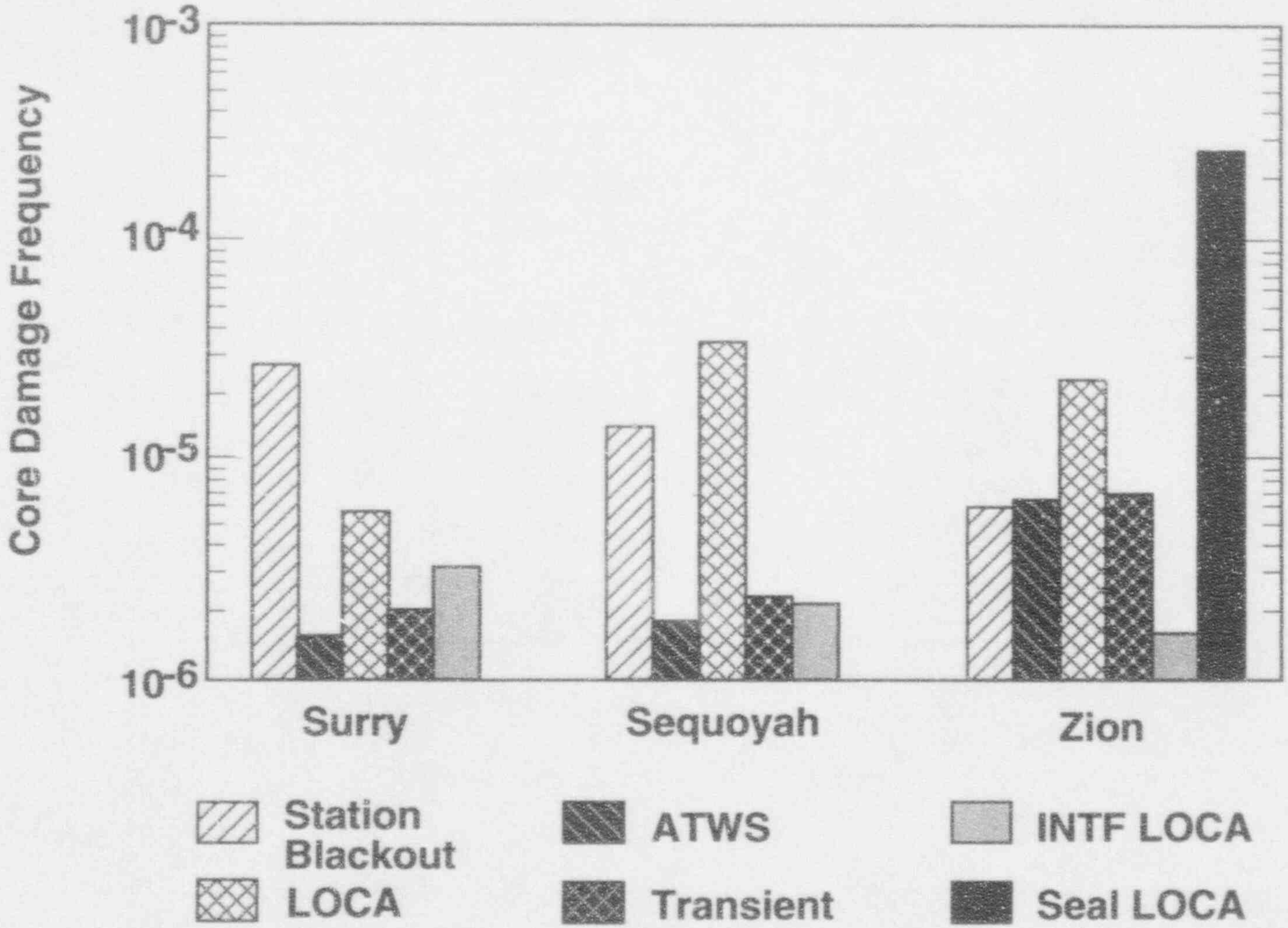


Figure 2.6-8 PWR principal contributors to internal core damage frequencies

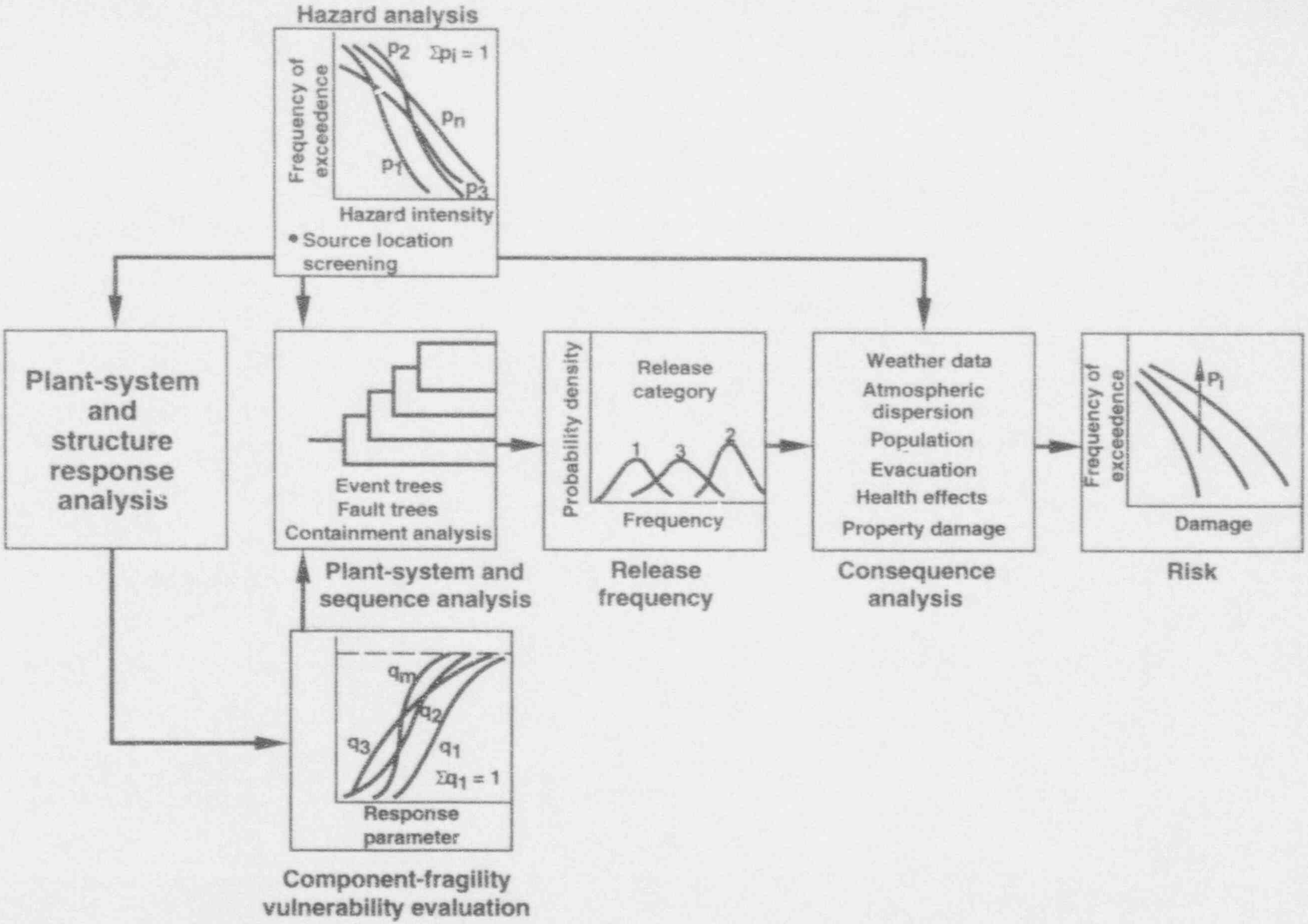


Figure 2.6-9 Risk-assessment procedure for external events

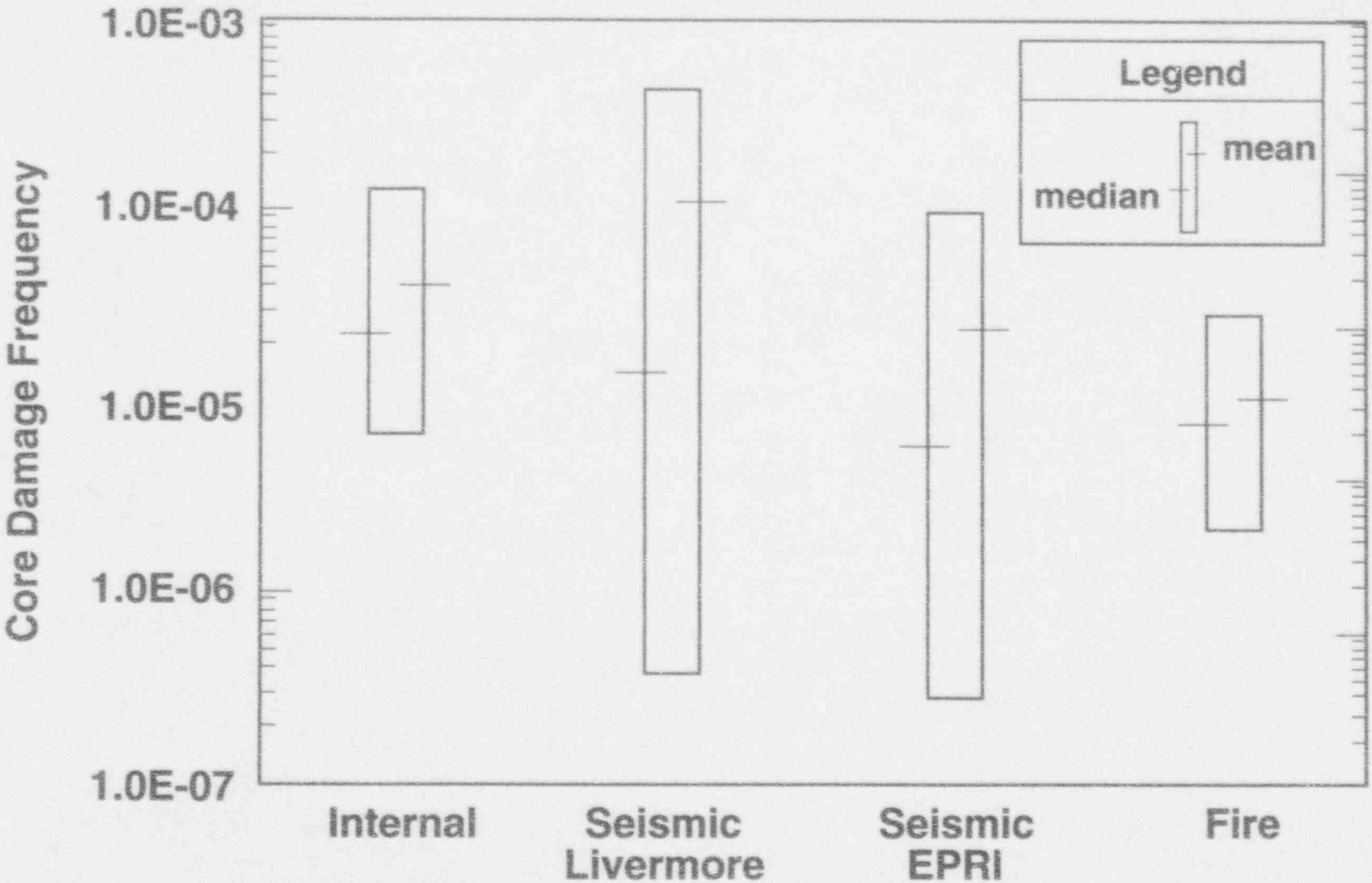


Figure 2.6-10 Surry internal-and external-event core damage frequency ranges

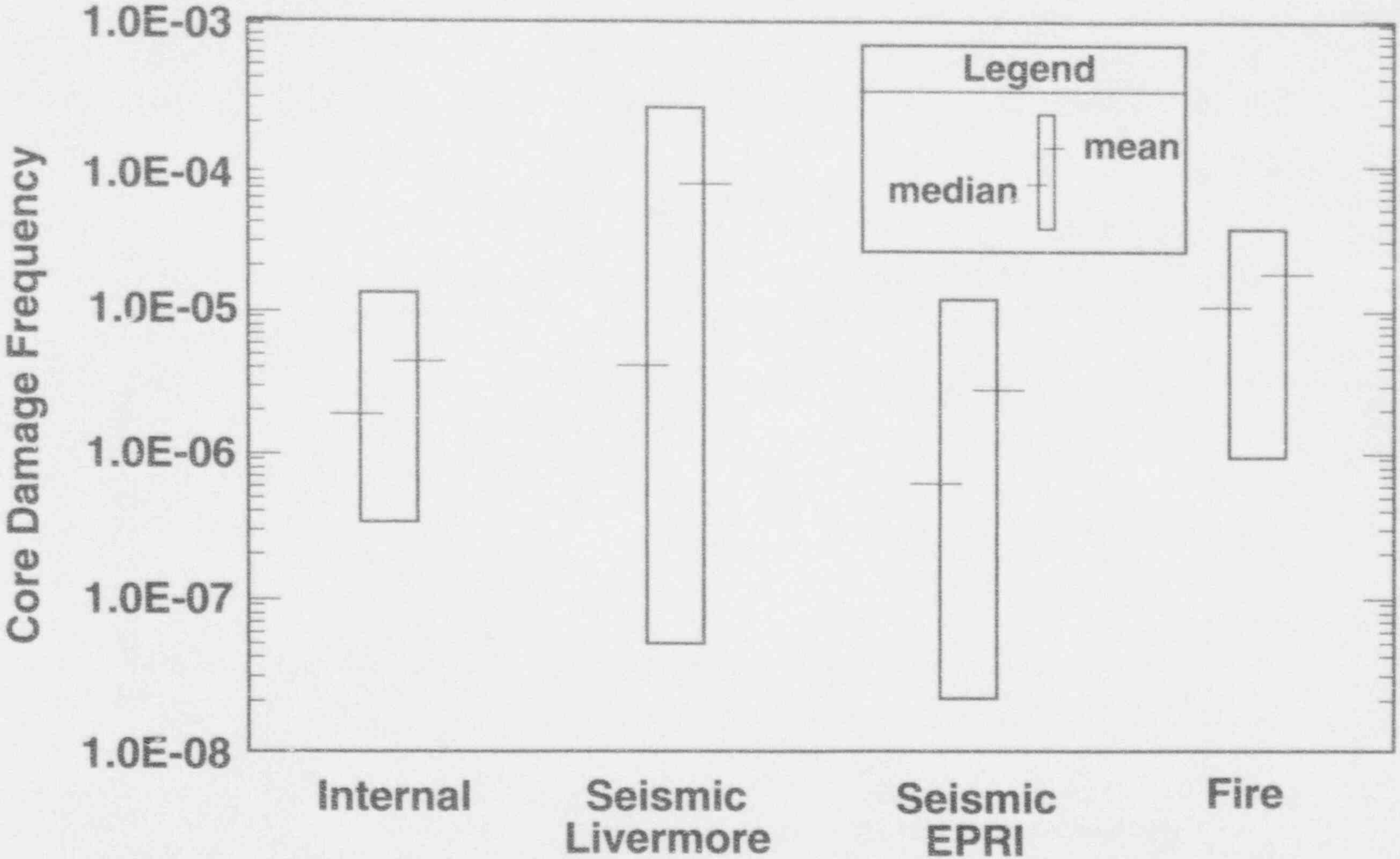


Figure 2.6-11 Peach Bottom internal- and external-event core damage frequency ranges

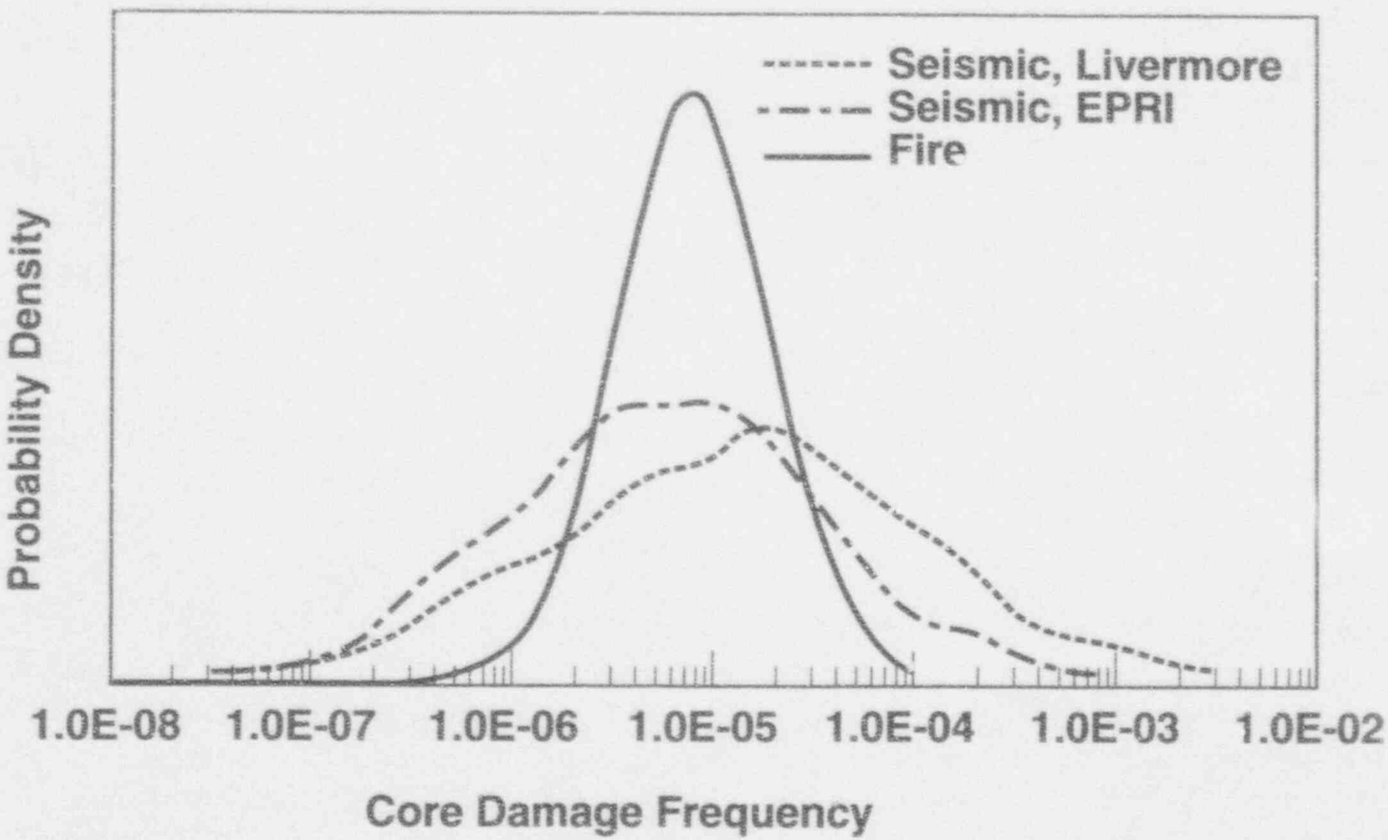


Figure 2.6-12 Surry external-event core damage frequency distributions

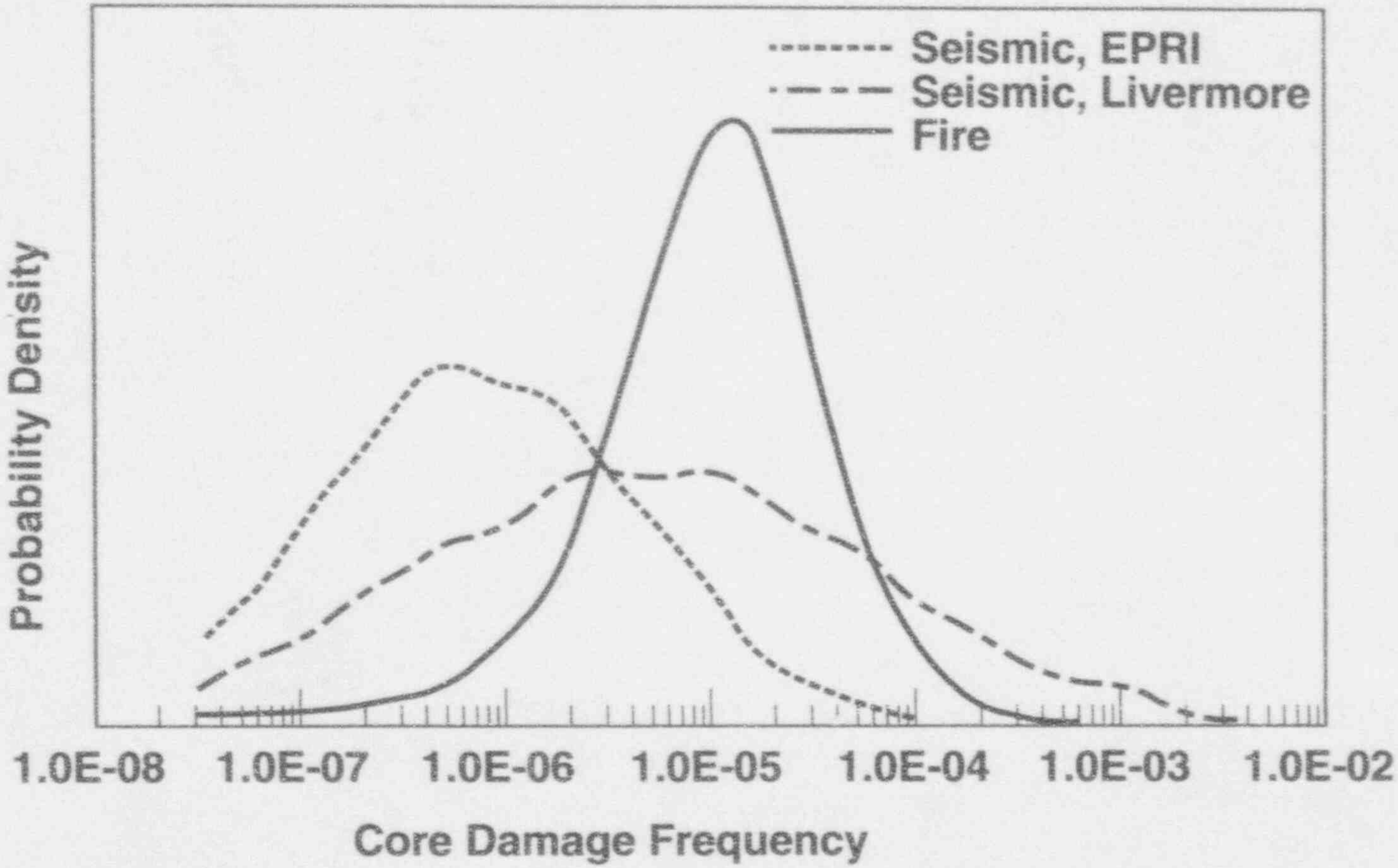


Figure 2.6-13 Peach Bottom external-event core damage frequency distributions

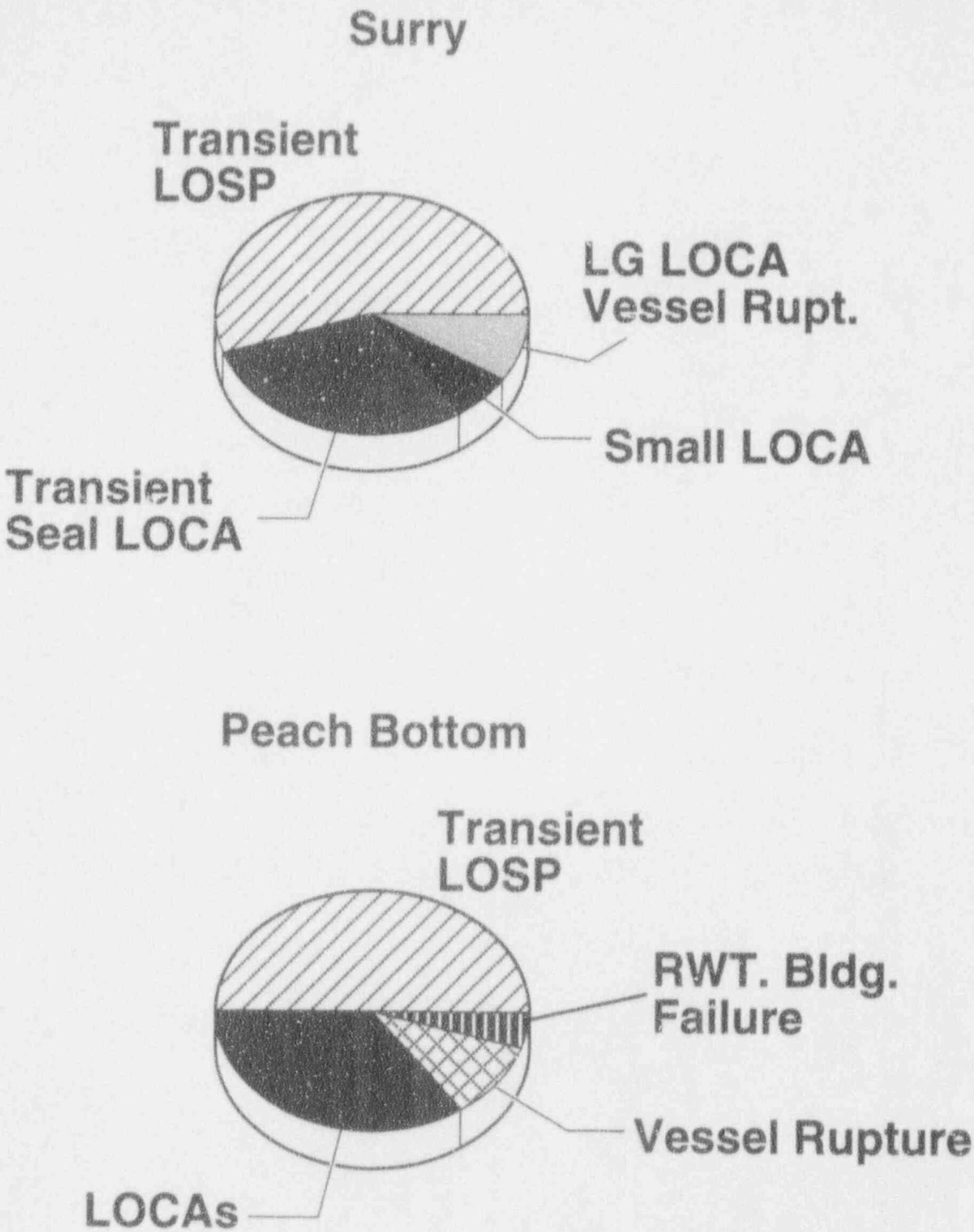


Figure 2.6-14 Principal contributors to seismic core damage frequencies

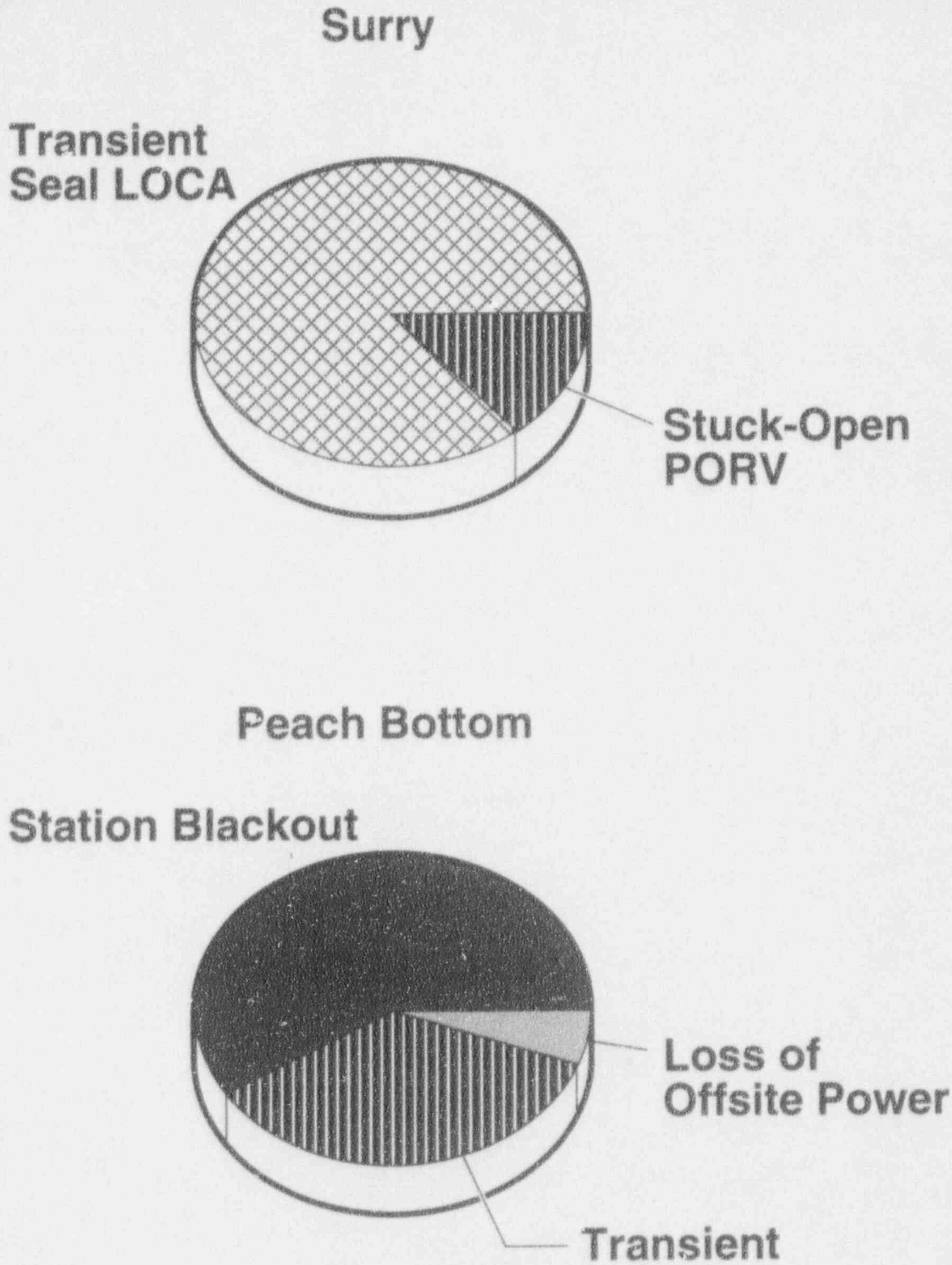


Figure 2.6-15 Principal contributors to fire core damage frequencies

References for Section 2.6

1. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, Nuclear Regulatory Commission, December 1990.

2. *PRA Course*, NUREG/CR-4350 1 OF 7, SAND 85-1495/1 of 7, (August 1985).

3. NUREG 75/014, U.S. Nuclear Regulatory Commission, October, 1975.

4. D. M. Ericson, Jr., *Analysis of Core Damage Frequency: Internal Events Methodology*, et al., NUREG/CR-4550, Vol. 1, Rev. 1., January 1990.

5. Whitehead, D.W., et al. *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf Unit 1: Analysis of Core Damage Frequency From Internal Events for Plant Operational State 5 During a Refueling Outage.*, 1994. NUREG/CR-6143.

6. G. E. Cummings, *Summary Report on the Seismic Safety Margins Research Program*, Lawrence Livermore National Laboratories, NUREG/CR-4431, UCID-20549, January 1986.

7. Seismicity Owners Group and Electric Power Research Institute, *Seismic Hazard Methodology for the Central and Eastern United States*, EPRI NP-4726, July 1986.

8. Title 10, Code of Federal Regulations, Part 50, Appendix R, January 1, 1991.

2.7 Risk-Based Policies and Regulations

As discussed in Section 1.2.1, the Atomic Energy Act of 1954 requires the NRC to ensure that

> *"the utilization or production of special nuclear material will ... provide adequate protection to the health and safety of the public."*

In its rules and decisions, the Commission refers to this standard as either the "*adequate protection*" standard or the "*no undue risk*" standard. The interchangeable use of these two terms has been accepted in legal decisions.[1,2] Congress left it to the AEC/NRC to determine what constituted "*no undue risk.*" Prior to the TMI-2 accident, such determinations were based primarily on the engineering judgment of the NRC staff, the ACRS, and the Commissioners. Following the TMI-2 accident, the NRC began to deal with risk in a more systematic and quantitative manner through the use of PRA techniques (Section 2.6). Quantitative risk limits are not imposed in NRC regulations; however, quantitative risk estimates provide much of the supporting rationale and impetus for regulatory decisions. The Reactor Safety Study and subsequent PRAs identified severe accidents that are important to risk and warranted further attention.

The next three subsections describe the role that quantitative risk estimates played in addressing and resolving three important regulatory issues: Anticipated Transients Without Scram, Auxiliary Feedwater System Reliability, and Station Blackout. Following these discussions, current policies and practices of the NRC regarding the use of quantitative risk estimates are discussed in subsections addressing the Safety Goal Policy, the Backfit Rule, and Individual Plant Examinations.

2.7.1 Anticipated Transients Without Scram

An "anticipated transient" is an event that is expected to occur one or more times during the life of a nuclear power plant. There are a number of anticipated transients, some quite trivial and others that are more significant in terms of the demands imposed on plant equipment. Anticipated transients include such events as a loss of electrical load that leads to closing of the turbine stop valves, a load increase such as opening of a condenser bypass valve, a loss of feedwater flow, and a loss of reactor coolant flow.

The reactor protection system (RPS) is designed to monitor key plant variables to detect off-normal plant conditions arising from anticipated transients and automatically initiate whatever safety action is needed. For some anticipated transients, to assure that no damage to the plant occurs, the RPS is designed to automatically "scram" the reactor, that is, to cause the control rods to rapidly move into the core, thereby shutting down the nuclear reaction and reducing the heat generation rate to that associated with radionuclide decay (see Figure 2.1-1). An "anticipated transient without scram" or ATWS event would occur if the RPS failed to scram the reactor given such a transient.

As discussed in Appendix 2B, the RPS is designed to make an ATWS event very unlikely. The RPS has multiple (at least 3, usually 4) channels to meet the single failure criterion, permit sensor calibration during plant operation, and reduce the potential for spurious scrams. The RPS is specifically designed to be separate from plant control systems.

2.7.1.1 Origin of the ATWS Issue

The concern about ATWS originated in discussions of the ACRS, the regulatory staff, and reactor manufacturers about potential interactions between reactor control and protection systems. S. H. Hanauer, who became an ACRS member in 1965, strongly advocated that systems provided to shut the reactor down be strictly separated from systems used to control the reactor. He cited many reasons for this position including a classic accident that occurred at the High Temperature Reactor Experiment (HTRE-3), an experimental reactor in Idaho.[3] Both the control system and protection system for this reactor took inputs from the same neutron flux instruments. A design defect in these instruments prevented an increase in current when the reactor power increased. The unchanging current caused the reactor control system to withdraw the control rods and simultaneously blinded the reactor protection system to the resulting power increase. The core was destroyed.

Hanauer began raising the control/protection separation issue in connection with specific plants being reviewed by the ACRS in 1966 and 1967. Reactor instrument designers carried out analyses of various kinds of failures. After considerable discussion, and some design changes, it was determined that separation of control and protection functions was being achieved to a reasonable degree, either by physical separation or by electrical isolation. It became clear that failures caused by equipment wear-out or failures occurring on a random basis in protection systems would not cause appreciable deterioration of reliability because of the redundancy of the systems. It was not so clear, however, that these systems were sufficiently invulnerable to common cause failures (see Appendix 2B).

In a letter to the ACRS dated January 21, 1969, E. P. Epler, an ACRS consultant, pointed out that common cause failures could reduce the reliability of protection systems in such a way that the system might not function properly in the event of an anticipated transient.[3] Epler argued as follows: (1) Reactor scram was needed to prevent core meltdown and a loss of containment integrity following a routine operating event such as loss of electric load, which might occur about once a year. (2) A scram failure probability smaller than 10^{-4} per demand could not be defended because of the possibility of common cause failures. (3) Therefore, core melt and a major release of radioactivity might occur with a probability larger than 10^{-4} per reactor-year.

In a memorandum enclosed with his letter, Epler noted that public figures like Alvin Weinberg, the Director of ORNL, and Chauncey Starr, then Dean of Engineering at the University of California, Los Angeles, and formerly President of Atomics International, had publicly indicated that the probability of a serious reactor accident was similar to that of a jet airliner plunging into Yankee Stadium during a World Series game, which Epler estimated as roughly 10^{-7} per year. However, because of the lack of measures to cope with the China Syndrome, and because of his own estimate of the probability of scram failure, Epler felt that the actual probability of a serious accident might be a factor of 1,000 higher.

The ATWS issue posed by Epler sparked heated debate and took over 15 years to resolve. Initial efforts to resolve the issue took two general directions. The first involved attempts to evaluate the likelihood of common cause or other failures of reactor protection systems that might lead to ATWS events. Second, in late 1970, analyses of the consequences of postulated ATWS events were requested of reactor designers, and all the designers made these analyses.

2.7.1.2 Plant Response to Postulated ATWS Events

In late 1970, all LWR designers and NRC contractors began performing thermal-hydraulic analyses of hypothetical ATWS events. The aim was to determine whether the consequences of

ATWS were potentially severe enough to require further measures should the reliability of reactor trip systems be judged unacceptable. In analyzing each transient, all other systems were assumed to react normally unless the consequences of the transient would make them inoperative. (By postulating an ATWS, one is already postulating multiple failures--more failures than postulated using the single failure criterion.) Initial conditions for such analyses, such as power level, flow rate, pressure, power distribution, etc., correspond to normal power operation. The course of each transient is followed in the analysis until the reactor is essentially at zero power in a coolable geometry, normal decay heat removal systems are operating, and containment pressure is within design limits.

The thermal-hydraulic analyses show that for transients in which plant heat removal systems are not greatly affected, the consequences of the transients without scram occurring would not be particularly severe. After some period of off-normal operation, the plant stabilizes and can be shut down without damage. However, for those transients where the heat removal systems are affected, the potential exists for significant damage. If the reactor is at full power, it will continue to generate substantial power during the transient. If the transient involves the interruption of the normal process of heat removal from the reactor, then the energy being generated in the core must appear as increased temperature and pressure in the reactor coolant system. For transients such as a loss of feedwater in PWRs and loss of condenser vacuum in BWRs, some early analyses indicated that the pressure increase might be great enough to challenge the integrity of the reactor coolant system.

One of the results of the early ATWS analyses was that reasonably prompt insertion of negative reactivity of about 1 to 2 percent would reduce the consequences of most ATWS events to acceptable levels. Such prompt insertions would not require the operation of all the control rods. This suggested that modifications might be feasible that would enable plants to withstand ATWS events.

Analyses performed by GE in early 1971 indicated that the peak reactor coolant pressure in an ATWS event could be significantly higher than the reactor vessel design pressure. As part of their analyses, GE found that tripping the recirculation pumps on coincident signals of high neutron flux and high reactor vessel pressure caused an increase in the moderator void fraction in the core region. This introduced a substantial negative reactivity and significantly reduced the power and pressure increases that would otherwise accompany a transient resulting from loss of condenser vacuum without scram. In August 1971, both the Newbold Island and Limerick stations committed to the use of the recirculation pump trip.

2.7.1.3 WASH-1270 and 1975 NRC Position

In September 1973 the NRC publicly adopted a position on ATWS with the publication of the WASH-1270 report.[4] Plants for which ATWS had already been noted as a concern in licensing proceedings or which would apply for construction permits before October 1, 1976, (Class B plants) would be required to "incorporate any design changes necessary to assure that the consequences of anticipated transients would be acceptable in the event of a postulated failure to scram." The need for backfitting older (Class C) plants would be considered on a case by case basis. Future (Class A) plants, those applying for construction permits after October 1, 1976, "should incorporate design changes that improve significantly the reliability of the reactor shutdown systems, as compared with current designs."

One important aspect of the WASH-1270 report was that it defined an overall safety goal, as well as a quantitative goal for ATWS, for future plants. Specifically, the overall safety goal was that

> *"... the risk to the public from all reactor accidents should be very small compared to other risks of life such as disease or natural catastrophes."*

Projecting about one thousand nuclear plants in the United States by the year 2000, it was argued that the safety objective would require

> *"that there be no greater than one chance in one million per year for an individual plant of an accident with potential consequences greater than the Part 100 guidelines."*

WASH-1270 further proposed to allocate only one-tenth of their objective to any one accident type; hence, the safety objective for ATWS was that it not lead to an accident with serious offsite consequences more frequently than 10^{-7} per reactor-year.

With the issuance of the WASH-1270 report in September 1973, the regulatory staff had taken a position on ATWS and it was seemingly resolved except for implementation. The ACRS moved the ATWS issue into the resolved column on their list of generic issues in February 1974. In the period 1974-1975 all the reactor vendors submitted analyses on ATWS in general response to the requirements set forth in the WASH-1270 report.

In September 1975, the NRC proposed a major change in their ATWS position by stating that future (Class A) plants, like the older (Class B) plants, would have to be designed to tolerate the occurrence of an ATWS event. Implicitly there appeared to be doubt among the staff that diverse shutdown systems could or would be proposed and developed to the point where the NRC could agree that the probability of ATWS was acceptably low. However, without a rulemaking the new NRC position did not have the force of law, and arguments between NRC and the nuclear industry continued regarding what constituted an acceptable solution to the ATWS issue.

2.7.1.4 Impact of Reactor Safety Study

Many representatives of the nuclear utilities and the reactor vendors pointed to results of the 1975 Reactor Safety Study to demonstrate that ATWS was not a major contributor to risk for LWRs. They concluded that the existing situation was satisfactory and no design modifications were needed to improve either the reliability of scram systems or the ability of the reactors to tolerate an ATWS.

Beginning in the fall of 1976, a series of reports entitled "ATWS: A Reappraisal" was published by the Electric Power Research Institute (EPRI). The EPRI reports reevaluated the probability of failure to scram and estimated the risk to the public from ATWS. Using their assumptions and choice of data, the authors concluded that the probability of failure to scram was much lower than 10^{-4} per demand (by a few factors of 10) and that ATWS posed insignificant risk to the health and safety of the public.

In March 1977 the NRC formed a task force on ATWS in an effort to finally resolve the matter. In July 1977, the NRC reiterated their general position of December 1975 that scram unreliability could not be shown to be acceptably low and that measures were required to mitigate the consequences of ATWS.

In April 1978 the regulatory staff issued a new report, NUREG-0460, titled "Anticipated Transients Without Scram for Light Water Reactors."[5] This report proposed a change in safety objective for an unacceptable ATWS from 10^{-7} per reactor-year as set forth in the WASH-1270 to 10^{-6} per reactor-year. This was apparently based on the overall frequency of core melt predicted in the Reactor Safety Study

($5x10^{-5}$ per reactor-year). The staff employed a mixture of deterministic and probabilistic analyses to prescribe the design approaches that would be needed to meet the new safety objective for each LWR vendor. The new staff proposals were again opposed very strongly by the industry, and after many meetings between the NRC staff, the ACRS, and representatives of the nuclear industry, strong differences of opinion still existed.

In early 1979, the Risk Assessment Review Group (Lewis committee) issued their report (NUREG/CR-1400),[6] which was highly critical of the Reactor Safety Study. After the NRC commissioners endorsed the Lewis committee report, the NRC proposed a greatly revised position on ATWS, one which strongly reflected the difficulties in backfitting an operating plant or even a plant under construction. For such plants, emphasis was placed on changes in circuitry that were relatively easy to accomplish and that might provide increased scram reliability. For plants that were to be constructed, the emphasis remained on hardware changes to mitigate the consequences of an ATWS (should it occur) by keeping pressure and temperatures below acceptable limits. In arriving at their new position the regulatory staff stated they were now using engineering judgment since the commissioners had stated that probabilistic methods could not be used to provide a quantitative basis in licensing.

2.7.1.5 Impact of TMI-2 Accident

In the spring of 1979, the Three Mile Island accident introduced additional questions on the behavior of PWRs which caused the NRC staff to reevaluate their ATWS position for PWRs. In early 1980, the NRC staff proposed a more stringent position with the stated intention of trying to resolve ATWS once and for all. The industry once again disagreed and took a position that would require less backfitting.[3] More than eleven years after the letter by Epler, the ATWS issue remained unresolved. However, major events at the Browns Ferry 3 BWR and the Salem 1 PWR soon provided significant motivation for resolution to the ATWS issue.

2.7.1.6 Failure of Control Rods to Fully Insert at Browns Ferry 3

On June 28, 1980, Browns Ferry Unit 3, a BWR, reported that 76 of 185 control rods failed to insert fully into the core when a manual scram was initiated by the reactor operator. Fortunately, this occurred during a routine shutdown from about 35% power, rather than during the kind of reactor transient in which complete and rapid scram of all the rods might have been important.

The problem was determined to be hydraulic in nature rather than electrical or mechanical. The control rod drives (CRDs), which insert and withdraw the attached control rods in a General Electric BWR, are essentially water-driven hydraulic pistons. On a scram, a relatively high water pressure is applied to the bottom side of the piston by opening a scram inlet valve. A scram outlet valve opens to relieve water and pressure above the piston and the rods are rapidly driven up into the reactor core. Water discharged from the 185 individual CRDs during scram insertion is collected in two separate headers called the scram discharge volumes (SDVs). During normal operation, both SDVs are designed to remain empty.

Tests, inspections, and analyses conducted after the event led to the conclusion that the east SDV was substantially full of water at the time of the event, leaving insufficient room for the discharge water. Accordingly, upon scram actuation, the CRDs rapidly drove the control rods partially into the core but rod motion prematurely ceased when pressure quickly equalized on each side of the pistons. Following each scram actuation, the scram signal was reset by the operator, allowing more water to drain from the SDV and permitting the rods to insert further. Sufficient water was finally drained from the SDV to allow the rods to insert fully on the fourth scram signal.

A Preliminary Notification was issued promptly, and, on July 3, 1980, the NRC issued IE Bulletin 80-17 to all BWR licensees. Continuing NRC review of the Browns Ferry event identified other problems, which required tests, inspections, hardware changes, new procedures, and operator training at various BWR plants. These actions are discussed in Appendix 2B. Browns Ferry Unit 3 was authorized to restart on July 13, 1980, following completion of the actions required by IE Bulletin 80-17 and other extensive tests.

2.7.1.7 ATWS Event at Salem 1

At 12:21 a.m. on February 25, 1983, a low-low water level condition in one of the four steam generators at Salem 1 initiated a reactor trip signal in the reactor protection system. At the time, the reactor was at 12% rated thermal power in preparation for power escalation after a recently completed refueling outage. Upon receipt of the valid reactor trip signal, both of the redundant reactor trip breakers failed to open (opening of either reactor trip breaker would have caused the reactor to trip). About 25 seconds later, operators manually initiated a reactor trip from the control room. The reactor trip breakers opened as a result of the manual trip signal and this resulted in insertion of all control rods and shutdown of the reactor. Following the manual trip, the plant was stabilized in the hot standby condition. All other systems functioned as designed. Approximately two hours after the Salem 1 event, the cause of the failure to trip was determined by licensee instrumentation technicians to be failure of the UV trip device in both reactor trip breakers to function as designed. The plant was placed in cold shutdown at the request of the NRC.

On February 26, 1983, NRC investigators discovered that a similar failure had occurred on at Salem 1 on February 22, 1983. Based on a computer printout of February 22 events, it was evident that on that day (as on February 25) the two reactor trip breakers failed to open upon receipt of an automatic trip signal from the reactor protection system. The operators initiated a manual trip even though they were unaware that the automatic trip had failed.

As a result of the manual reactor trips on both February 22 and February 25, no adverse consequences occurred and the reactor was in a safe condition. However, as the first actual ATWS events, the Salem 1 events were of major safety concern.

Other pressurized water reactors (PWRs) have experienced reactor trip breaker failures, both before and after the February 1983 Salem 1 events. None of them however, involved an ATWS event. The reactor trip breaker failures prior to the February 1983 events at Salem 1 had been the subject of several actions taken since 1971 by the AEC/NRC, Westinghouse, and General Electric.

Due to the serious nature of Salem 1 ATWS event, the NRC issued Inspection and Enforcement Bulletin No. 83-01[7] on the same day (on February 25, 1983) to all PWR licensees for action and to other nuclear power reactor facilities for information. Subsequent initiatives on the part of NRC and industry identified and corrected potential deficiencies in reactor trip breakers and related maintenance procedures at several other plants as described in Appendix 2B.

Because of previously identified problems at Salem and the licensee's failure to recognize that an ATWS event had occurred on February 22, 1983, the NRC did not permit the Salem plants to restart until both technical and management corrective actions were satisfactory addressed. On April 26, 1983, the NRC agreed that the plants could be returned to service; however, on May 5, 1983, the NRC forwarded to the Salem licensee a Notice of Violation and Proposed Imposition of Civil Penalties (for \$850,000).[8] Violations included operation of the reactor even though the reactor protection system could not be considered operable, and several significant deficiencies which contributed to the inoperability of the reactor trip breakers. Region I instituted an augmented inspection program at Salem to monitor the licensee's progress towards completion of longer term corrective actions, including independent management consultants' recommendations.

The special NRC task force prepared a two-volume report, NUREG-1000.[9] The first volume dealt with the generic implications of the Salem events. The second volume documented the NRC actions to be taken based on the work of the task force. The results of the task force were considered in deliberations regarding the ATWS position and rule, which was being developed by the NRC.

2.7.1.8 10 CFR 50.62, The ATWS Rule

On November 24, 1981, 15 months before the Salem 1 ATWS event, the NRC invited comments on three proposed ATWS rules.[10] Each of the three alternatives had the objective of reducing risk from ATWS and each featured a different approach to achieve that objective. One alternative, the Staff Rule would have resolved ATWS by establishing performance criteria. For example, there would be analyses to verify that Service Level C of the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code would not be exceeded, fuel integrity would be maintained, there would be no excessive radioactivity release, the containment would not fail, and long-term shutdown and cooling would be assured. The second alternative, the Hendrie Rule, while using much of the same information base as the Staff Rule, proposed to resolve ATWS by establishing a reliability assurance program for systems that prevent or mitigate ATWS accidents and prescribing certain hardware modifications. The third alternative, the Utility Rule, was proposed by the Utility Group on ATWS in their petition for an ATWS rulemaking. The Utility Rule prescribed specific modifications that were keyed to the type of reactor and its manufacturer.

In July 1982 a Task Force and Steering Group of NRC personnel from several offices was formed to consider comments received on the three proposals and to develop a final rule on ATWS. The vast majority of the commentors felt that the approach of the Staff Rule was too open-ended in terms of costs to resolve ATWS (e.g., the analyses could be very costly and time consuming). The Hendrie Rule was found difficult to interpret by most commentors. The ATWS Steering Group opted to evaluate generic plants, in a fashion similar to the Utility Group approach, and define the various fixes and estimate the reduction in probability for ATWS sequences as each additional requirement was added. This gave a value (reduction in risk) that could be compared to the impact (cost in dollars) of each incremental requirement. Although, there are large uncertainties in such analyses, they proved useful in evaluating the various modifications proposed for resolving ATWS. Appendix 2B reproduces the final ATWS rule and also discusses the key changes that were considered.[11]

In view of the redundancy provided in existing reactor trip systems, the equipment required by the ATWS rule did not have to be redundant within itself. Also, since the combination of an anticipated operational occurrence, failure of the existing reactor trip system, and a seismic event or an event which results in significant plant physical damage has a low probability, seismic qualification and physical separation criteria were not applied to the equipment required by the ATWS rule. The NRC staff provided guidance on quality assurance for non-safety related equipment required by the ATWS rule.

The Salem 1 ATWS event occurred in February 1983, before the final ATWS rule was published in November 1983. One of the principal findings regarding the Salem 1 ATWS event was the lack of adequate attention being paid to the reliability of the reactor trip system. The Salem Generic Issues Task Force recommended to the Commission that a reliability assurance program be included in the final ATWS rule.[9] While the ATWS rule did not require such a program, the Commission strongly urged the voluntary development of a reliability assurance program.

The Commission stressed that ATWS risk reductions can also be achieved by reducing the frequency of transients which call for the reactor protection system to operate. Challenges to the reactor protection system may arise from unreliable components, inadequate post-trip reviews, poor testing, or tolerance of inadequate or degraded control systems. Operating experience in Japan indicated a transient frequency that was substantially less than in the United States. Utilities had categorized transients for over ten years but had not specifically instituted a program to reduce them. While not specifically required by the ATWS rule, the Commission urged licensees to analyze challenges to the plant safety systems, particularly the reactor trip system, and determine how improvements could be made.[13] Industry response to this challenge has been positive as indicated in Figure 2.7-1.

2.7.2 Auxiliary Feedwater Reliability

The auxiliary feedwater system (AFWS) normally operates during startup, hot standby and shutdown to provide feedwater to PWR steam generators. In conjunction with a Seismic Category I water source, it also functions as an emergency system for the removal of heat from the primary system when the main feedwater system is not available for emergency conditions including small LOCAs. The AFWS operates over a time period sufficient either to hold the plant at hot standby for several hours or to cool down the primary system (at a rate not to exceed limits specified in technical specifications) to temperature and pressure levels at which the low pressure decay heat removal system can operate.

The Reactor Safety Study found the AFWS to be important in preventing certain core damage scenarios, and, the loss of auxiliary feedwater at TMI-2 reinforced concerns regarding the reliability of the AFWS. Prior to the accident at TMI-2 there was wide variance in design philosophy for auxiliary feedwater systems. In particular the degree of diversity and redundancy varied widely. Some multi-plant sites had only one auxiliary feedwater pump per plant with interconnections between units. Other plants had two motor driven and one turbine-driven pump.

The NRC reviews information provided on the AFWS in the applicant's Safety Analysis Report following the Standard Review Plan.[12] In July 1981, Section 10.4.9 of the Standard Review Plan required that, as part of their review, the NRC assure that an AFWS reliability analysis be performed in accordance with NUREG-0737[13] using the methodology defined in NUREG-0611[14] and NUREG-0635.[15] Such an analysis provides an estimate the AFWS reliability and indicates major contributors to AFWS failure for various loss of main feedwater transients.

As set forth in Standard Review Plan Section 10.4.9, an acceptable AFWS should have an unreliability in the range of 10^{-4} to 10^{-5}. Compensating factors such as other methods of accomplishing the safety functions of the AFWS or other reliable methods for cooling the reactor core during abnormal conditions may be considered to justify a larger unavailability of the AFWS.

In December 1986, additional regulatory guidance regarding auxiliary feedwater systems was set forth.[16] The new guidance called for operating plants to demonstrate a 10^{-4} unreliability using plant-specific data.

2.7.3 Station Blackout Rule

Station blackout is the complete loss of alternating current (AC) electrical power to the essential and nonessential switchgear buses in a nuclear power plant. Many safety systems required for reactor core cooling and containment heat removal depend on AC power; however, because station blackout requires multiple component failures, U.S. plants were not specifically designed (before the July 21, 1988 station blackout rule) to withstand station blackout. In 1975, the Reactor Safety Study showed that station blackout could be an important contributor to the total risk from nuclear power plant accidents.[17] As operating experience accumulated, the concern arose that the reliability of both the onsite and offsite emergency AC power systems might be less than originally anticipated. In 1979 the NRC designated station blackout as an unresolved safety issue. A task action plan for issue resolution (TAP A-44) was issued in July 1980, and work was begun to determine whether additional safety requirements were needed.

Operating plant data and several plant specific probabilistic studies yielded the quantitative information presented in Table 2.7-1 and the following important findings regarding station blackout.[18]

1. *The variability of estimated station blackout likelihood is potentially large, ranging from approximately 10^{-5} to 10^{-3} per reactor-year. A "typical" estimated frequency is on the order of 10^{-4} per reactor-year.*

2. *The capability to restore offsite power in a timely manner (less than 8 hours) can have a significant effect on accident consequences.*

3. *The redundancy of onsite AC power systems and the reliability of individual power supplies have a large influence on the likelihood of station blackout events.*

4. *The capability of the decay heat removal system to cope with long duration blackouts (greater than 2 hours) can be a dominant factor influencing the likelihood of core damage or core melt for the accident sequence.*

5. *The estimated frequency of station blackout events that result in core damage or core melt can range from approximately 10^{-6} to greater than 10^{-4} per reactor-year. A "typical" core damage frequency estimate is on the order of 10^{-5} per reactor-year.*

The station blackout rule 10 CFR 50.63,[19] which became effective on July 21, 1988, was promulgated to reduce the risk of severe accidents resulting from station blackout by: (a) maintaining highly reliable ac electric power systems; and (b) as additional defense in depth, assuring that plants can cope with a station blackout for a specified duration selected on a plant-specific basis.[20]

It should be noted that station blackout was not deemed to constitute an undue risk without the station blackout rule. It was recognized that even with the rule, station blackout may still remain an important contributor to residual risk. The station blackout rule was developed to enhance safety by accident prevention and thereby reduce the likelihood of a core damage accident being caused by a station blackout. Like the ATWS rule (Section 2.7.1) it recognizes and addresses the threat posed by common cause failures.

The station blackout rule identifies the reliability of onsite emergency ac power sources as being one of the main factors contributing to risk of core melt resulting from station blackout. Diesel generator units have been widely used as the power source for the onsite electric power systems. The NRC staff developed Regulatory Guide 1.155 entitled "Station Blackout," which presents guidance on (1) maintaining a high level of reliability for emergency diesel generators, (2) developing procedures and training to restore offsite and onsite emergency ac power should either one or both become unavailable, and (3) selecting a plant-specific acceptable station blackout duration that the plant would be capable of surviving without core damage. Application of the methods in this guide would result in selection of an acceptable station blackout duration (e.g. 2, 4, 8, or 16 hours) that depends on the specific plant design and site-related characteristics.

The station blackout rule allows utilities several design alternatives to ensure that an operating plant can safely shut down in the event that all ac power (offsite and onsite) is lost. The NRC staff prefers demonstrating compliance with 10 CFR 50.63 through the installation of a spare (full capacity) alternate ac power source of diverse design that is consistent with the guidance in Regulatory Guide 1.155 and is capable of powering at least one complete set of normal safe shutdown loads. Although an alternate ac power source is the preferred resolution to this issue in 10 CFR 50.63, NRC imposition would exceed current NRC regulations. For advanced LWRs the NRC staff has recommended that the NRC commissioners approve imposition of an alternate ac power source.

The resolution of the station blackout safety issue established the need for an emergency diesel generator (EDG) reliability program that has the capability to achieve and maintain the emergency diesel generator reliability levels in the range of 0.95 per demand or better to cope with station blackout. Explicit guidance in the areas of diesel-generator preoperational testing, periodic testing, and reporting requirements have been developed for meeting this reliability goal in a revision to Regulatory Guide 1.9,[21] which was prepared for the resolution of Generic Safety Issue B-56, "Diesel Reliability."

2.7.4 Safety Goal Policy and Backfitting

While risk importance began to be an important consideration in decision-making during the 1970s and early 1980s, the process was largely ad hoc, with no clear guidance concerning what risk levels were acceptable for any particular issue. A quantitative safety goal was first considered in conjunction with the ATWS issue as indicated in Section 2.7.1. Subsequently, as noted in Section 1.4, the TMI-2 investigators recommended that the NRC explicitly identify a safety goal -- a level of risk at which reactors would be safe enough. The NRC established both qualitative and quantitative safety goals in August 1986, to more clearly delineate acceptable levels of risk.[22] These safety goals are presented in Section 1.4.

The relatively low core damage frequencies generated in NUREG-1150 have implications for comparisons with the NRC Safety Goals. Because the core damage frequencies are relatively low, and the severe accident consequences are not unusually high, the five NUREG-1150 plants readily meet the two primary safety goals. Figure 2.7-2 shows comparisons with the safety goals for internally initiated accidents. Even considering the significant uncertainties, the five plants readily meet the safety goals. Plants with higher core damage frequencies may have more difficulty in meeting the goals.

The safety goal policy makes it clear that the quantitative safety goals are not hard and fast requirements (such as a rule would be) and are intended to apply to the industry as a whole, rather than individual plants. However, an actual safety goal implementation approach has not yet been well defined. Among the issues to consider are:

1. What computational PRA methods are to be used?

2. How are uncertainties to be treated?

3. How are seismic and other external events to be treated?

As of early 1992, these questions remain largely unanswered. Since 1986, the NRC has struggled with implementation and the possible inclusion of "subsidiary" safety goals. Of particular interest and controversy has been the large release goal contained in the 1986 policy statement:

"Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than 1 in 1,000,000 per year of reactor operation."

Details concerning the large release goal were left to the staff to develop. Subsequently, the Commission indicated that:

1. *The staff may partition the large release guideline and establish quantitative core damage frequency and containment performance objectives.*

2. *A core damage probability of less than 1 in 10,000 per reactor year of reactor operation appears to be a very useful subsidiary benchmark in making judgments about regulations directed toward accident prevention.*

This guidance has been controversial because:

1. There is not yet an accepted definition of a "large release," although one is being developed,

2. The large release and core damage probability goals are more restrictive (and thus subsume) the health effects goals in most cases,

3. PRA calculations of large release frequencies have large uncertainties, and

4. Many plants would not be expected to meet these subsidiary goals.

The second concern listed above relates to the hierarchical nature of the safety goals, starting with qualitative goals and proceeding through the quantitative health effects goals down to more detailed, subsidiary quantitative goals. The ACRS and others have raised concerns that the proposed goals are not self-consistent and that each successive layer in the hierarchy tends to subsume the previous layer.[23] For example, virtually all plants that meet the large release goal would be expected to meet all of the other goals. The question then becomes, "Why have the other goals?" The NRC recognizes this concern, but believes that the current approach is consistent with defense-in-depth (a 10^{-6} core damage frequency does not justify the absence of containment) and that an entirely self-consistent approach is not possible. In any case, these subsidiary goals are gaining acceptance because they are treated as targets and not firm requirements.

Despite the concerns noted above, implementation of the Safety Goal Policy is beginning to take shape in the form of guidance for backfitting. The evolution of the Backfit Rule was discussed in detail in Section 1.4. In January 1992, the NRC staff presented the Commission with an approach to use PRA results to achieve consistency between the Safety Goal Policy and the Backfit Rule.[24] The approach is based on comparison of the core damage frequency to 10^{-4} per year and the containment release frequency (as a surrogate for large release) to 10^{-6} per reactor year. Table 2.7-2 summarizes the interim implementation guidance. A proposed backfit would be evaluated in terms of core damage frequency and containment release frequency. Table 2.7-2 would be used to determine if the backfit warranted further analysis. Note that this guidance only deals with issues of enhanced protection; it is not necessary to consider the safety goals concerning questions of adequate protection or regulatory compliance.

Once a consistent approach for dealing with Safety Goals and Backfits is established, the NRC will have a means to consider backfits and safety issues in a systematic and consistent manner. The process for selecting backfit options will be clarified, and efforts can be focused on those issues most important to risk. While risk will not become the sole measure of the importance of an issue, it can be used to assure that issues are placed in their proper perspective. If a risk-based approach to backfitting is to be implemented, risk analyses must be available to the decision-makers, and the validity of those analyses clearly understood. In some cases, NRC-sponsored risk assessments and special studies can provide the needed information; however, another source of information is becoming available. That information source is the Individual Plant Examinations (IPEs).

2.7.5 Individual Plant Examinations

As noted in the discussion of the Severe Accident Policy in Section 1.4, the NRC recognized the desirability of performing a systematic examination of each nuclear power plant in order to identify potential plant-specific vulnerabilities to severe accidents.[25] Experience with probabilistic risk assessments has demonstrated that the undesirable risk from such vulnerabilities can often be reduced to an acceptable level by low-cost changes in procedures or minor design modifications. Three years after issuance of the Severe Accident Policy, after considerable planning and discussions of severe accident issues with industry representatives, the NRC issued a generic letter (88-20) and guidance (NUREG-1335), which called for licensees to perform a systematic Individual Plant Examination (IPE) of each nuclear power plant operating or under construction.[26,27] The stated purpose of the IPE was to have each utility

1. develop an appreciation of severe accident behavior;
2. understand the most likely severe accident sequences that could occur at its plant;
3. gain a more quantitative understanding of the overall probabilities of core damage and fission product releases; and
4. if necessary, reduce the overall probabilities of core damage and fission product releases by modifying, where appropriate, hardware and procedures that would help prevent or mitigate severe accidents.

The Generic Letter does not prescribe a particular method for performing the IPE, but indicates some methods (such as those used in NUREG-1150) that are considered acceptable and further states that other methods will be considered, provided that the selected method is capable of identifying important severe accident vulnerabilities.

The IPE Generic Letter does not require the IPE to be a full scope PRA. No estimate of offsite consequences is required. Estimates of core damage frequency are required, along with fission product release probabilities (source term). Estimates of uncertainty are not required; only best estimates must be submitted. The IPE Generic Letter requires consideration of accidents initiated internally to the plant, including internal floods. Accidents initiated externally to the plant (seismic, tornado, etc.) and internal fires are excluded. These external initiators are being addressed in a supplement to the IPE Generic Letter dealing with Individual Plant Examinations for External Events (IPEEE).[28] Guidance for the IPEEEs is still evolving, but is likely to require a less rigorous approach than used for the IPE activities.[29]

Independent of the Generic Letter guidance, some utilities are likely to perform full scope PRAs, including external events, because they believe that the results have multiple benefits to the plant. All plants are being required to develop accident management programs, and a full scope PRA will facilitate this effort. A full scope PRA also allows a stronger case to be made in licensing decisions.

IPE results were to be reported to the NRC within three years according to guidance provided in NUREG-1335. The results of the IPEs that have been received are currently being reviewed by the NRC. These results will be used, in part, to deal with Unresolved Safety Issues and Generic Safety Issues. The IPE submittals will indicate whether particular issues apply to the plant and the utility's case for resolution. If vulnerabilities are found, the utility is to provide a plan and schedule for resolving the problem. Both the Safety Goal Policy and the Backfit Rule will influence the utility approach for identifying and resolving severe accident vulnerabilities and provide a partial framework for NRC evaluation of utility conclusions and proposals

TABLE 2.7.1
STATION BLACKOUT SUMMARY DATA

Operational Experience	
Loss of offsite power (occurrences per year)	
Average	0.1
Range	0 to 0.4
Time to restore offsite power (hours)	
Median	0.6
90% restored	3.0
Emergency diesel generator reliability (per demand)	
Average	0.98
Range	0.9 to 1.0
Emergency Diesel Generator Repair Time (hours)	
Median	8
Analytical Results	
Estimated range of unavailability of emergency AC power systems (per demand)	10^{-4} to 10^{-2}
Estimated range of frequency of station blackout (per year)	10^{-5} to 10^{-3}
Estimated range of frequency of core damage as a result of station blackout (per year)	10^{-6} to 10^{-4}

Table 2.7-2. Safety Goal Implementation Guidance

Change in Core Damage Frequency (ΔCDF)	1E-02 – 1E-01	1E-01 – 1
1E-03 – 1E-04	Proceed to Cost Benefit Analysis	Proceed to Cost Benefit Analysis (Priority)
1E-04 – 1E-05	Management Decision Whether to [illegible]ed to Cost Benefit [illegible]alysis	Proceed to Cost Benefit Analysis
1E-05 – 1E-06	No Action	Management Decision Whether to Proceed to Cost Benefit Analysis

Estimated Conditional Containment Failure Probability (CCFP)

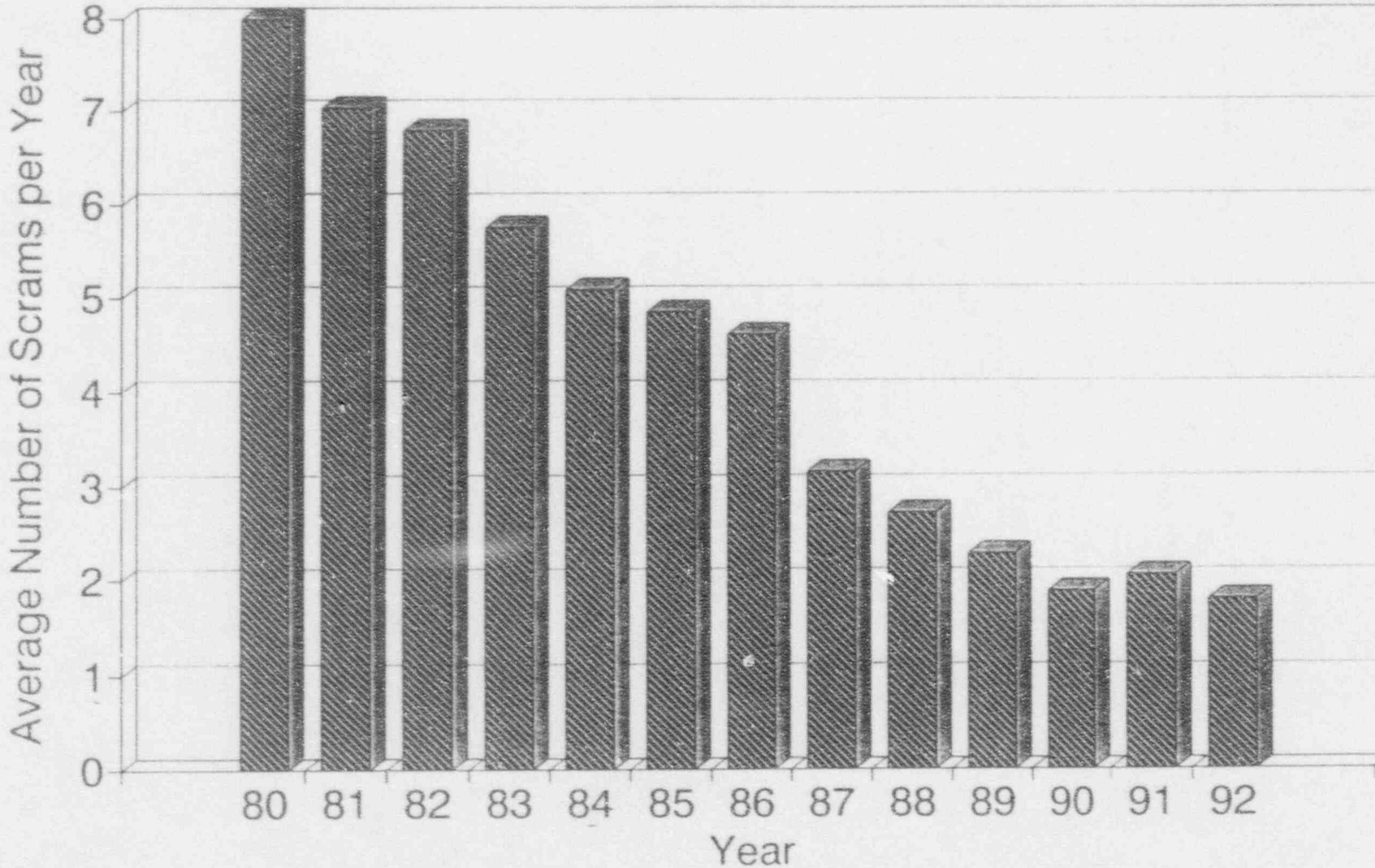


Figure 2.7-1 Average Number of Scrams per Year

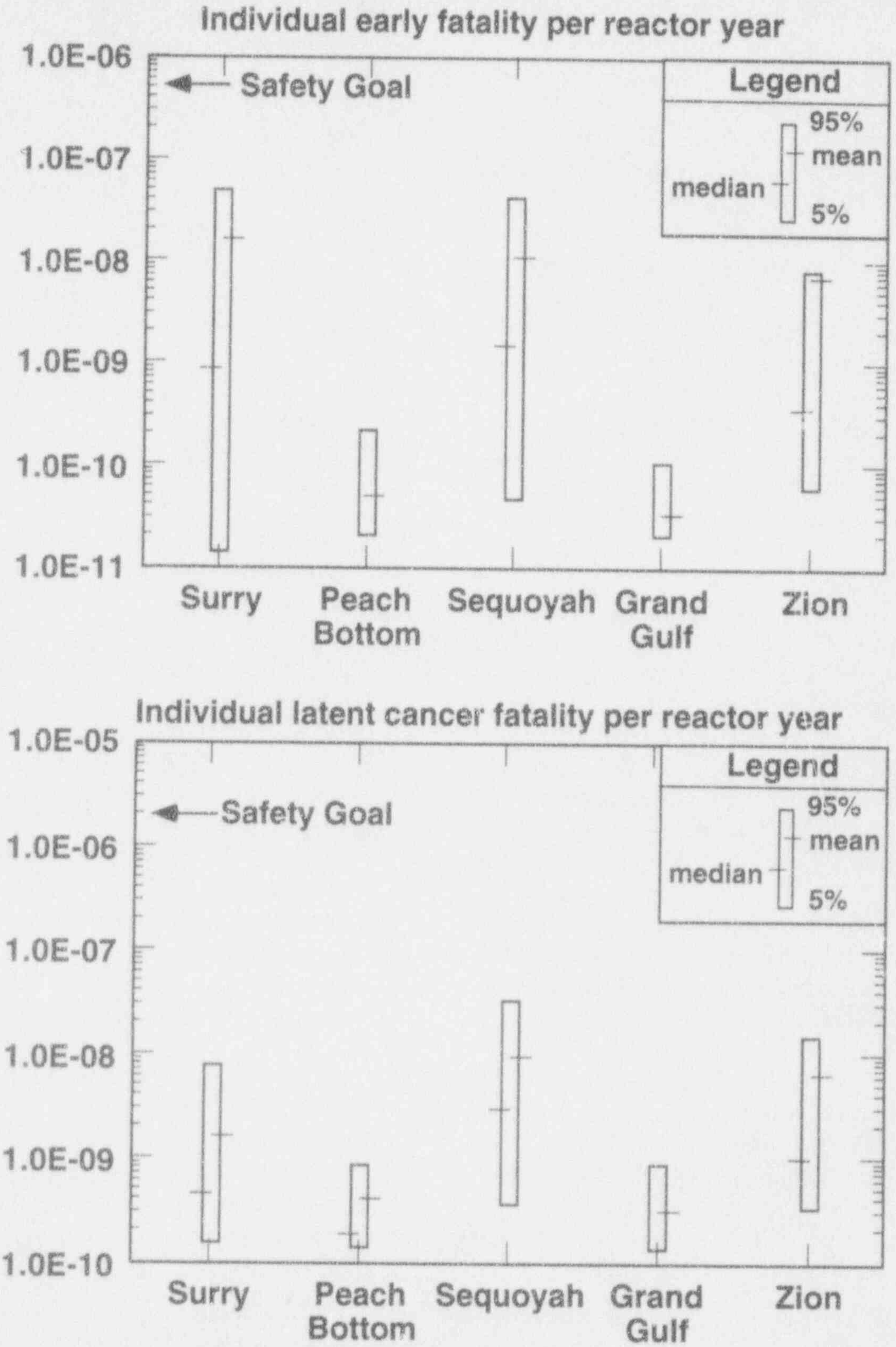


Figure 2.7-2 Individual early and latent cancer fatality risks (internal initiators)

References for Section 2.7

1. Long Island Lighting Company, 18 NRC 445, 464-65 (1983).

2. Union of Concerned Scientists v. U.S. NRC, 824 F.2d 108 (DC Cir 1987).

3. David Okrent, *Nuclear Reactor Safety: On the History of the Regulatory Process*, The University of Wisconsin Press, Madison, WI, 1981, p239.

4. U.S. Atomic Energy Commission Regulatory Staff, "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors," WASH-1270, September 1973.

5. U. S. Nuclear Regulatory Commission Staff Report, "Anticipated Transients Without Scram for Light Water Reactors, NUREG-0460, December, 1978.

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

7. U.S. Nuclear Regulatory Commission, Inspection and Enforcement Bulletin No. 83-01, "Failure of Reactor Trip Breakers (Westinghouse DB-50) to Open on Automatic Trip Signal," February 25, 1983.

8. Letter from Richard C. DeYoung, Director, NRC Office of Inspection and Enforcement, to Robert Smith, Chairman of the Board, Public Service and Gas Company, transmitting a Notice of Violation and Proposed Imposition of Civil Penalties, Docket Nos. 50-272 and 50-311 (May 5, 1983).

9. U.S. Nuclear Regulatory Commission, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," USNRC Report NUREG-1000, Vol. 1, (April 1983).

10. 46 FR 57521, Proposed ATWS Rule, November 24, 1981.

11. 49 FR 26036, Statement of Considerations for ATWS Rule, June 26, 1984.

12. U. S. Nuclear Regulatory Commission Standard Review Plan, Office of Nuclear Reactor Regulation, NUREG-0800, Section 10.4.9, Rev. 2, July 1981.

13. NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980, Item II.E.1.1.

14. NUREG-0611 "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants," January 1980, Appendix III and Annex 1 of Appendix X.

15. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants," January 1980, Appendix III and Annex 1 of Appendix X.

16. NUREG-0933, "A Prioritization of Generic Safety Issues", December 1986.

17. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, WASH-1400, October 1975.

18. NUREG-1032, "Evaluation of Station Blackout Accidents at Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-44, June 1988, p. 1-1.

19. 10 CFR 50.63, "Loss of All Alternating Current Power," July 21, 1988.

20. 53 FR 23203, Statement of Considerations for Final Station Blackout Rule, June 21, 1988.

21. Regulatory Guide 1.9, "Selection, Design, Qualification, Testing, and Reliability of Diesel Generator Units Used as Class 1E Onsite Electric Power Systems at Nuclear Power Plants, Working Draft, November 28, 1989.

22. Title 10, Code of Federal Regulations, Part 50, "Safety Goals for the Operation of Nuclear Power Plants; Policy Statement," August 4, 1986.

23. Letter from the Advisory Committee on Reactor Safeguards to Lando W. Zech, Jr., "ACRS Comments on an Implementation Plan for the Safety Goal Policy," May 13, 1987.

24. Presentation by the Steering Group on Regulatory Analysis to the Commission, "Interim Guidance on Staff Implementation of the Commission's Safety Goal Policy," January 17, 1992.

25. 50 Federal Register 32138, August 8, 1985.

26. United States Nuclear Regulatory Commission, Title 10, Code of Federal Regulations, Part 50.54 (f), Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities, November 23, 1988.

Individual Plant Examination: Submittal Guidance, NUREG-1335, August 1989.

IPEEE Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities, 10 CFR 50.54(f)" August 29, 1989.

NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities", June 1992.

APPENDIX 2A DAVIS-BESSE LOSS OF FEEDWATER

The one-unit Davis-Besse nuclear power plant is located in Oak Harbor, Ohio. The plant is operated by the Toledo Edison Company. The plant consists of one Babcock & Wilcox PWR designed for a maximum operational power of 874 MWe. The Davis-Besse plant has been in operation since July of 1978. Key systems of the Davis-Besse plant are depicted in Figures 2A-1 through 2A-6.

The following sections describe a loss-of-feedwater incident that occurred at the Davis-Besse plant. In view of the importance of the operator actions in this event, the description is a narrative based upon a composite of the operator interviews performed by an NRC review team following the incident (NUREG-1154). The review team decided that this would best convey the effects of stress, training, experience, teamwork, and impediments on operator performance.

The following text is extracted directly from NUREG-1154.

2A.1 Initiating Events

On June 9, 1985, the midnight shift of operators assumed control of the Davis-Besse nuclear power plant. The oncoming shift included four licensed operators, four equipment operators, an auxiliary operator, and an administrative assistant. The shift supervisor and the assistant shift supervisor are licensed senior reactor operators and the most experienced members of the operating crew. Both were at the plant before it was issued an operating license in April 1977. The reactor operators, who were responsible for the control room, had decided between themselves who would be responsible for the primary-side and who would take the secondary-side work stations. The secondary-side operator had been a licensed reactor operator for about two years. The primary-side operator was licensed in January 1985; he had previous nuclear Navy experience and was an equipment operator before being licensed. Prior to the morning of June 9, neither reactor operator had been at the controls during a reactor trip at Davis-Besse.

The four equipment operators are a close-knit group, three of whom had been operators in the nuclear Navy. Their experience at the plant ranges from three to nine years, averaging six-and-one-half years per operator. Equipment operators receive directions from the control room operators to manipulate and troubleshoot equipment in the reactor auxiliary building and the turbine building. Generally, equipment operators occupy this position temporarily as they participate in a development program leading to the position of licensed operator. However, two equipment operators did not intend to become licensed operators.

The shift turnover of June 9 was easy, there were no ongoing tests or planned changes to plant status. The plant was operating at 90% of the full power authorized in the license granted by the NRC in April 1977, to minimize the potential for an inadvertent reactor trip due to noise on primary coolant flow instrumentation. All the major equipment control stations were running on automatic except the No. 2 main feedwater pump. As a result, the integrated control system instruments were monitoring and controlling the balance between the plant's reactor *coolant system and the secondary coolant system.*

Since April 1985, there had been control problems with both main feedwater pumps. Troubleshooting had not identified or resolved the problems. In fact, a week earlier, on June 2, 1985, both feedwater pumps tripped unexpectedly after a reactor trip. After some additional troubleshooting, the decision was made to not delay startup any longer, but to put instrumentation on the pumps to help diagnose the cause of a pump trip, if it occurred again. As a precaution, the number two main feedwater pump was operating in manual control to prevent it from tripping and to ensure that all main feedwater would not be lost should the reactor trip. Some operators were uneasy about going up to power with problems in the feedwater pumps, but they complied with the decisions made by their management.

During the first hour of the shift, the operators' attention and thoughts were directed to examining the control panels and alarm panels, and performing instrument checks and routine surveillance associated with shift turnover. Thus, at 1:35 in the morning, the plant generator was providing electricity to the Ohio countryside. The secondary-side operator had gone to the kitchen where he joined an equipment operator for a snack. The other reactor operator was at the operator's desk studying procedures for requalification examinations. The assistant shift supervisor had just left the kitchen on his way back to the control room after a break. The shift supervisor was in his office outside the control room performing administrative duties.

2A.2 Reactor Trip - Turbine Trip

The assistant shift supervisor entered the control room and was examining one of the consoles when he noticed that main feedwater flow was decreasing and that the No. 1 main feedwater pump had tripped. Since the No. 2 feedwater pump was in manual control, it could not respond to the integrated control system demand automatically to increase feedwater flow.

The "winding down" sound of the feedwater pump turbine was heard by the reactor operator in the kitchen, and by the administrative assistant and the shift supervisor, both of whom were in their respective offices immediately outside the control room. They headed immediately for the control room -- the event had begun.

The secondary-side reactor operator ran to his station and immediately increased the speed of the No. 2 main feedwater pump to compensate for the decrease of feedwater flow from the No. 1 pump. The primary-side operator had already opened the pressurizer spray valve in an attempt to reduce the pressure surge resulting from the heatup of the reactor coolant system due to a decrease in feedwater flow.

The plant's integrated control system attempted automatically to reduce reactor/turbine power in accordance with the reduced feedwater flow. The control rods were being inserted into the core and reactor power had been reduced to about 80%. At the same time the primary-side reactor operator held open the pressurizer spray valve in an attempt to keep the reactor coolant pressure below the high pressure reactor trip set point of 2300 psig (normal pressure is 2150 psig). However, the reduction of feedwater and subsequent degradation of heat removal from the *primary coolant system caused the reactor to trip on high reactor coolant pressure. The operators had done all they could do to prevent the trip, but the safety systems had acted automatically to shut down the nuclear reaction.*

The primary-side operator acted in accordance with the immediate post-trip actions specified in the emergency procedure that he had memorized. Among other things, he checked that all control rod bottom lights were on, hit the reactor trip (shutdown) button, isolated letdown from the reactor coolant system, and started a second makeup pump to anticipate a reduced pressurizer inventory after a normal reactor trip. Then he waited, and watched the reactor coolant pressure to see how it behaved.

The secondary-side operator heard the turbine stop valves slamming shut and knew the reactor had tripped. This "thud" was heard by most of the equipment operators who also recognized its meaning and two of them headed for the control room. Almost simultaneously, the secondary-side operator heard the loud roar of main steam safety valves opening, a sound providing further proof that the reactor had tripped. The lifting of safety valves after a high-power reactor trip was normal. Everything was going as expected as he waited and watched the steam generator water levels boil down - each should reach the normal post-trip low level limit of 35 inches on the startup level instrumentation and hold steady.

The shift supervisor joined the operator at the secondary-side control console and watched the rapid decrease of the steam generator levels. The rapid feedwater reduction system (a subsystem of the integrated control system) had closed the startup feedwater valves, but as the level approached the low level limits, the startup valves opened to hold the level steady. The main steam safety valves closed as expected. The system response was looking "real good" to the shift supervisor.

The assistant shift supervisor in the meantime opened the plant's looseleaf emergency procedure book. (It is about two inches thick, with tabs for quick reference. The operators refer to it as emergency procedure 1202:01; the NRC refers to it as the ATOG procedure -Abnormal Transient Operating Guidelines) As he read aloud the immediate actions specified, the reactor operators were responding in the affirmative. After phoning the shift technical advisor (STA) to come to the control room, the administrative assistant began writing down what the operators were saying, although they were speaking faster than she could write.

The STA was working a 24-hour shift and was asleep when awakened by a telephone call from the shift supervisor, which was followed immediately by the call from the administrative assistant. (The STAs are provided an apartment-type room in the administrative building, which is outside the protected area about one-half mile from the plant. According to procedures, they must be able to get to the control room within 10 minutes of being called.) He had detected a sense of urgency in the telephone calls and so he ran out of the building to his car for the drive to the site. He was anxious himself -- this was his first reactor trip since becoming a shift technical advisor in January 1985.

2A.3 Loss of Main Feedwater

Although the assistant shift supervisor was loudly reading the supplementary actions from the emergency procedure book, the shift supervisor heard the main steam safety valves open again. He knew from experience that something was unusual and instinctively surveyed the control console and panel for a clue. He discovered that both main steam isolation valves (MSIVs) had closed -- the first and second of a list of unexpected equipment performances and failures that occurred during the event.

The secondary-side operator was also aware that something was wrong because he noticed that the speed of the only operating main feedwater pump was decreasing. After verifying that the status of the main feedwater pump turbine was normal, he concluded that the turbine was losing steam pressure at about the same time that the shift supervisor shouted that the MSIVs were closed. All eyes then turned up to the annunciators at the top of the back panel. They saw nothing abnormal in the kind or number of annunciators lit after the reactor trip. The operators expected to find an alarm indicating that the Steam Feedwater Rupture Control System (SFRCS, pronounced S-FARSE) had activated. Based on their knowledge of previous events at the plant, they believed that either a partial or full actuation of the SFRCS had closed the MSIVs. However, the SFRCS annunciator lights were dark. The MSIVs had closed at 1:36 a.m. and they were going to stay closed. It normally takes at least one-half hour to prepare the steam system for reopening the valves.

The No. 2 main feedwater pump turbine, deprived of steam, was slowly winding down. Since the MSIVs were closed and there was limited steam inventory in the moisture separator reheaters, there was inadequate motive power to pump feedwater to the steam generators. At about 1:40 a.m., the discharge pressure of the pump had dropped below the steam pressure which terminated main feedwater flow.

2A.4 Loss of Emergency Feedwater

The secondary-side operator watched the levels in both steam generators boil down; he had also heard the main steam safety valves lifting. Without feedwater, he knew that an SFRCS actuation on low steam generator level was imminent. The SFRCS should actuate the auxiliary feedwater system (AFWS) which in turn should provide emergency feedwater to the steam generators. He was trained to trip manually any system that he felt was going to trip automatically. He requested and received permission from the shift supervisor to trip the SFRCS on low level to conserve steam generator inventory, i.e., the AFWS would be initiated before the steam generator low-level setpoint was reached.

He went to the manual initiation switches at the back panel and pushed two buttons to trip the SFRCS. He inadvertently pushed the wrong two buttons and, as a result, both steam generators were isolated from the emergency feedwater supply. He had activated the SFRCS on low pressure for each steam generator instead of on low level. By manually actuating the SFRCS on low pressure, the SFRCS was signalled that both generators had experienced a steamline break or leak and the system responded, as designed, *to isolate both steam generators. The operator's anticipatory action defeated the safety function of the auxiliary feedwater system -- a common-mode failure and the third abnormality to occur within 6 minutes after the reactor trip.*

The operator returned to the auxiliary feedwater station expecting the AFWS to actuate and provide the much-needed feedwater to the steam generators that were boiling dry. Instead, he first saw the No. 1 AFW pump, followed by the No. 2 AFW pump trip on overspeed - a second common-mode failure of the auxiliary feedwater system and abnormalities four and five. He returned to the SFRCS panel to find that he had pushed the wrong two buttons.

The operator knew what he was supposed to do. In fact, most knowledgeable people in the nuclear power industry, even control room designers, know that the once-through steam generators in Babcock & Wilcox-designed plants can boil dry in as little as 5 minutes; consequently, it is vital for an operator to be able to quickly start the AFWS. There could have been a button labeled simply "AFWS--Push to start." But instead, the operator had to do a mental exercise to first identify a signal in the SFRCS that could indirectly start the AFW system, find the correct set of buttons from a selection of five identical sets located knee-high from the floor on the back panel, and then push them without being distracted by the numerous alarms and loud exchanges of information between operators.

The shift supervisor quickly determined that the valves in the AFWS were improperly aligned. He reset the SFRCS, tripped it on low level, and corrected the operator's error about one minute after it occurred. This action commanded the SFRCS to realign itself such that each AFW pump delivered flow to its associated steam generator. Thus, had both systems (the AFWS and SFRCS) operated properly, the operator's mistake would have had no significant consequences on plant safety.

The assistant shift supervisor, meanwhile, continued reading aloud from the emergency procedure. He had reached the point in the supplementary actions that require verification that feedwater flow was available. However, there was no feedwater, not even from the AFWS, a safety system designed to provide feedwater in the situation that existed. (The Davis-Besse emergency plan identifies such a situation as a Site Area Emergency.) Given this condition, the procedure directs the operator to the section entitled, "Lack of Heat Transfer." He opened the procedure at the tab corresponding to this condition, but left the desk and the procedure at this point to diagnose why the AFWS had failed. He performed a valve alignment verification and found that the isolation valve in each AFW train had closed. Both valves (AF-599 and AF-608) had failed to reopen automatically after the shift supervisor had reset the SFRCS. He tried unsuccessfully to open the valves by pressing the buttons on the back panel. He went to the SFRCS cabinets in the back of the control panel to clear any trips in the system and block them so that the isolation valves could open. However, there were no signals keeping the valves closed. He concluded that the torque switches in the valve operators must have tripped. The AFW system had now suffered its third *common-mode failure, thus increasing the number of malfunctions to seven within 7 minutes after the reactor trip (1:42 a.m.).*

2A.5 Reactor Coolant System Heatup

Meanwhile, about 1:40 a.m., the levels in both steam generators began to decrease below the normal post-reactor-trip limits (about 35 inches on the startup range). The feedwater flow provided by the No. 1 main feedwater pump had terminated. The flow from the No. 2 main feedwater pump was decreasing because the MSIVs were closed, which isolated the main steam supply to the pump. With decreasing feedwater flow, the effectiveness of the steam generators as a heat sink for removing decay (i.e., residual) heat from the reactor coolant system rapidly decreased. As the levels boiled down through the low level setpoints (the auxiliary feedwater should automatically initiate at about 27 inches), the average temperature of the reactor coolant system began to increase, indicating a lack of heat transfer from the primary to the secondary coolant systems. When the operator incorrectly initiated SFRCS on low pressure, all feedwater was isolated to both steam generators. The reactor coolant system began to heat up because heat transfer to the steam generators was essentially lost due to loss of steam generator water level.

The average reactor coolant temperature increased at the rate of about 4°F/minute for about 12 minutes. The system pressure also increased steadily until the operator fully opened the pressurizer spray valve (at about 1:42 a.m.). The spray reduced the steam volume in the pressurizer and temporarily interrupted the pressure increase. The pressurizer level increased rapidly but the pressurizer did not completely fill with water. As the indicated level exceeded the normal value of 200 inches, the control valve for makeup flow automatically closed.

At this point, things in the control room were hectic. The plant had lost all feedwater; reactor pressure and temperature were increasing; and a number of unexpected equipment problems had occurred. The seriousness of the situation was fully appreciated.

2A.6 Operator Actions

By 1:44 a.m., the licensed operators had exhausted every option available in the control room to restore feedwater to the steam generators. The main feedwater pumps no longer had a steam supply. Even if the MSIVs could be opened, the steam generators had essentially boiled dry, and sufficient steam for the main feedwater pump turbines would likely not have been available. The turbines for the AFW pumps had tripped on overspeed, and the trip throttle valves could not be reset from the control room. Even if the AFW pumps had been operable, the isolation valves between the pumps and steam generators could not be opened from the control room, which also inhibited the AFWS from performing its safety function. The likelihood of providing emergency feedwater was not certain, even if the AFW pump overspeed trips could be reset and the flow path established. For example there was a question as to whether there was enough steam remaining in the steam generators to start the steam driven pumps. Unknown to the operators, the steam inventory was further decreased because of problems controlling main steam pressure. The number of malfunctions had now reached eight.

Three equipment operators had been in the control room since shortly after the reactor tripped. They had come to the control room to receive directions and to assist the licensed operators as necessary. They were on the sidelines watching their fellow operators trying to gain control of the situation.

The safety-related AFW equipment needed to restore water to the steam generators had failed in a manner that could only be remedied at the equipment location and not from the control room. The affected pumps and valves are located in locked compartments deep in the plant.

The primary-side reactor operator directed two of the equipment operators to go to the auxiliary feedwater pump room to determine what was wrong -- and to hurry.

The pump room, located three levels below the control room, has only one entrance: a sliding grate hatch that is locked with a safety padlock. One of the operators carried the key ring with the padlock key in his hand as they left the control room. They violated the company's "no running" policy as they raced down the stairs. The first operator was about 10 feet ahead of the other operator who tossed him the keys so as not to delay unlocking the auxiliary feedwater pump room. The operator ran as fast as he could and had unlocked the padlock by the time the other operator arrived to help slide the hatch open.

The operators descended the steep stairs resembling a ladder into the No. 2 AFW pump room. They recognized immediately that the trip throttle valve had tripped. One operator started to remove the lock wire on the handwheel while the other operator opened the water-tight door to the No. 1 AFW pump. He also found the trip throttle valve tripped and began to remove the lock wire from the handwheel.

The shift supervisor had just dispatched a third equipment operator to open AFW isolation valves AF-599 and AF-608. These are chained and locked valves, and the shift supervisor gave the lock-valve key to the operator before he left the control room. He paged a fourth equipment operator over the plant communications systems and directed him also to open valves AF-599 and AF-608. Although the operators had to go to different rooms for each valve, they opened both valves in about 3 1/2 minutes. They were then directed to the AFW pump room.

As operators ran to the equipment, a variety of troubling thoughts ran through their minds. One operator was uncertain if he would be able to carry out the task that he had been directed to do. He knew that the valves he had to open were locked valves, and they could not be operated manually without a key. He did not have a key and that concerned him. As he moved through the turbine building, he knew there were numerous locked doors that he would have to go through to reach the valves. He had a plastic card to get through the card readers, but they had been known to break and fail. He did not have a set of door keys and he would not gain access *if his key card broke and that concerned him too.*

The assistant shift supervisor came back into the control console area after having cleared the logic for the SFRCS and he tried again, unsuccessfully, to open the AFWS isolation valves. At this point, the assistant shift supervisor made the important decision to attempt to place the startup feedwater pump (SUFP) in service to supply feedwater to the steam generators. He went to the key locker for the key required to perform one of the five operations required to get the pump running.

The SUFP is a motor-driven pump, usually more reliable than a turbine-driven pump, and more importantly, it does not require steam from the steam generators to operate. The SUFP is located in the same compartment as the No. 2 AFW pump. But since the refueling outage in January 1985, the SUFP had been isolated by closing four manual valves and its fuses were removed from the motor control circuit. This isolation was believed necessary because of the consequences of a high energy break of the non-seismic grade piping which passes through the two seismic-qualified AFW pump rooms. Prior to January 1985, the SUFP could be initiated from the control room by the operation of a single switch.

The assistant shift supervisor headed for the turbine building where he opened the four valves and placed fuses in the pump electrical switchgear. This equipment is located at four different places; in fact, other operators had walked through the procedure of placing the SUFP in operation and required 15 to 20 minutes to do it. The assistant shift supervisor took about 4 minutes to perform these activities. He then paged the control room form the AFW pump room and instructed the secondary-side operator to start the pump and align it with the No. 1 steam generator.

The two equipment operators in the AFW pump rooms had been working about 5 minutes to reset the trip throttle valves when the assistant shift supervisor entered the room to check the SUFP. The equipment operators thought that they had latched and opened the valves. However, neither operator was initially successful in getting the pumps operational. Finally, after one equipment operator had tried everything that he knew to get the No. 1 AFW pump operating, he left it and went to the No. 2 AFW pump where the other operator was having the same problem of getting steam to the turbine. Neither operator had previously performed the task that he was attempting.

The assistant shift supervisor went over to assist the equipment operators and noticed immediately that the trip throttle valves were still closed. Apparently, the equipment operators had only removed the slack in attempting to open the valve. The valve was still closed and the differential pressure on the wedge disk made it difficult to turn the handwheel after the slack was removed, thus necessitating the use of the valve wrench. A third, more experienced operator had entered the pump room and used a valve wrench to open the trip throttle valve on AFW pump No. 2. Without the benefit of such assistance the equipment operators may well have failed to open the trip throttle valves to admit steam to the pump turbines.

The third equipment operator then proceeded to the No. 1 AFW pump trip throttle valve. The valve had not been reset properly and he experienced great difficulty in relatching and opening it because he had to hold the trip mechanism in the latched position and open the valve with the valve wrench. Because the trip mechanism was not reset properly, the valve shut twice before he finally opened the valve and got the pump operating.

2A.7 PORV Failure

Prior to being informed by the assistant shift supervisor that the SUFP was available, the secondary-side operator requested the primary-side operator to reset the isolation signal to the startup feedwater valves in preparation for starting the SUFP. In order to perform this task, the operator left the control console and went to the SFRCS cabinets in back of the control room. As he re-entered the control panel area, he was requested to reset the atmospheric vent valves. As a result of these activities the primary side operator estimated that he was away from his station for 20 to 30 seconds. (In fact, he was away for about two minutes.)

While the operator was away from the primary-side control station, the pressurizer PORV opened and closed twice without his knowledge. The pressure had increased because of the continued heatup of the reactor coolant system that resulted when both steam generators had essentially boiled dry.

According to the emergency procedure, a steam generator is considered "dry" when its pressure falls below 960 psig and is decreasing, or when its level is below 8 inches on the startup range (normal post-trip pressure is 1010 psig and post-trip level is 35 inches). The instrumentation in the control room is inadequate for the operator to determine with certainty if these conditions exist in a steam generator. The lack of a trend recorder for steam generator pressure makes it difficult to determine if the steam pressure is 960 psig and decreasing. The range of the steam generator level indicator in the control room is 0-250 inches, a scale which makes determining the 8-inch level difficult. The safety parameter display system (SPDS) was intended to provide the operators with these critical data, but both channels of the SPDS were inoperable prior to and during this event. Thus, the operators did not know that the conditions in the steam generators beginning at about 1:47 a.m. were indicative of a "dry" steam generator, or subsequently, that both steam generators were essentially dry.

When both steam generators are dry, the procedure requires the initiation of make-up/high pressure injection (MU/HPI) cooling, or what is called the "feed-and-bleed" method for decay heat removal. Even before conditions in the steam generators met these criteria, the shift supervisor was fully aware that MU/HPI cooling might be necessary. When the hot-leg temperature reached 591°F (normal post-trip temperature is about 550°F), the secondary-side operator recommended to the shift supervisor that MU/HPI cooling be initiated. At about the same time, the operations superintendent told the shift supervisor in a telephone discussion that if an auxiliary feedwater pump was not providing cooling to one steam generator *within one minute, to prepare for MU/HPI cooling. However, the shift supervisor did not initiate MU/HPI cooling. He waited for the equipment operators to recover the auxiliary feedwater system.*

The shift supervisor appreciated the economic consequences of initiating MU/HPI cooling. One operator described it as a drastic action. During MU/HPI, the PORV and the high point vents on the reactor coolant system are locked open, which breaches one of the plant's radiological barriers. Consequently, radioactive reactor coolant is released inside the containment building. The plant would have to be shut down for days for cleanup even if MU/HPI cooling was successful. In addition, achieving cold shutdown could be delayed. Despite his delay, the shift supervisor acknowledged having confidence in this mode of core cooling based on his simulator training; he would have initiated MU/HPI cooling if "it comes to that."

The primary-side operator returned to his station and began monitoring the pressure in the pressurizer, which was near the PORV set point of 2425 psig. The PORV then opened and he watched the pressure decrease. The indicator in front of him signaled that there was a closed signal to the PORV and that it should be closed. The acoustic monitor installed after the TMI accident was available to him to verify that the PORV was closed, but he did not look at it. Instead, he looked at the indicated pressurizer level, which appeared steady, and based on simulator training, he concluded that the PORV was closed. In fact, the PORV had not completely closed and, as a result, the pressure decreased at a rapid rate for about 30 seconds.

The operator did not know that the PORV had failed. He believed the RCS depressurization was due either to the fully open pressurizer spray valve or to the feedwater flow to the steam generators. He closed the spray valve and the PORV block valve as precautionary measures. But subsequent analyses showed that the failed PORV was responsible for the rapid RCS depressurization. Two minutes later, the reactor operator opened the PORV block valve to ensure that the PORV was available. Fortunately, the PORV had closed by itself during the time the block valve was closed. The failed PORV was the ninth abnormality that had occurred within 15 minutes after reactor trip.

2A.8 Steam Generator Refill

At about 1:50 a.m. the No. 1 atmospheric vent valve opened and depressurized the No. 1 steam generator to about 750 psig when the SFRCS signal was reset by the primary-side operator. The vent valve for the No. 2 steam generator had been closed by the secondary-side operator before the SFRCS signal was reset. The indicated No. 1 steam generator level was less than 8 inches. The corresponding pressure and indicated level in No. 2 steam generator were about 928 psig and 10 inches, respectively. The indicated levels continued to decrease until the secondary-side operator started the SUFP after being informed by the assistant shift supervisor that it was available and after the other operator had reset the isolation signal to startup feedwater valves.

Although the flow capacity of the SUFP is somewhat greater, approximately 150 gallons per minute were fed to the steam generators because the startup valves were not fully opened. Essentially all the feedwater from the SUFP was directed to the No. 1 steam generator. At about 1:52 a.m., the pressure in the No. 1 steam generator increased sharply while the indicated water level stopped decreasing and began slowly to increase. Since there was little feedwater sent to the No. 2 steam generator, its condition did not change significantly.

The trip throttle valve for No. 2 AFW pump was opened by the equipment operators at about 1:53 a.m. After the SFRCS was reset and tripped on low level by the shift supervisor, the AFWS aligned itself so that each AFW pump would feed only its associated steam generator, i.e., the No. 2 AFW pump would feed the No. 2 steam generator. Thus, the No. 2 AFW pump refilled the No. 2 steam generator and its pressure increased abruptly to the atmospheric vent valve relief set point. The turbine governor valve was fully open when the trip throttle valve was opened and the pump delivered full flow for about 30 seconds until the operator throttled the flow down.

The No. 1 trip throttle valve was opened by the equipment operator about 1:55 a.m. and feedwater from the AFWS flowed to the No. 1 steam generator. However, the No. 1 AFW pump was not controlled from the control room but controlled locally by the equipment operators.

The equipment operators controlled the pump locally using the trip throttle valve. One operator manipulated the valve based on hand signals from the operator who was outside the No. 1 AFW pump room communicating with the control room operator. For two hours the AFW pump was controlled in this manner by the operators. Their task was made more difficult from the time they first entered the AFW pump room by the intermittent failures of the plant communication station in the room.

With feedwater flow to the steam generators, the heatup of the reactor coolant system ended. At about 1:53 a.m. the average reactor coolant temperature peaked at about 592°F and then decreased sharply to 540°F in approximately 6 minutes (normal post-trip average temperature is 550°F). Thus, the reactor coolant system experienced an overcooling transient caused by an excessive AFW flow from the condensate storage tank. The overfill of the steam generators caused the reactor coolant system pressure to decrease towards the safety features actuation system (SFAS) setpoint of 1650 psig. To compensate for the pressure decrease, and to avoid an automatic SFAS actuation, at approximately 1:58 a.m., the primary-side operator aligned one train of the emergency core cooling system (ECCS) in the piggyback configuration. In this configuration the discharge of the low pressure injection pump is aligned to the suction of the high pressure injection pump to increase its shutoff head pressure to about 1830 psig. At about the time the train was actuated, the combination of pressurizer heaters, makeup flow, and reduction of the AFW flow increased the reactor coolant pressure above 1830 psig. As a result, only a limited amount (an estimated 50 gallons) of borated water *was injected into the primary system from the ECCS.*

At 1:59 a.m., the No. 1 AFW pump suction transferred spuriously from the condensate storage tank to the service water system (malfunction number 10). This action was not significant, but it had occurred before and had not been corrected. Similarly, a source range nuclear instrument became inoperable after the reactor trip (malfunction number 11) and the operators initiated emergency boration pursuant to procedures. (Note: One channel had been inoperable prior to the event.) The source range instrumentation had malfunctioned previously and apparently had not been properly repaired. Also, the control room ventilation system tripped into its emergency recirculation mode (malfunction number 12), which had also occurred prior to this event.

The steam generator water levels soon exceeded the normal post-trip level and the operator terminated AFW flow to the steam generators. The subcooling margin remained adequate throughout this event. The event ended at about 2 o'clock in the morning, twelve malfunctions and approximately 30 minutes after it began.

2A.9 NRC Findings and Conclusions

The NRC review team concluded that the underlying cause of the Davis-Besse loss-of-feedwater incident was the licensee's lack of attention to detail in the care of plant equipment. The licensee had a history of performing troubleshooting, maintenance and testing of equipment, and of evaluating operating experience related to equipment in a superficial manner and, as a result, the root causes of problems were not always found and corrected. Engineering design and analysis effort to address equipment problems had frequently either not been utilized or had not been effective. Furthermore, operator interviews made clear that equipment problems were not aggressively addressed and resolved beyond compliance with NRC regulatory requirements.

In addition to this major conclusion on the underlying cause of the event, the NRC Review Team findings and conclusions included:

- *The key safety significance of the event is that multiple equipment failures occurred resulting in a transient beyond the design basis of the plant. These failures included several common-mode failures affecting redundant safety-related equipment.*

- *The operators' understanding of procedures, plant system designs, and specific equipment operation, and operator training all played a crucial role in their success in mitigating the consequences of the event.*

- *If the manual initiation features of the SFRCS had originally been properly designed with regard to human factors considerations, such as labeling and placement, it is likely that no operator error in auxiliary feedwater initiation would have occurred.*

- *The post-TMI improvements: Temperature-saturation meters, additional training on transient behavior, and ATOG emergency procedures had a positive contribution to the mitigation of* *the event. Of these, training on transient behavior was the most important.*

- *For plant events involving conditions outside the plant design basis, operator training and operator understanding of system and equipment are key to the success of mitigating actions taken by the operators. It is not practical to rely on detailed step-by-step procedures for such events.*

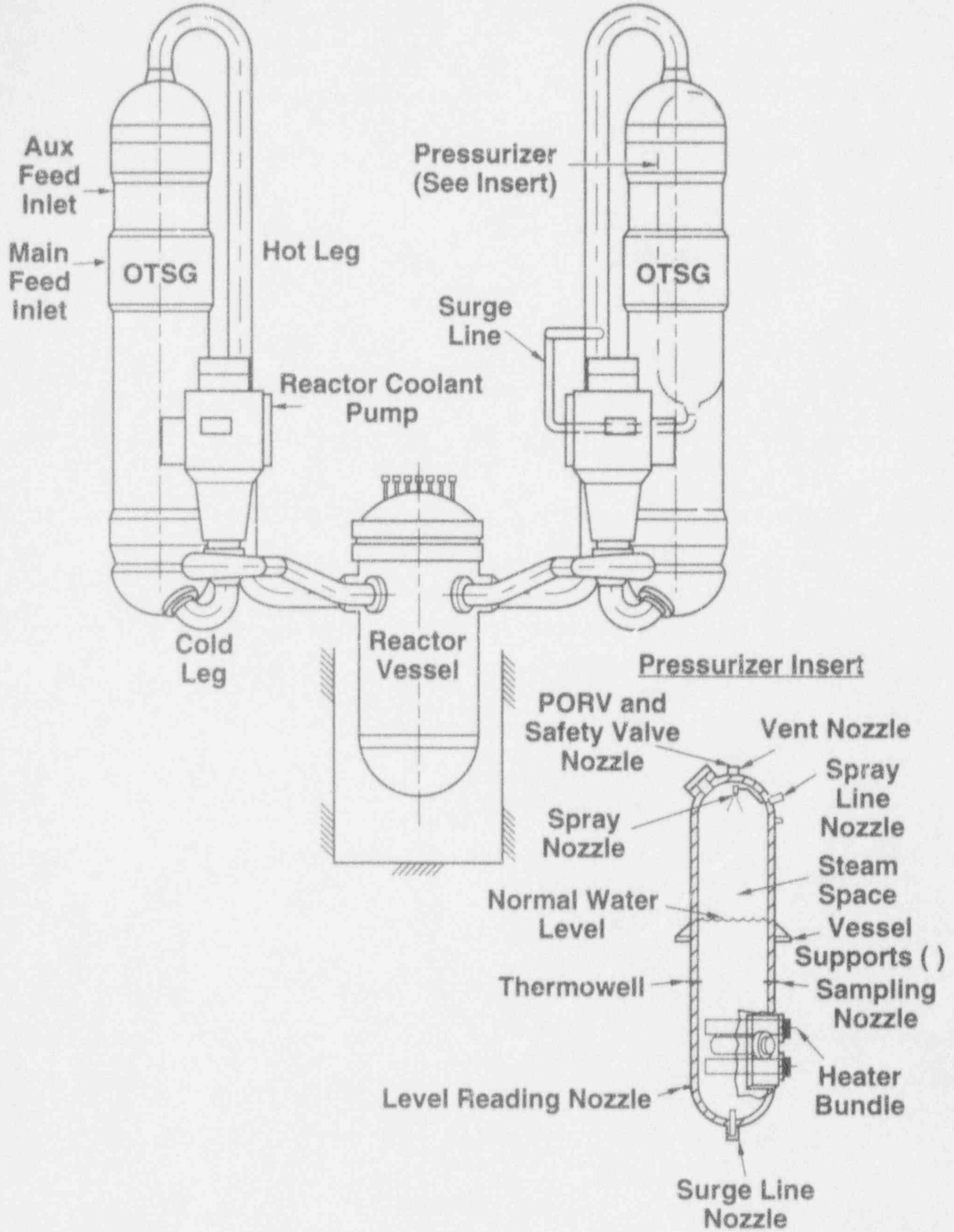


Figure 2A-1 Davis-Besse nuclear steam supply system

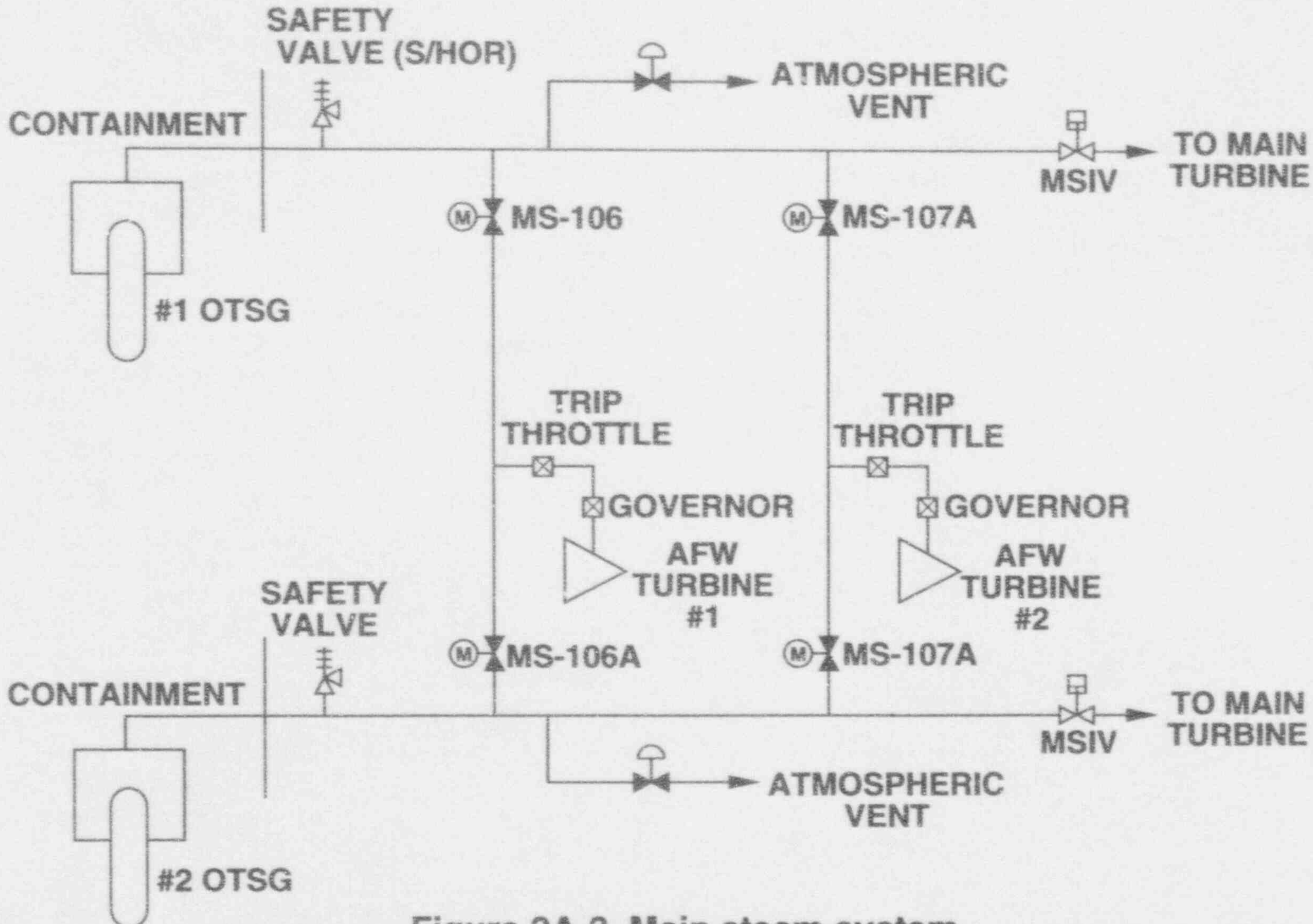


Figure 2A-2 Main steam system

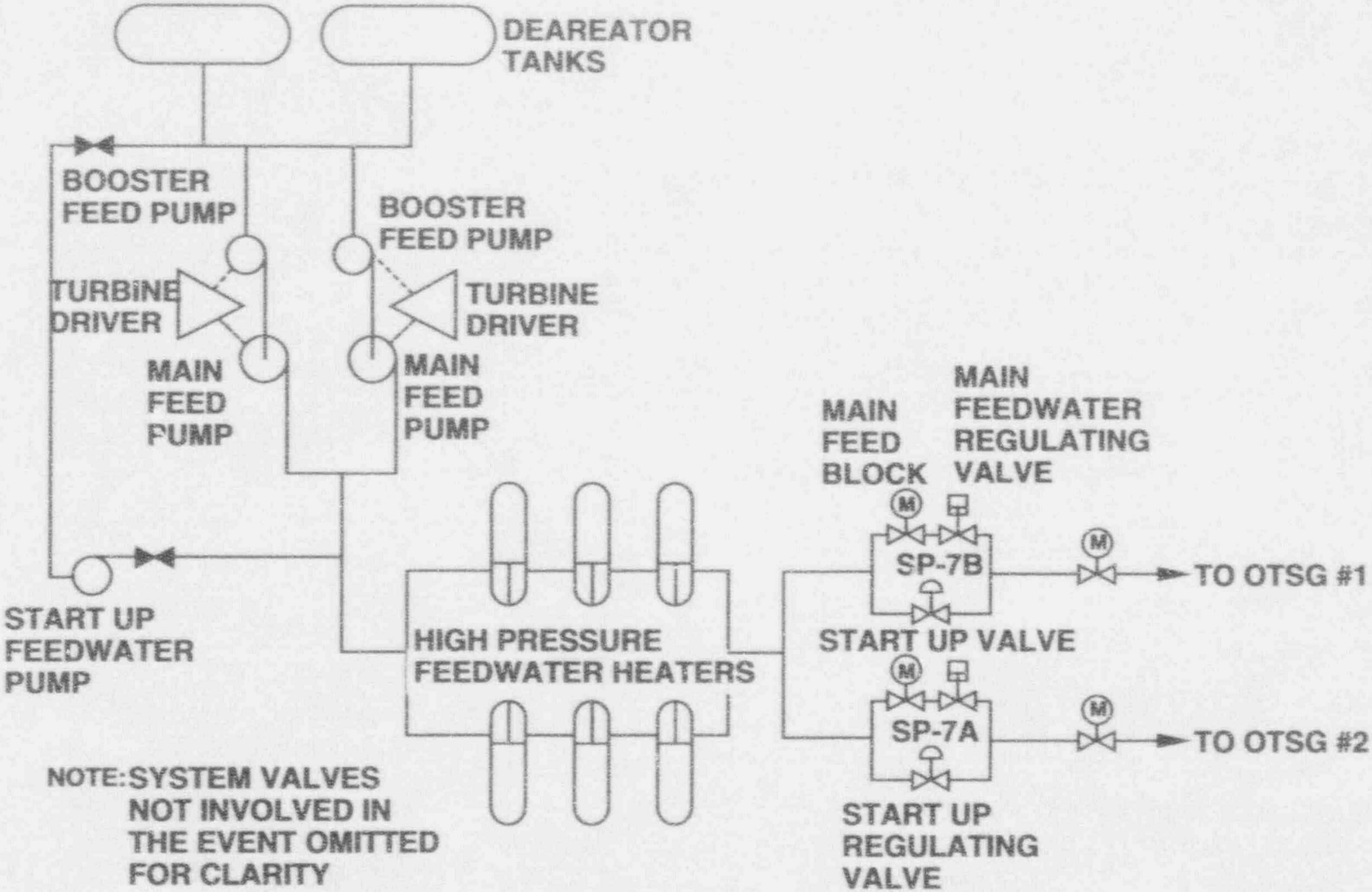


Figure 2A-3 Main feedwater system

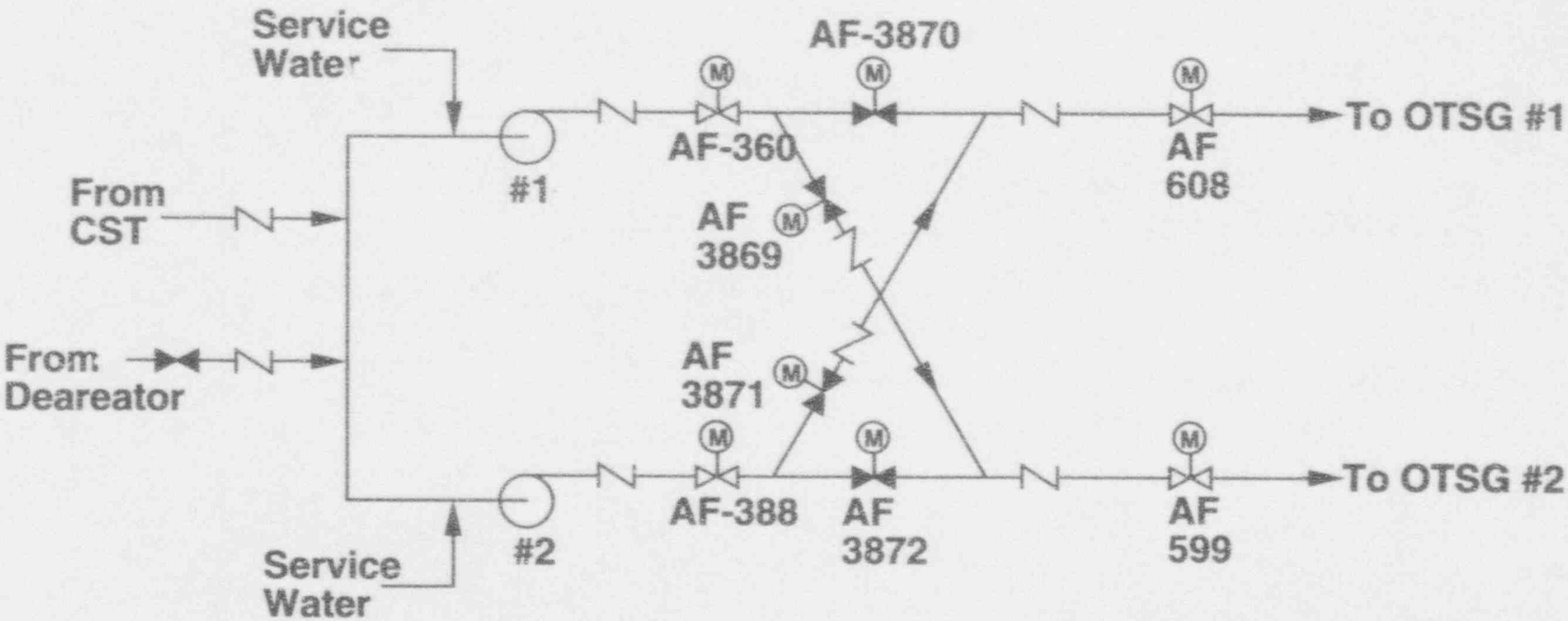


Figure 2A-4 Schematic of auxiliary feedwater system

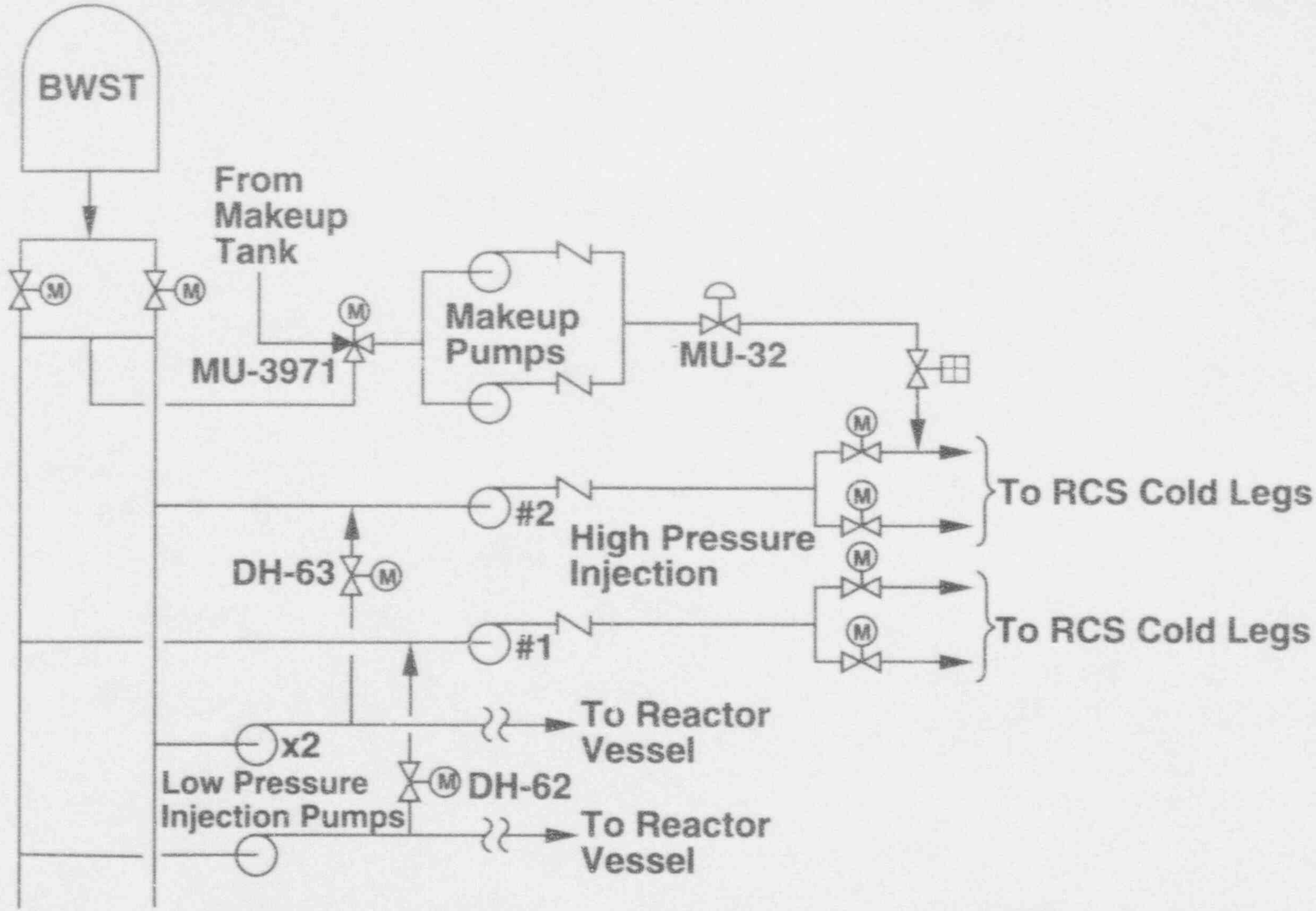


Figure 2A-5 Makeup/HPI cooling system

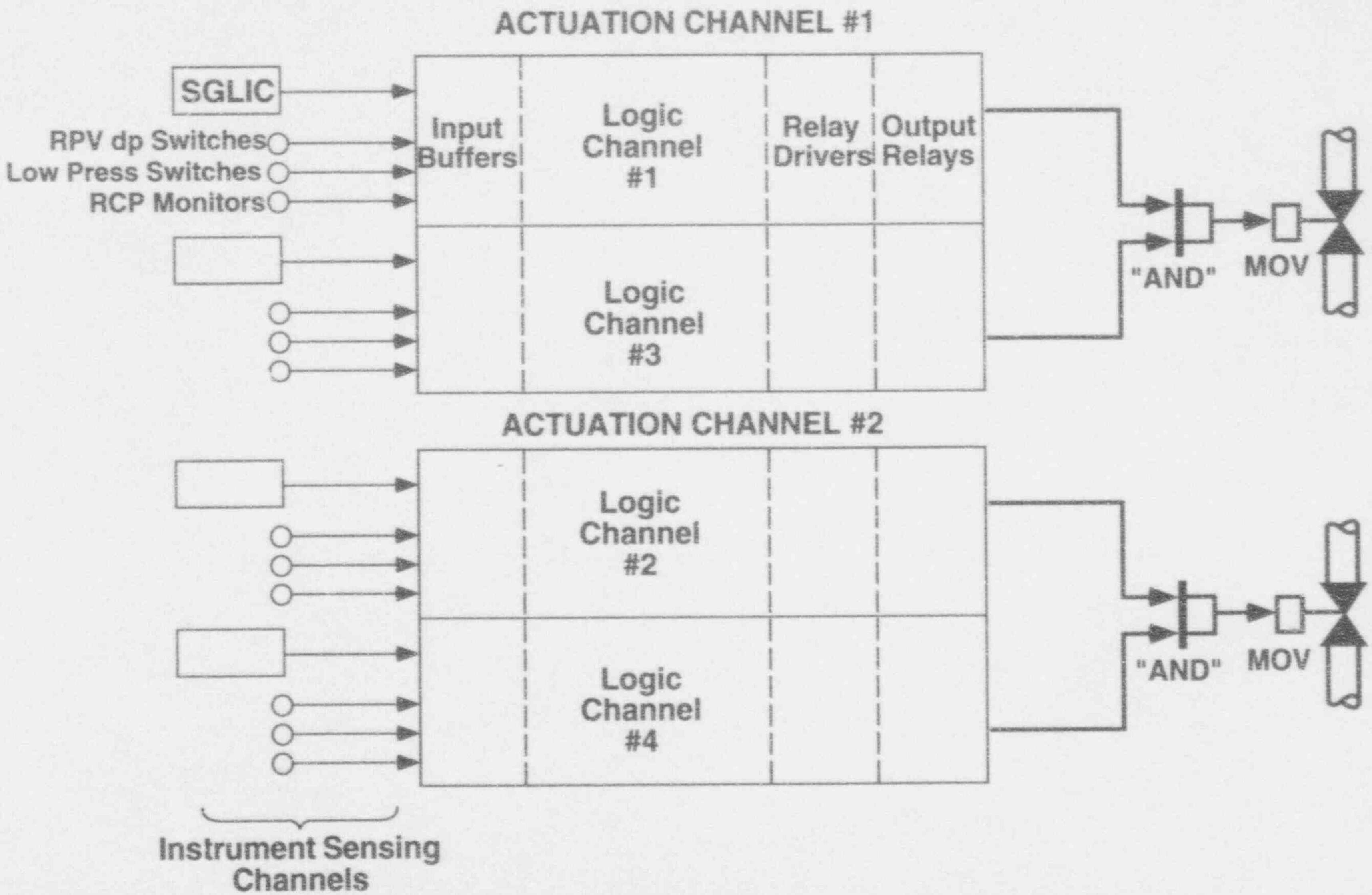


Figure 2A-6 Steam feedwater rupture control system (SFRCS) block diagram

APPENDIX 2B INFORMATION ON ATWS

In September 1973 the regulatory staff issued a report, WASH-1270, called "Technical Report on Anticipated Transients without Scram for Water-Cooled Power Reactors,"[1] in which they publicly adopted a position on ATWS. Significant WASH-1270 insights regarding reactor protection systems and plant responses to ATWS events are presented in the next two subsections. Subsections 2B.3 and 2B.4 discuss the Browns Ferry partial failure to scram, and the Salem 1 ATWS event respectively. The final ATWS rule is reproduced as Subsection 2B.5, and Subsection 2B.6. These sections discuss the changes considered in formulating the final rule.

2B.1 Protection Systems Designs and Failure Analyses

The reactor protection system (RPS) is a safety-related system that is designed to monitor key operating plant variables; and to cause alarms, control rod insertions, or scram, as the occasion may require when off-normal conditions occur. The reactor trip system (RTS) is part of the RPS and includes those power sources, sensors, initiation circuits, logic matrices, bypasses, interlocks, racks, panels, control boards, actuation devices, and actuated devices, that are required to initiate reactor shutdown. The RTS automatically initiates control rod insertion when required to assure that acceptable fuel design limits are not exceeded. It is designed to fail safe for most internal component failures. The RTS can also be actuated manually by operator action.

The essential RTS design bases are that no single failure can negate a reactor scram when one is needed, and all instrument channels and associated trip logic must be capable of being calibrated, tested, and maintained while the plant operates. These features are implemented in protection system designs by providing for each variable that is to be measured several redundant instrument channels. In most cases, four such redundant channels are provided for each monitored variable. The output responses of the redundant channels are collected and an appropriate alarm, control rod insertion, or scram is initiated when two of the redundant channels agree that action is needed.

Just as the system designer is concerned that no failure in a subsystem should render the protective feature of a group of redundant channels inoperative, he also is concerned that the occurrence of spurious scrams be minimized. This is the reason that two concurrent trip signals are required in the normal protection system arrangement.

The kinds of single failures for which protection systems are designed to be resistant include a wide range of possible occurrences. Component malfunctions and failures are some of the kinds of single failures considered. Both a simple failure to function and an improper function, from whatever cause, are considered on the component, channel, and subsystem levels. Accidental electrical grounds at any point in the system are considered as single failure events, as are short circuits from whatever higher voltage circuits may exist in the vicinity of a given section of the protection system. An additional feature of the single failure design basis is that any damage or other consequence that follows from a hypothesized failure is included in determining the effects of that single failure. Thus, if a hypothesized hot short at some point in a protection system circuit might cause failure of several components, or spurious signals to other channels, then all of these effects are taken into account in determining the vulnerability of the overall system to the single initiating event.

Full scram tests in which the rods are actually driven into the core are carried out during shutdowns for refueling and maintenance, or on other occasions when the plant may have been shut down. During operating periods, control rods are moved periodically to adjust reactivity and power distribution in the core. This operation of the rods gives some assurance of operability, although it does not completely guarantee that the rods will scram if called upon to do so. All plants are designed to be shut down safely with the most effective control rod malfunctioning such that it does not enter the core. This "stuck rod" criterion gives assurance of the ability of the system to surmount a limited degree of operational failure.

The results of the designer's failure analyses of protection systems for random independent failures show that the systems are generally resistant to such failures. The probability of scram failure can be demonstrated to be quite low (less than 10^{-7} per demand) if only these random failure events are considered. This is due to the highly redundant nature of the protection systems and the testability provided in their designs.

As discussed in Section 2.2.4.4, common cause failures could be a result of: environmental conditions; design, manufacturing, operating or maintenance errors; or functional deficiencies such as an unrecognized deficiency in sensing instrumentation or a misunderstanding of the behavior of process variables in the design of a system. For common cause failures, the analysis of protection systems is more difficult. Techniques to analyze a system for common cause failures are not as well-developed as techniques to analyze a system for random failures. However, the fault tree models used for random failure analysis are helpful in making qualitative judgments as to the effects of common cause failures.

Defenses against common cause failures all involve "diversity" of one kind or another. One form, called equipment diversity, involves use of instruments operating on different principles to measure the same reactor variable. Use of different kinds of components in the amplifying and scram logic systems leading from the sensing instruments is also a form of equipment diversity, as in the use of different kinds of trip breakers and control rod drive mechanisms. A second form is called functional diversity, which involves instrument systems responding to different variables to provide trip action for the same transient or accident. The value of diversity of one sort or another in defending against common cause failures is that with systems of different principle and with different kinds of components, the likelihood of a common failure affecting all the elements that are significant for a given transient or accident is much diminished.

In making analyses of the effects of common cause failures on reactor protection systems, each transient is examined on the assumption that all the instrument channels pertaining to a given reactor variable (e.g., neutron flux) fail in such a way as to not give any protective action signal. All other portions of the protection system are assumed to be operative. In general, the results of these analyses show that protection systems have a reasonable degree of functional diversity in the sensor portions of the systems. If a required protective action signal is not generated by the several redundant channels for a given variable, then, in most cases, another variable is driven off-normal and the necessary signal is generated from that source. The functional diversity of protection system designs, however, often applies mainly to the sensing elements. The transmitters, amplifiers, and circuitry leading into the scram logic matrices for various reactor variables that are monitored, as well as the logic matrix relays and switches or solid-state devices, the scram breakers or pilot valves, control rod drive mechanisms, and control rods often have much less diversity.

2B.2 Plant Response to ATWS Events

For pressurized water reactor plants the transients with the greatest potential for damage in the event of a failure to scram are the loss of feedwater and certain loss of load transients occurring with the reactor at full power. Loss of feedwater flow could occur as the result of malfunctions of the interlock and supervisory circuitry controlling the feedwater or condensate pumps or valves. The sequence of events for a typical pressurized water reactor plant given a loss of feedwater transient without reactor scram may be summarized as follows:

a. An accidental trip of the feedwater or condensate pumps or valves would cause a rapid reduction of feedwater flow. Low feedwater flow compared to steam flow, in coincidence with low steam generator water level, would initiate a reactor scram signal.

b. This scram signal is ignored in the ATWS analysis, as are three or more subsequent reactor scram signals generated as the transient proceeds. The loss of feedwater flow to the steam generator secondary side would result in a drop in water level in the steam generator.

c. A falling water level in the steam generator results in reduced heat transfer from the primary system. The primary coolant temperature would begin to increase since reactor power would remain high, and this, in turn, would cause the primary pressure to increase.

d. The auxiliary feedwater pumps would be started automatically after the main feedwater pumps or condensate pumps were tripped. However, the auxiliary feedwater pump capacity is not large enough to remove ali the heat being generated in the core;

e. consequently, the steam generator would boil dry.

f. The primary system temperature and pressure would continue to increase and the primary safety valves in the surge volume of the pressurizer vessel would open and discharge steam.

g. The increasing temperature of the primary coolant would cause expansion of the coolant and the water level would rise in the pressurizer.

h. When the pressurizer vessel became filled completely with water, the safety valves would discharge water instead of steam, but at a rate less than required to keep the primary system pressure from rising sharply.

i. The reactor power would decrease throughout the transient because of the negative reactivity feedback arising from increased water temperature and reduced density. This effect, combined with heat removal by the auxiliary feedwater system and with the discharge of water through the pressurizer safety valves, would reduce the pressure.

j. The pressurizer safety valves would then close and steam would reappear in the pressurizer dome. If the primary system survived the pressure peak, which was estimated in early analyses to reach values between 3000 and 7000 psi, heat generation in the core would be reduced and the heat removal capacity of the auxiliary feedwater system on the secondary side of the plant would cool the core and prevent further pressure increase.

k. Lower pressure in the primary system would allow boron solution injection into the primary system initiated by a safety injection signal generated by low pressure in the secondary steam line or by manual actuation.

l. When the boron solution reached the core, enough negative reactivity would be provided to shut the plant down.

A loss of electrical load transient could occur from a generator trip, a turbine trip, or a loss of main condenser vacuum. Generally, the most severe transient would be caused by the loss of condenser vacuum. The main feedwater pumps in many plants are steam turbine-driven and exhaust to the main condenser. Thus, loss of condenser vacuum also could cause a loss of the main feedwater pumps. In this case the sequence of events would be similar to the loss of feedwater transient. The most severe effect of the transient, the peak pressure in the primary system, would be of about the same magnitude as in the loss of feedwater flow transient.

For boiling water reactor plants, the transients having the greatest potential for significant damage are those leading to a reactor coolant system pressure increase. The most severe of these are the loss of condenser vacuum and the closure of all main steam isolation valves. A loss of condenser vacuum causes automatic closure of the turbine stop valves and the turbine bypass valves. The turbine stop valves are fast-acting valves, so there is an abrupt interruption of steam flow from the reactor. The main steam isolation valves are slower in closing, but in this case the large steam line volume is not available to buffer the pressure rise. The result in either case would be an increase in reactor coolant pressure and temperature. The pressure increase would decrease the volume of steam bubbles in the reactor core and this, in turn, would increase the reactivity and cause an increase in reactor power. The power increase would cause a further increase in system temperature and pressure. The other transients that lead to primary system pressure increase are less severe.

Generator or turbine trips are less severe because the turbine bypass valves can be assumed to open and the condenser to be operative. Although the transient proceeds more slowly in these cases, the result still would be a high reactor coolant system pressure.

2B.3 Failure of Control Rods to Fully Insert at Browns Ferry 3

On June 28, 1980, Browns Ferry Unit 3, a BWR, reported that 76 of 185 control rods failed to insert fully into the core when a manual scram was initiated by the reactor operator. Fortunately, this occurred during a routine shutdown from about 35% power, rather than during the kind of reactor transient in which complete and rapid scram of all the rods might have been important.

The partially inserted rods were all (with one exception) on the east side of the core where reactor power level was indicated to be 2% or less. The west side of the core was subcritical. A second manual scram was initiated 6 minutes later and all partially inserted rods were observed to drive inward, but 59 remained partially withdrawn. A third manual scram was initiated 2 minutes later, and 47 rods remained partially withdrawn. Six minutes later, an automatic scram occurred and all the rods inserted fully when the scram discharge level bypass switch was returned from "bypass" to "normal" and there was a high water level in the scram discharge instrument volume. It appears that this was a coincidence in that a manual scram would probably have produced the same result. Core coolant flow, temperature, and pressure remained normal for the existing plant conditions.

The problem was determined to be hydraulic in nature rather than electrical or mechanical. The control rod drives (CRDs), which insert and withdraw the attached control rods in a General Electric BWR, are essentially water-driven hydraulic pistons. On a scram, a relatively high water pressure is applied to the bottom side of the piston by opening a scram inlet valve. A scram outlet valve opens to relieve water and pressure above the piston and the rods are rapidly driven up into the reactor core. Water discharged from the 185 individual CRDs during scram insertion is collected in two separate headers consisting of a series of interconnected 6-inch-diameter pipes (four on each side of the reactor) called the scram discharge volume (SDV). During normal operation, both SDVs are designed to remain empty by being continuously drained to a separate scram discharge instrument volume (SDIV) tank. The SDVs are therefore normally ready to receive the scram discharge water when a scram occurs. This instrumented tank is monitored for water level and initiates an automatic scram on high level, in anticipation of too much water in the SDV preventing a scram.

The control rod drives at Browns Ferry Unit 3 are grouped in such a manner that the east and west sides of the reactor core are connected to separate SDVs. Later tests, inspections, and analyses resulted in the conclusion that the east SDV was substantially full of water at the time of the event, leaving insufficient room for the discharge water. Accordingly, upon scram actuation, the CRDs rapidly drove the control rods partially into the core but rod motion prematurely ceased when pressure quickly equalized on each side of the pistons. Following each scram actuation, the scram signal was reset by the operator, allowing some water to drain from the SDV, permitting the rods to insert further with each scram attempt. Sufficient water was finally drained from the SDV to allow the rods to insert fully on the fourth scram signal. It is believed that the east SDV water accumulation problem resulted from improper drainage into the SDIV from the SDV due to inadequate SDV venting, an obstruction in the line between the SDV and SDIV, or a combination of these problems.

The unit remained shut down while a series of tests was performed in an attempt to determine the cause of the water accumulation in the SDV. Ultrasonic probes were installed on the SDVs to continuously monitor the water level in the SDVs. A Preliminary Notification was issued to inform other NRC offices promptly. On July 3, 1980, IE Bulletin No. 80-17 was issued to all licensees operating BWRs and required them to conduct prompt and periodic inspections of the SDV; perform two reactor scrams within 20 days while monitoring pertinent variables to further confirm operability; review emergency procedures to assure pertinent requirements are included; and conduct additional training to acquaint operating personnel with this type of problem.

On July 18, 1980, Supplement 1 to Bulletin 80-17 was issued to all licensees operating BWRs. This supplement required an analysis of the "as built" SDV; revised procedures on initiation of the standby liquid control system (SLCS); specifying in operating procedures action to be taken if water is found in the SDV; daily monitoring of the SDV until a continuous monitor can be installed; and studying of designs to improve the venting of the SDV. During testing required by IE Bulletin 80-17, additional SDV anomalies were found at seven other BWRs. As a result, Supplement 2 to IE Bulletin 80-17 was issued on July 22, 1980. This required the BWR licensees to provide a vent path from the SDV directly to the building atmosphere without any intervening component except for the vent valve itself. These modifications had to be completed within 48 hours for plants operating or prior to startup for plants shut down.

Browns Ferry Unit 3 was authorized to restart on July 13, 1980, following completion of the actions required by IE Bulletin 80-17 and other extensive tests.

Continuing NRC review of this event identified a potential for unacceptable interaction between the control rod drive system and the nonessential control air system; therefore, IE Bulletin 80-17 Supplement 3 was issued on August 22, 1980. This Supplement required affected BWR licensees to implement operating procedures within five days, which required an immediate manual scram on low control air pressure, or in the event of multiple rod drift-in alarms, or in the event of a marked change in the number of control rods with high temperature alarms. In addition, the licensees were requested to implement procedures, which require a functional test using water for the instrument volume level alarm, rod block, and scram switches after each scram event.

On October 2, 1980, the NRC issued Confirmatory Orders to the licensees of 16 BWR plants requiring the installation of equipment to continuously monitor water levels in all SDVs and provisions for water level indication and alarm for each SDV in the control room. This equipment permits the reactor operators to take timely action if water accumulates in the SDV. The equipment was required to be operable by December 1980 or prior to restart for those reactors in refueling. In the interim, the licensees were required to increase their surveillance of the SDV water level.

The NRC prepared two detailed reports ("Report on the Browns Ferry 3 Partial Failure to Scram Event on June 28, 1980," dated July 30, 1980, and "Report on the Interim Equipment and Procedures at Browns Ferry to Detect Water in the Scram Discharge Volume," dated September 1980. The various aspects of the BWR scram systems were studied further by the NRC, the BWR licensees, and General Electric.

2B.4 ATWS Event at Salem 1

Salem 1, like other Westinghouse PWRs, uses two redundant reactor trip breakers (RTBs) in series in the RTS. For Salem 1, each RTB includes an under-voltage (UV) trip attachment and a shunt trip attachment to actuate (open) the trip breaker. The UV device initiates a breaker trip when de-energized, while the shunt device initiates a breaker trip when energized. For an automatic trip, only the UV device is actuated; initiation of the UV devices in either or both RTBs will actuate the control rods. A manual trip signal operates both the UV device and the separate shunt device. Either device is designed to cause the RTBs to open. Salem Unit 1 uses Westinghouse DB-50 type RTBs.

At 12:21 a.m. on February 25, 1983, a low-low water level condition in one of the four steam generators at Salem 1 initiated a reactor trip signal in the RPS. At the time, the reactor was at 12% rated thermal power in preparation for power escalation after a recently completed refueling outage. Upon receipt of the valid reactor trip signal, both of the redundant RTBs failed to open (opening of either RTB would have caused the reactor to trip). About 25 seconds later, operators manually initiated a reactor trip from the control room. The RTBs opened as a result of the manual trip signal and this resulted in insertion of all control rods and shutdown of the reactor. Following the manual trip, the plant was stabilized in the hot standby condition. All other systems functioned as designed. Approximately two hours after the Salem 1 event, the cause of the failure to trip was determined by licensee instrumentation technicians to be failure of the UV trip device in both RTBs to function as designed. The plant was placed in cold shutdown at the request of the NRC.

During investigation of this incident on February 26, 1983, by the NRC, it was found that a similar failure had occurred on February 22, 1983, at Salem 1. At 9:55 p.m. on February 22, with the reactor at 20% power, operators were attempting to transfer the 4160 volt group electrical busses from the station power transformers to the auxiliary power transformers, a routine evolution during power escalation. During the transfer attempt, one of the 4160 busses failed to transfer and deenergized, resulting in the loss of one reactor coolant pump and power for the operating main feed pump control and indication. At 9:56 p.m., a low-low level condition occurred in one steam generator (due to the loss of the main feed pump), initiating a reactor trip signal. Due to the abnormal conditions created by the loss of the 4160 volt bus and in anticipation of loss of steam generator water levels, the operator was directed at about the same time to manually initiate a reactor trip. It was understood by plant personnel and was reported to the NRC that the automatic reactor trip signal due to the low-low level in one steam generator had, in fact, caused the reactor to trip. On February 26, 1983, as a result of NRC queries, the sequence of events computer printout for February 22 was reviewed in detail and it revealed that the RTBs actually opened in response to the operator's manual trip signal. Consequently, it became evident that on February 22 (as on February 25) the two RTBs failed to open upon receipt of an automatic trip signal from the RPS. The operators initiated a manual trip even though they were unaware that the automatic trip had failed.

Since the operators initiated a manual reactor trip shortly after receipt of the automatic trip signals on both February 22 and February 25, no adverse consequences occurred and the reactor was in a safe condition. However, as the first actual ATWS events, the Salem 1 events were of major safety concern.

With few exceptions, all PWR plants designed by the three nuclear steam system suppliers (Westinghouse, Babcock & Wilcox, and Combustion Engineering) use an RTS design requiring circuit breakers to open to trip the reactor. Although the basic designs of the RTSs and the number of RTBs per plant differ considerably among the plant designers, each RTB generally includes a UV trip attachment and a shunt trip attachment to actuate the circuit breaker. Westinghouse designed plants use a Westinghouse breaker (DB type for older plants, DS type for newer plants) while the other two PWR designers use General Electric breakers (AK type).

Other pressurized water reactors (PWRs) have experienced RTB failures, both before and after the February 1983 Salem 1 events. None of them however, involved an ATWS event. The RTB failures prior to the February 1983 events at Salem 1 had been the subject of several actions taken since 1971 by the AEC/NRC, Westinghouse, and General Electric.

Due to the serious nature of Salem 1 failure of both redundant RTBs on February 25, 1983, the NRC issued Inspection and Enforcement Bulletin No. 83-01[2] on the same day to all pressurized water nuclear power reactor facilities holding an operating license for action and to other nuclear power reactor facilities for information. The Bulletin informed the licensees of the Salem 1 February 25, 1983, event (the similarity of the February 22, 1983, event had not yet been ascertained) and mentioned that failures involving only one of the two breakers had previously occurred at Salem Unit 2, Robinson Unit 2, Connecticut Yankee, and St. Lucie. The Bulletin referenced two previously issued NRC notifications of RTB problems and Westinghouse-issued technical information on their breakers. Action items required of licensees using Westinghouse DB type breakers by Bulletin No. 83-01 included, a) testing of the DB type breakers, (b) assuring maintenance is in accord with the recommended Westinghouse program, (c) notifying licensed operators of the Salem 1 events, (d) reviewing with the operators the procedures to follow in the event of failure of trip, and (e) reporting the results to the NRC.

On February 28, 1983, the NRC Executive Director for Operations (EDO) directed that NRC Region I was to develop a detailed report of the Salem 1 events. This report was subsequently issued as NUREG-0977.[3] The EDO further directed that a special NRC task force be formed to evaluate the generic implications of the events.

Possible contributors to failures of UV trip devices include: (1) dust and dirt; (2) lack of lubrication; (3) wear;(4) more frequent operation than intended by design; and (5) nicking of latch surfaces caused from repeated operation of the breakers. Based on an independent evaluation of the failed UV trip devices identified by the licensee, the NRC staff concluded that, while the Salem 1 breaker failures occurred as a result of several possible contributors, the predominant cause was excessive wear accelerated by lack of lubrication and improper maintenance.

During the testing required by Bulletin No. 83-01, no further failures of Westinghouse DB type RTBs occurred. However, even though not required to do so by Bulletin No. 83-01, Southern California Edison decided to test the General Electric type AK-2 breakers on their Combustion Engineering designed San Onofre Units 2 and 3. On March 1, 1983, one of eight RTBs in Unit 3 failed to trip on undervoltage. On March 8, 1983, three of eight RTBs in Unit 2 failed to trip on undervoltage. (Note: Contrary to the Salem design in which an automatic trip signal is fed only to the UV trip devices, the signal is fed to both the UV and shunt trip devices for the San Onofre Units 2 and 3 design. The shunt devices were satisfactorily tested; therefore, the RTBs would have tripped from an automatic trip signal during operations.) During the investigations of these events, it was found that previous failures had occurred at these units during 1982 but had not been reported to the NRC.

Accordingly, Inspection and Enforcement Bulletin No. 83-04[4] was issued on March 11, 1983, to all pressurized water nuclear power reactor facilities holding an operating license except those with Westinghouse DB type breakers for action and to other nuclear power reactor facilities for information. The Bulletin described the San Onofre events and mentioned that similar events involving the General Electric AK-2 type breakers had previously occurred at Arkansas Unit 1, Crystal River Unit 3, Oconee Units 1 and 3, Three Mile Island Unit 1, St. Lucie Unit 1, and Rancho Seco Unit 1. Licensees were to (a) take actions similar to those required by Bulletin No. 83-01, (b) provide a description of all RPS breaker malfunctions not previously reported to the NRC, and (c) verify that procurement, testing, and maintenance activities treat the RTBs and associated UV devices as safety related.

In response to Bulletin No. 83-04, additional cases of past RTB failures were reported to the NRC. In addition, other failures occurred after the testing required by Bulletin Nos. 83-01 and 83-04. In all cases, the NRC closely monitored the corrective actions taken by the licensees to assure that the plants were safe for continued operation.

In parallel with the NRC initiated actions, Westinghouse formed an intercompany task force to conduct an internal review of their procedures for dissemination of technical information to utilities. In addition, they reviewed the testing program for the breakers. Since there were generic implications associated with the Salem 1 ATWS event, Westinghouse worked with the Owners Group (licensees of Westinghouse designed plants) to review operating and emergency procedures, to look for similar failures in other plant systems, and to assure that the owners had current Westinghouse technical information. Westinghouse also identified potential deficiencies with their DS type breakers, which were being used in five operating plants, and 24 plants under construction. Westinghouse developed updated maintenance procedures for both DB and DS type RTBs. Combustion Engineering and Babcock & Wilcox made similar reviews, and in cooperation with General Electric, developed updated maintenance procedures for the licensees with AK-2 type breakers.

As noted previously, the Salem 1 licensee failed to recognize on February 22, 1983, that an ATWS event had occurred. This was due to the lack of a thorough and systematic review to achieve the necessary understanding of the event. This, and previously identified problems at Salem, indicated the need for both a number of technical term corrective actions and some significant management improvements. The NRC did not permit the Salem plants to restart until both technical and management corrective actions were satisfactory addressed. On April 26, 1983, the Commission agreed that the plants could be returned to service, after the NRC staff is satisfied with the licensee's commitment to meet certain restart conditions. On May 5, 1983, the NRC forwarded to the Salem licensee a Notice of Violation and Proposed Imposition of Civil Penalties (for $850,000).[5] Violations included operation of the reactor even though the RPS could not be considered operable, and several significant deficiencies which contributed to the inoperability of the RTBs. Region I instituted an augmented inspection program at Salem to monitor the licensee's progress towards completion of longer term corrective actions, including independent management consultants' recommendations.

The special NRC task force prepared a two-volume report, NUREG-1000.[6] The first volume dealt with the generic implications of the Salem events. The second volume documented the NRC actions to be taken based on the work of the task force. The results of the task force were considered in deliberations regarding the ATWS position and rule, which was being developed by the NRC.

2B.5 10 CFR 50.62, The ATWS Rule

50.62 Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants.

(a) *Applicability.* The requirements of this section apply to all commercial light-water-cooled nuclear power plants.

(b) *Definition.* For purposes of this section, "Anticipated Transient Without Scram" (ATWS) means an anticipated operational occurrence as defined in Appendix A of this part followed by the failure of the reactor trip portion of the protection system specified in General Design Criterion 20 of Appendix A of this part.

(c) *Requirements.* (1) Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions' indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

(2) Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods).

(3) Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.

(4) Each boiling water reactor must have a standby liquid control system (SLCS) with a minimum flow capacity and boron content equivalent in control capacity to 86 gallons per minute of 13 weight percent sodium pentaborate solution. The SLCS and its injection location must be designed to perform its function in a reliable manner. The SLCS initiation must be automatic and must be designed to perform its function in a reliable manner for plants granted

a construction permit after July 26, 1984, and for plants granted a construction permit prior to July 26, 1984, that have already been designed and built to include this feature.

(5) Each boiling water reactor must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.

(6) Information sufficient to demonstrate to the Commission the adequacy of items in paragraphs (c)(1) through (c)(5) of this section shall be submitted to the Commission as specified in *50.4.

(d) *Implementation.* By 180 days after the issuance of the QA guidance for non-safety related components, each licensee shall develop and submit to the Commission, as specified in *50.4, a proposed schedule for meeting the requirements of paragraphs (c)(1) through (c)(5) of this section. Each shall include an explanation of the schedule along with a justification if the schedule calls for final implementation later than the second refueling outage after July 26, 1984, or the date of issuance of a license authorizing operation above 5 percent of full power. A final schedule shall then be mutually agreed upon by the Commission and licensee.
[49 FR 26044, June 26, 1984; 49 FR 27736, July 6, 1984, as amended at 51 FR 40310, Nov. 6,1986]

2B.6 Changes Considered for ATWS Rule

10 CFR 50.62 (c)(1)
Diverse and Independent Auxiliary Feedwater Initiation and Turbine Trip for PWRs

This was proposed by the Utility Group on ATWS. It consists of equipment to trip the turbine and initiate auxiliary feedwater independent of the reactor trip system. It has the acronym AMSAC, which stands for Auxiliary (or ATWS) Mitigating Systems Actuation Circuitry. It showed a highly favorable value/impact for Westinghouse plants and a marginally favorable value/impact for CE and B&W plants. It should be designed to minimize the potential for causing a spurious reactor trip.

10 CFR 50.62 (c)(2) and (c)(3)
Diverse Scram System

This was proposed by the Utility Group on ATWS for CE, B&W and GE plants. The NRC staff analysis showed a favorable value/impact. However, the principal reasons for requiring the feature are to assure emphasis on accident prevention and to obtain the resultant decrease in potential common cause failure paths in the RTS. It should be designed to minimize the potential for causing a spurious trip of the reactor. A diverse scram system for Westinghouse plants was not a recommendation of the Utility Group on ATWS and was not a clear requirement of the Staff Rule or the Hendrie Rule. NRC staff analyses indicated a marginally favorable value/impact for Westinghouse plants; however, a diverse scram was ultimately not required for Westinghouse plants.

10 CFR 50.62 (c)(4)
Increased Standby Liquid Control System (SLCS) Capacity

The SLCS is a system for injecting borated water into the reactor primary coolant system. The neutron absorption by the boron causes shutdown of the reactor. Addition of this system was proposed by the Utility Group on ATWS for new plants (those receiving an operating license three years after the effective date of the final rule). Because of the vulnerability of BWR containments to ATWS sequences, the NRC determined that increased SLCS capacity was warranted. The preferred location for SLCS injection was into HPCS or HPCI lines, which provides significant improvement in mixing of borated water when compared to SLCS injection into the standpipe at the core inlet plenum. The HPCS/HPCI injection location is also preferred, since it could prevent local power increases and possible power excursions during the recovery phase of an ATWS when cold unborated ECCS water could be added above the core. Some BWR/5 and BWR/6 licensees already had this injection location.

10 CFR 50.62 (c)(4)
Automatic Initiation of Standby Liquid Control System

One of the alternatives considered by the Task Force was an automatically initiated standby liquid control system with a capacity of greater than 86 gpm (such as 150-200 gpm). This would have resulted in a considerable ATWS risk reduction (about a factor of seven) for operating plants. Unfortunately, the cost to do this (based on information supplied by the Utility Group on ATWS) would have been on the order of $24 million per plant. This cost is significantly impacted by the costs of downtime for installation in existing plants and by an allowance for potential downtime from an inadvertent trip that would inject boron into the reactor vessel. The value/impact did not favor this alternate for existing plants. New plants (those which receiving construction permits after the effective date of the ATWS rule) are required to have automatic SLCS initiation. The equipment for automatic SLCS actuation should be designed to perform its function in a reliable manner while minimizing the potential for spurious actuation.

10 CFR 50.62 (c)(5)
Automatic Recirculation Pump Trip for BWRs

Recirculation pump trip (RPT) results in a reduction of reactor power from 100 percent to about 30 percent within a minute or so of an ATWS. This requirement had already been implemented on all operational BWRs in response to a show cause order dated February 21, 1980. The BWR owners generally agreed that this was a necessary requirement. It was included in the final rule for completeness.

Adding Extra Safety Valves or Burnable Poisons

One of the alternatives considered by the NRC Task Force was adding more safety valves to plants manufactured by CE and B&W. This would reduce the peak pressure in the reactor vessel and yield a higher probability of the plant surviving an ATWS with no core damage. The peak overpressure could also be reduced by modifying the core behavior (the fraction of the time the moderator temperature coefficient is unfavorable) by adding burnable poisons. The Utility Group on ATWS estimated that installing larger valve capacity could cost up to $10 million per plant. A large fraction of this is the cost of downtime for installation of the valves. The NRC found the value/impact of this option to be unfavorable for existing plants. Thus, the ATWS rule does not cover enhanced pressure relief capacity for new CE and B&W plants. However, the NRC expects this issue to be addressed during licensing reviews of any specific new or standard plant application.

References for Appendix 2B

1. U. S. Atomic Energy Commission Regulatory Staff, "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors," WASH-1270, September 1973.

2. U.S. Nuclear Regulatory Commission, Inspection and Enforcement Bulletin No. 83-01, "Failure of Reactor Trip Breakers (Westinghouse DB-50) to Open on Automatic Trip Signal," February 25, 1983.

3. U.S. Nuclear Regulatory Commission, "NRC Fact-Finding Task Force on the ATWS Events at Salem Nuclear Generating Station, Unit 1, on February 22 and 25, 1983," USNRC Report NUREG-0977, published March 1983.

4. U.S. Nuclear Regulatory Commission, Inspection and Enforcement Bulletin No. 83-04, "Failure of the Undervoltage Trip Function of Reactor Trip Breakers," March 11, 1983.

5. Letter from Richard C. DeYoung, Director, NRC Office of Inspection and Enforcement, to Robert Smith, Chairman of the Board, Public Service and Gas Company, transmitting a Notice of Violation and Proposed Imposition of Civil Penalties, Docket Nos. 50-272 and 50-311 (May 5, 1983).

6. U.S. Nuclear Regulatory Commission, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," USNRC Report NUREG-1000, Vol. 1, (April 1983).

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ILLUSTRATIONS (Continued)

3.0 ACCIDENT PROGRESSION IN THE REACTOR VESSEL

3.0.1 Introduction

Given an accident sequence that leads to sustained uncovering of the core, the progression of core damage involves: overheating of fuel; exothermic oxidation of the cladding with accompanying production of high temperature hydrogen gas; distortion and breach of the fuel cladding; melting of the cladding; fuel liquefaction; downward relocation of core materials; interactions between molten fuel and residual water in the reactor vessel; and breach of the reactor vessel accompanied by the discharge of molten core materials to the containment.

The rates of core heating, and the temperatures attained, strongly influence the releases of radionuclides from the fuel and the potential for trapping such radionuclides on surfaces within the reactor coolant system. The very high temperature gases strongly influence the flow velocities, heat transfer, and turbulence levels. These factors, in turn, determine the potential for and timing of temperature-induced failures of structures in the reactor coolant system. They also govern the transport and retention of radionuclides within the reactor coolant system.

The hydrogen gas produced in-vessel can escape to containment, where its combustion can pressurize and heat the containment. Violent in-vessel fuel coolant interactions have the potential to fail the reactor vessel, or even containment, with the accompanying forceful ejection of radionuclides. The melting and downward relocation of core materials in the reactor vessel, if unarrested by the restoration of coolant, can breach the reactor vessel resulting in the discharge of hot core debris, radionuclides, and aerosols into containment, where they may interact with the containment atmosphere, water, and/or concrete. The characteristics of these discharges strongly affect the likelihood and timing of various containment failure modes and the magnitudes of radionuclide releases to the environment should containment fail.

Finally, to a large extent, in-vessel processes determine the likelihood of arresting core degradation and radionuclide releases from the fuel upon restoration of coolant supply.

3.0.2 Learning Objectives for Module 3

At the end of this module, the student should be able to:

1. List three energy sources that would be of concern in a severe accident.

2. Identify the three conditions that must be achieved to arrest a severe accident.

3. Characterize the time intervals in which the following events would be expected in severe accidents involving complete failure of cooling water flow to the core:

   a. In-vessel molten-core-coolant interaction
   b. Onset of Zr oxidation
   c. Core relocation
   d. Melt through of reactor pressure vessel bottom head
   e. Core uncovering

4. Indicate, for each pair of accident types below, the one that would proceed faster and explain why:

   a. Large LOCA versus small LOCA
   b. PWR transient versus comparable BWR transient
   c. Accident initiated at power versus shutdown

5. Explain what is meant by alpha-mode containment failure and indicate the currently perceived likelihood of such an event.

6. List at least one concern regarding the restoration of cooling water when molten core material is present in-vessel.

7. Describe the possible modes of bottom head failure and melt release to containment.

3.1 Severe Accident Stages

3.1.1 Delineation of Accident Stages

This module discusses the known in-vessel processes that play important roles in determining the severity and consequences of core-damage accidents. The discussion of in-vessel processes is divided into six parts, corresponding to successive stages of core damage. These stages of core damage are marked by:

1. The initiating event and subsequent failures leading to inadequate core cooling.

2. The onset of sustained core uncovering, which leads to core heatup.

3. The onset of exothermic oxidation of cladding by steam resulting in hydrogen production, cladding failure, and the release of gaseous fission products from the fuel-cladding gap.

4. The onset of clad melting and fuel liquefaction, which results in more substantial releases of radionuclides from the fuel.

5. Slumping of molten material into the lower plenum of the reactor vessel, which may contain residual reactor coolant.

6. The failure of the reactor vessel bottom head with consequent discharge of molten material into containment.

The significant phenomena occurring during each of these in-vessel stages are discussed in this module.

As indicated in Table 3.1-1, each stage of core damage begins with a particular starting event and terminates with the event that starts the next stage. Although the processes initiated in one stage can continue in subsequent stages, the event that delineates the next stage marks the onset of significant additional processes that can significantly alter the progression of the accident. The rationale for the starting events and stage durations in Table 3.1-1 is provided in the discussion of each stage. The stage durations are necessarily approximate and incorporate appropriate ranges of values both because the table applies to a range of accidents, and because of uncertainties inherent in predicting accident progression.

Figure 3.1-1 illustrates temperature and time intervals that encompass a wide spectrum of severe accident scenarios and key events and phenomena that would be anticipated to occur as core temperatures increase. The phenomena, events and timing depicted in Figure 3.1-1 are discussed in subsequent sections. However, a few points warrant consideration here. The times measured from the onset of sustained core uncovering in Figure 3.1-1 are based on scenarios in which there is no partial injection of core coolant, and in which the onset of sustained core uncovering begins within a few hours of reactor shutdown. For such accidents, in-vessel events would proceed to bottom head failure within 3 hours as indicated in Figure 3.1-1. The more accelerated accident scenarios are those involving large break LOCAs with immediate failure of emergency core cooling. BWR accident stages tend to progress somewhat more slowly than PWR accident stages due to the smaller core power density (W/cm^3). If there is partial injection of core coolant or if the core uncovering is delayed for many hours (allowing decay power to decrease) the accident stages may take longer than depicted in Figure 3.1-1.

Significantly, about 1 hour after shutdown, an injection flow of only a few hundred gallons of water per minute is sufficient to keep the core of a 3300 MWt plant covered. However, once core degradation has begun (stage 2) additional water is required to quench core materials.

Frequently, when students first see Figure 3.1-1 they are bothered by the fact that very rapid steam-zircaloy reaction is shown to begin at 1832°F (1000°C), which is under the peak cladding temperature of 2200°F (1204°C) allowed in the 10 CFR 50.46 as a result of the ECCS rulemaking. That is, the 2200°F design criterion for ECCS performance appears non-conservative. However, as indicated in Module 1, Section 1.3.6, 10 CFR 50.46 further requires that:

- Peak cladding temperature cannot exceed 2200°F.
- Oxidation cannot exceed 17% of the cladding thickness.
- Hydrogen generation from hot cladding-steam interaction cannot exceed 1% of its potential.
- The core geometry must be maintained in a coolable condition.
- Long-term cooling must be provided.

A fundamental problem in understanding core melt progression is that it is extremely difficult to perform the experiments necessary to fully understand the relevant phenomena. Over the years, computer code calculations of severe accident behavior have been extremely useful for forming and reinforcing engineering judgment. However, care must be taken in using and interpreting severe accident code calculations because such codes can never be fully validated. Even given the years of severe accident research that followed the 1979 TMI-2 accident, no computer code can calculate all major aspects of the TMI-2 accident. Modeling uncertainties tend to increase as the accident progresses, in particular, as significant changes in the core geometry occur. Chemistry plays an important role in determining the sequence of events and the fission product releases associated with core melt accidents. Figures 3.1-2 and 3.1-3 illustrate the wide spectrum of melt and boiling temperatures for elements, alloys, fuel, and fission products. Figure 3.1-4 indicates the chemical interactions and liquid phases that can form in a LWR fuel with increasing temperature.[1] Considering this diversity, chemistry is usually a significant contributor to uncertainty in core melt accident predictions. In addition, as indicated in Table 3.1-2, a broad spectrum of accident conditions is encountered in core melt accidents. This also make modeling difficult. Finally differences between BWRs and PWRs, which are discussed in the next subsection, are important in predicting in-vessel as well as ex-vessel severe accident progression. Accordingly, rather than display a plethora of code calculations, a general discussion of major in-vessel phenomena and their potential implications is presented.

This module concludes with a discussion of reactor vessel breach and discharge of core materials into the containment. Accident progression in containment is discussed in Module 4.

3.1.2 Review of Selected Design Features

The student is presumed to be familiar with the general design features of both BWRs and PWRs. The purpose of this subsection is to review with the aid of figures a few important design features that can significantly influence the in-vessel progression of severe accidents, particularly features that differ markedly between BWRs (Figures 3.1-5 to 3.1-7) and PWRs (Figures 3.1-8 to 3.1-11).

As shown in Figure 3.1-5 BWRs have massive steam separators and dryers above the core region. This is not the case for PWRs in which the reactor coolant is subcooled during normal operation and steam is produced in the steam generators, Figure 3.1-8.

BWR fuel assemblies have outer zircaloy flow channels, Figure 3.1-6, that prevent coolant flow between assemblies. PWR fuel assemblies, on the other hand, have no surrounding flow channels, so there is coolant mixing between assemblies, Figure 3.1-9.

BWRs have cruciform control blades, Figure 3.1-7, that enter from the bottom, Figure 3.1-5. PWRs have rod cluster control assemblies, Figure 3.1-10 that enter from the top, Figure 3.1-8. As a result, BWRs have a forest of control rod drives and guide tubes in the bottom heads of their reactor vessels, whereas PWRs have only the bottom (secondary) support assemblies, Figure 3.1-8 and in-core instruments and guide tubes, Figure 3.1-11.

In addition, of course, the BWR operates at about 1000 psia whereas the PWRs operate at about 2200 psia. BWRs have larger pressure vessels to accommodate their steam separators and dryers and their lower power densities (W/cm^3). Finally, BWRs have considerably more zircaloy in their cores than PWRs, mainly in the form of the fuel assembly flow channels.

3.1.3 Accident Initiation (Stage 1)

The extremely wide range of durations for this first stage of accident progression is due to the wide variety of possible accident sequences. In a large-break loss-of-coolant accident (LOCA) reactor coolant blowdown and pressure reduction occur in a matter of seconds. If emergency core cooling systems then fail on demand, Stage 1, accident initiation, has a very short duration. On the other hand, in many accident sequences the loss of coolant and/or the failure of coolant injection may take many hours. For example, in loss of suppression pool cooling accidents identified for Peach Bottom in the Reactor Safety Study, the core is successfully cooled for almost a day before suppression pool overheating causes overpressurization of containment, which, in turn, results in suppression pool flashing and failure of core cooling systems.

The risk posed by severe LWR accidents is considered to be dominated by transient and small-break loss-of-coolant accident sequences in which the core is uncovered only after a prolonged boiloff of reactor coolant. The discussions presented in this module presume, for the most part, that the reactor vessel is pressurized. However, the potential for temperature-induced failures of the reactor coolant system pressure boundary is addressed. In addition, the discussion presumes that reactor shutdown (scram) successfully terminates the fission process, so that decay heat drives the core-damage process. Most of the processes discussed in the context of pressurized, decay-heat driven accidents would exist in unpressurized and/or ATWS sequences as well; although such sequences would differ in timing, rates and extent of core heating and oxidation, thermal-hydraulic conditions including the presence of water in the lower plenum, and other factors.

3.1.4 Reflooding During Accident Progression

One element in the consideration of severe core damage is the potential for reintroducing coolant into a damaged core as occurred at TMI-2. Injection into a damaged core is likely under certain circumstances, for example, when lost electrical power is restored. If water is reintroduced early enough, the configuration of the fuel rods differs little from the original geometry, and the temperatures of the fuel and cladding are only slightly above operating levels. Cooling of the core under these conditions is reasonably assured. However, reintroduction of coolant at later times creates conditions under which the resultant outcome is uncertain. Uncertainties regarding core behavior during coolant reintroduction are discussed for Stages 2 through 6 in the sections indicated in Table 3.1-1. Each stage is first discussed under the presumption that adequate cooling is not restored. The potential for terminating core damage during each stage is then discussed.

Core damage can only be terminated when three conditions are satisfied:

1. Water must be continuously available to the core, core debris, or melt in quantities sufficient to quench the material and remove decay heat and heat associated with metal-water reactions.

2. The core, core debris, or melt configuration must be coolable.

3. Means must be available for cooling the water or condensing the steam produced.

Figure 3.1-12 is a functional event tree which shows the outcomes obtained by meeting all three termination conditions at various stages of core damage either in the reactor vessel or in containment.[2] Water could be delivered in-vessel by normal or emergency coolant supply systems. Water could be delivered ex-vessel by containment sprays or by normal or emergency coolant supply systems with coolant entering the vessel but flowing out of the opening in the bottom head into the reactor cavity. Possible heat sinks include steam generators, the suppression pool and suppression pool cooling system, residual heat removal systems, and containment heat removal systems (fan coolers or spray recirculation systems).

If adequate coolant injection is re-established after core uncovering, but early enough to prevent melting, the core geometry would still be coolable and releases would be limited to activity in the fuel clad gap (Outcome 1). If adequate cooling is re-established later, but in time to prevent extensive meltdown (Outcome 2), the resulting core configuration would be damaged but coolable, perhaps with some coolable debris in the lower head as at TMI-2. Coolability of core debris discharged to containment (Outcomes 3 and 6 in Figure 3.1-12) is discussed in Module 4.

If some, but not all, of the necessary termination conditions can be met, the accident progression can be delayed. For example, partial coolant injection flow can be used to delaying the onset of cladding oxidation. Similarly, if only a limited amount of water can be supplied to a coolable ex-vessel debris configuration, the accident progression may be delayed until the water supply is exhausted (Outcomes 4 and 7 in Figure 3.1-12).

Table 3.1-1 In-Vessel Accident Stages

Stage	Starting Condition	Description	Approximate Duration	Where Discussed
1	Accident Initiator	Initiation	0 -1 day	Section 3.1
2	Core uncovering begins	Core uncovering and heatup	5-35 min	Section 3.2
3	Hottest fuel attains 1832 °F (1000 °C)	Cladding oxidation	5-10 min	Section 3.3
4	Hottest fuel reaches 3350 °F (1843 °C)	Clad melting, fuel liquefaction, holdup in core region	10-30 min	Section 3.4
5	Core materials first enter lower plenum	Core slumping, quenching, reheating	0-80 min	Section 3.5
6	Vessel Breach	Vessel breach and materials discharge to containment	--	Module 4

Table 3.1-2 Severe Accident Conditions

Pressure Range	15 - 2500 psia	(0.1 - 17 MPa)
Decay Power Level	0.8 - 5 %	
Local Heatup Rates	1.3 - 18 °F/s	(0.7 - 10 K/s)
Steam Flow Rates	300 - 6,600 $lb_m/ft^2/hr$	(0.4 - 9 $kg/m^2/s$)
Maximum Midcore Steam Superheat	> 3600 °F	(> 2000 °C)
Maximum Fuel Temperature	> 5180 °F	(> 2860 °C = 3133 K)

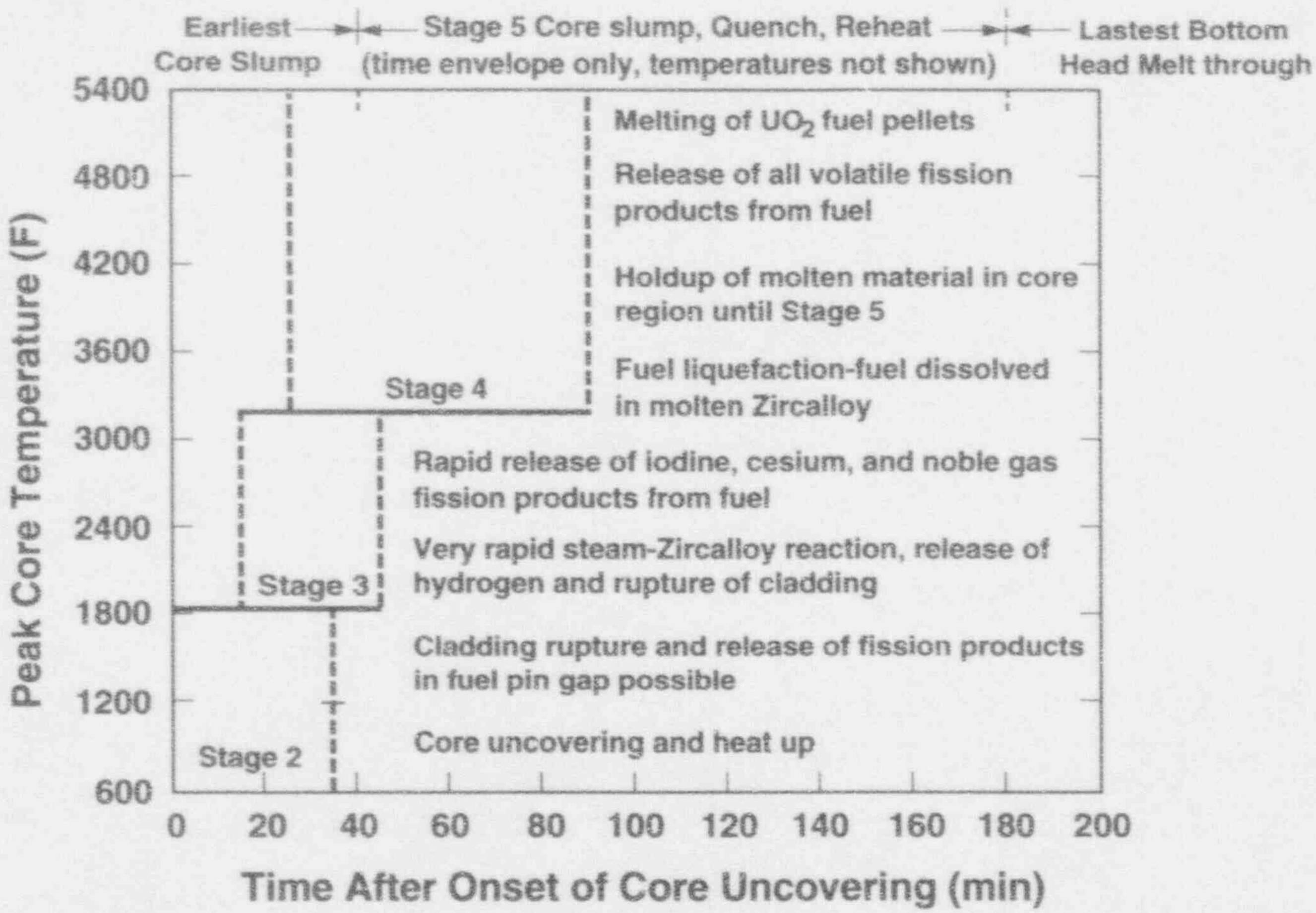


Figure 3.1-1 Approximate temperature and time envelopes for in-vessel severe accident stages assuming no coolant injection during core heatup and degradation

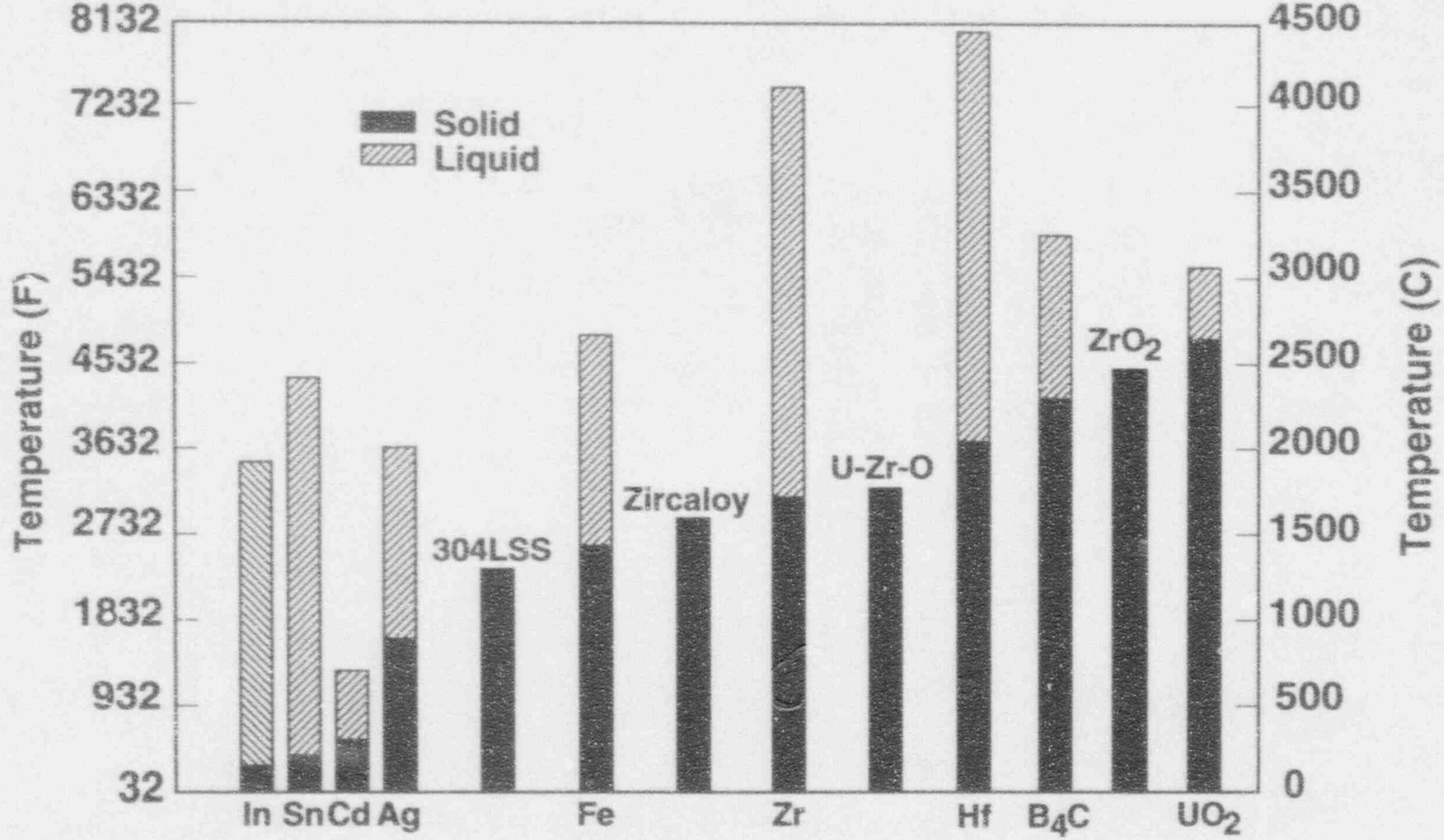


Figure 3.1-2 Melting points for metallic elements, reactor metals, and compounds

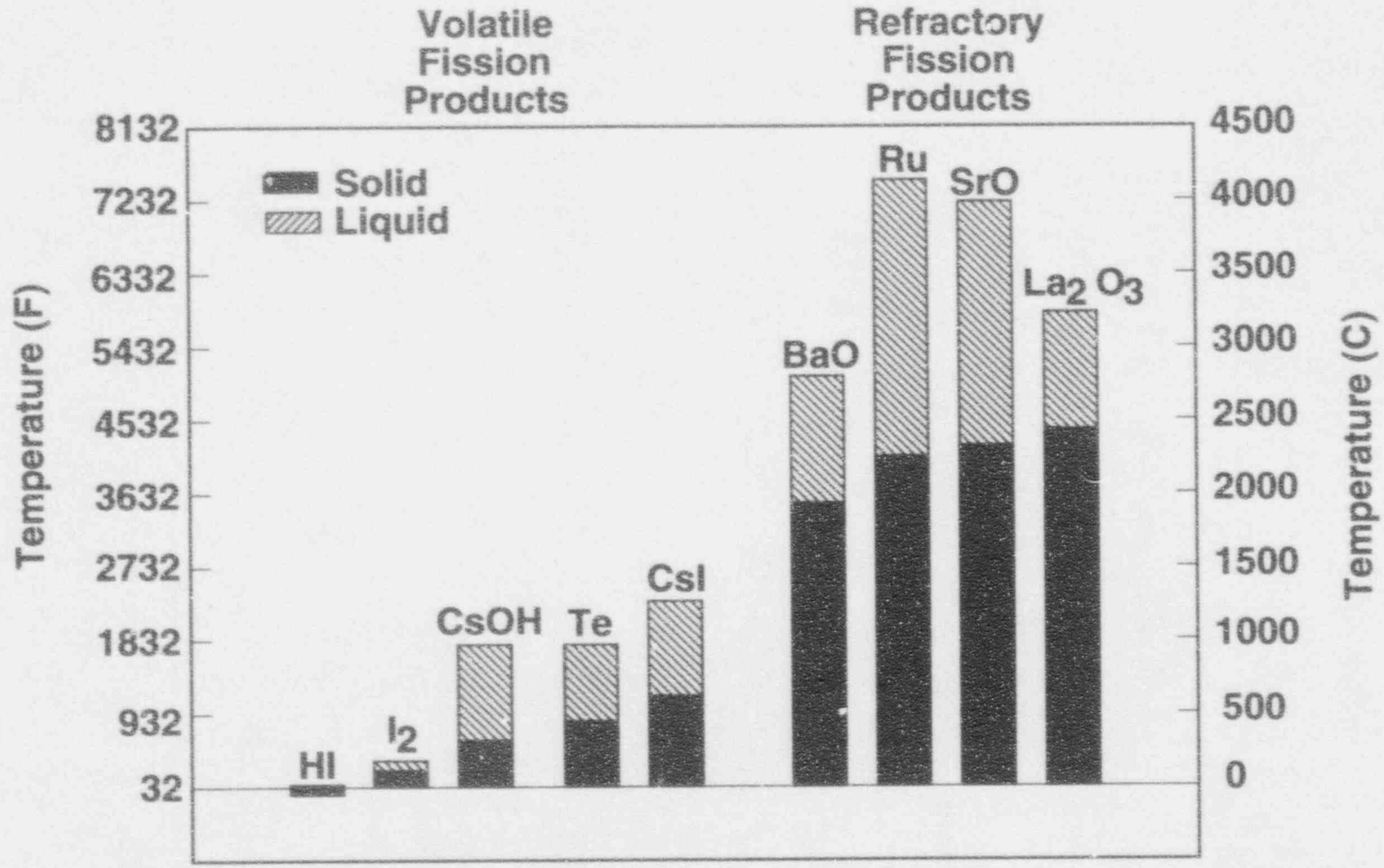


Figure 3.1-3 Melting and boiling points

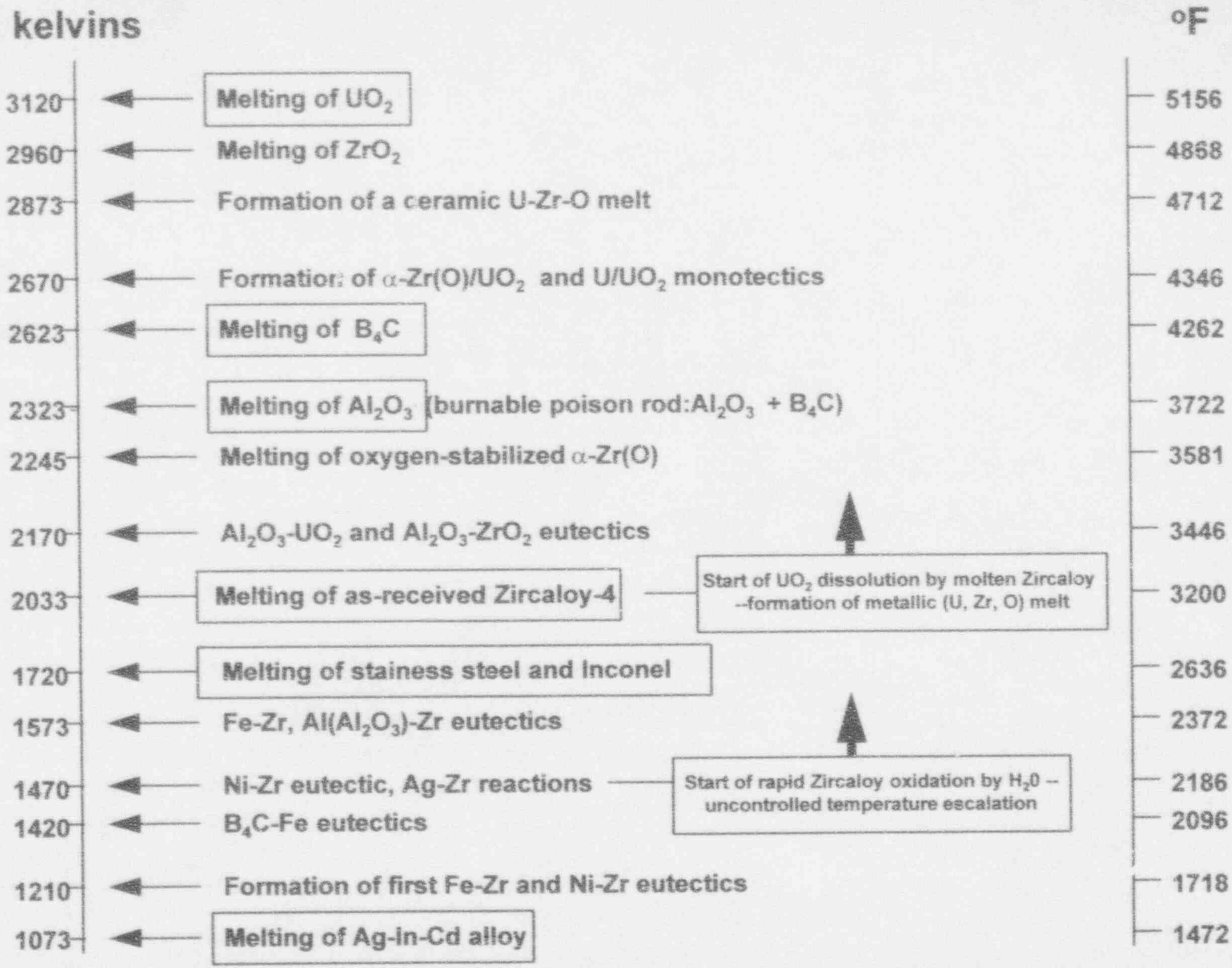


Figure 3.1-4 Chemical interactions and formation of liquid phases in an LWR fuel rod bundle with increasing temperature.

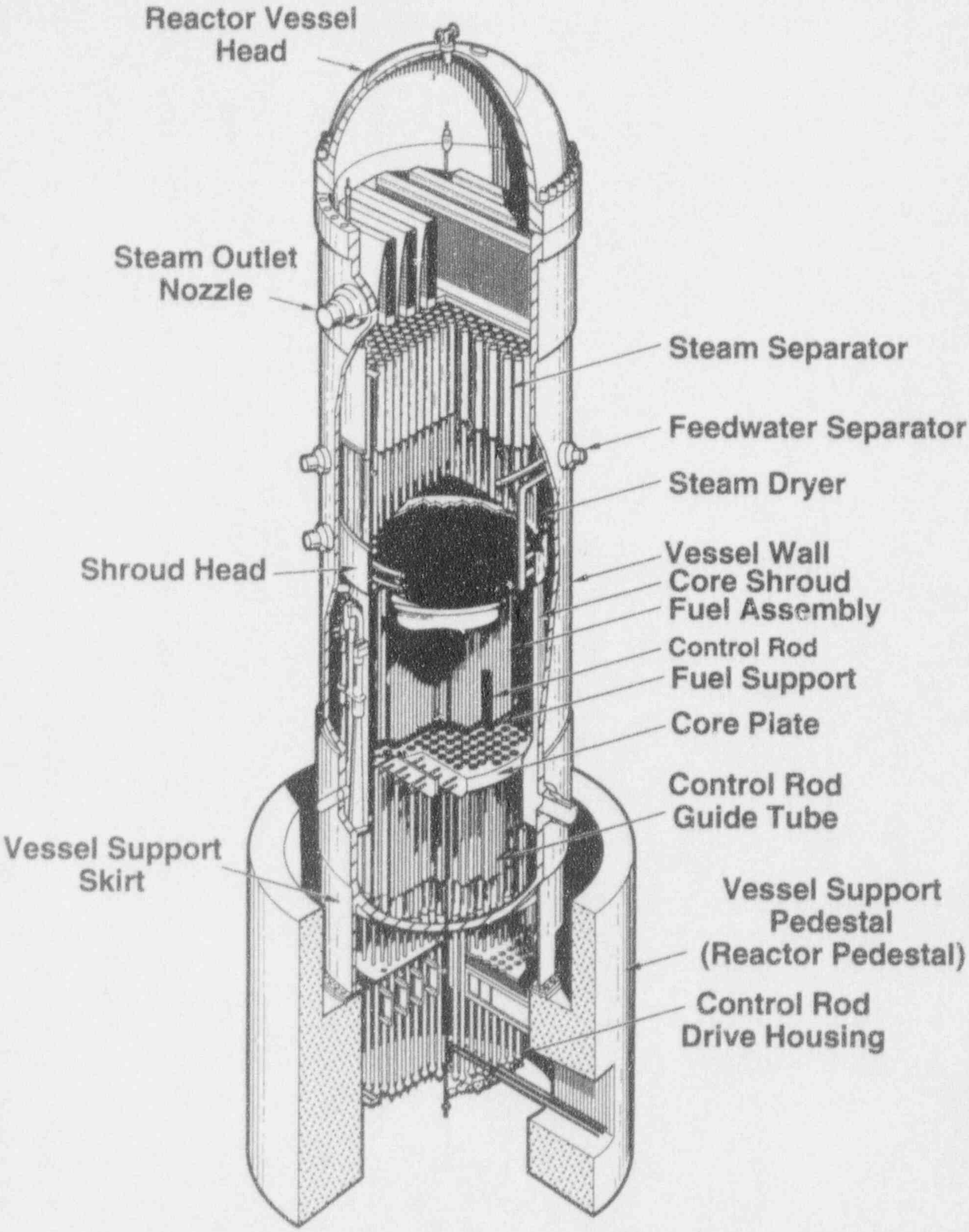


Figure 3.1-5 Schematic of BWR reactor vessel internal structure

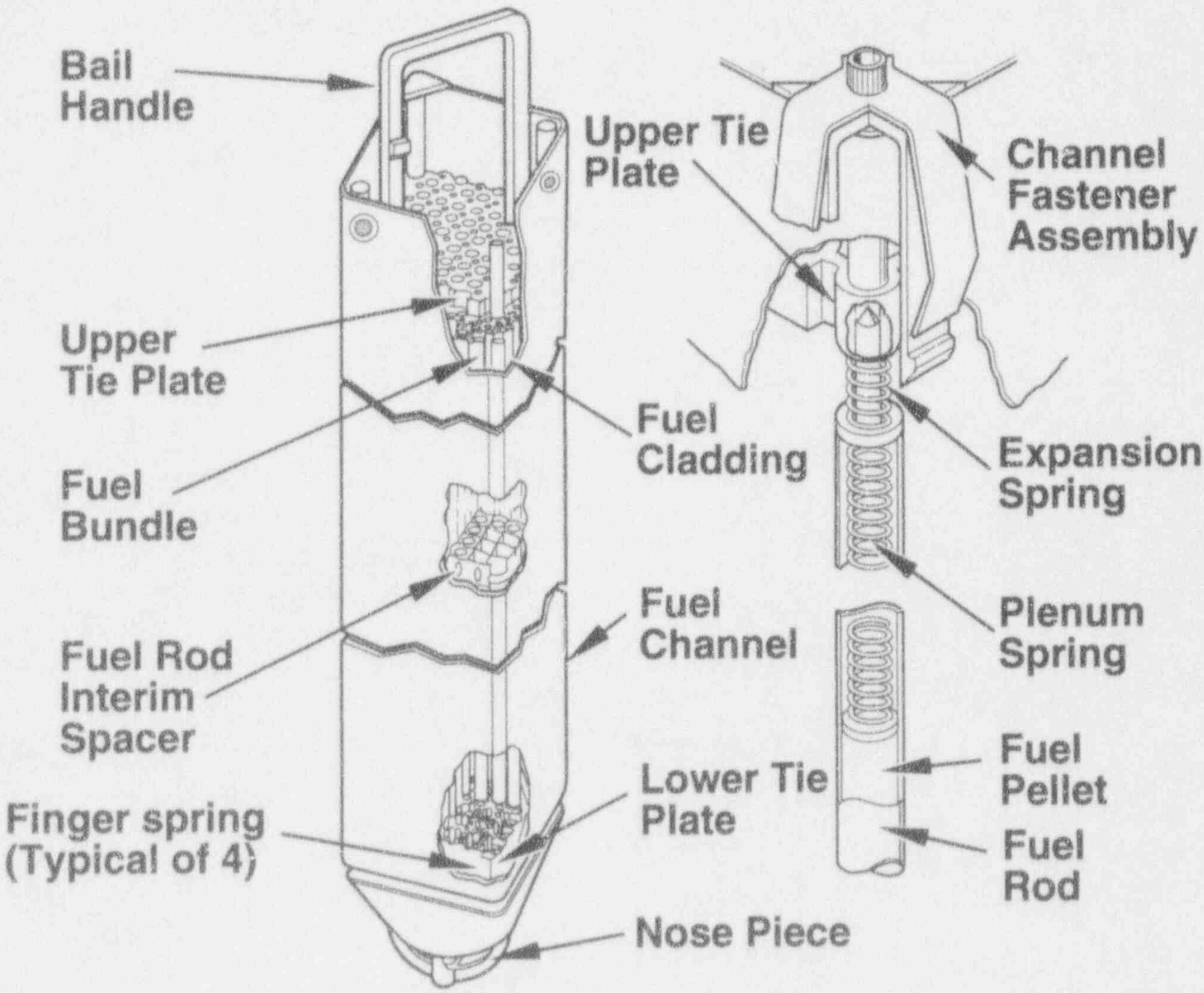


Figure 3.1-6 BWR Fuel Assembly

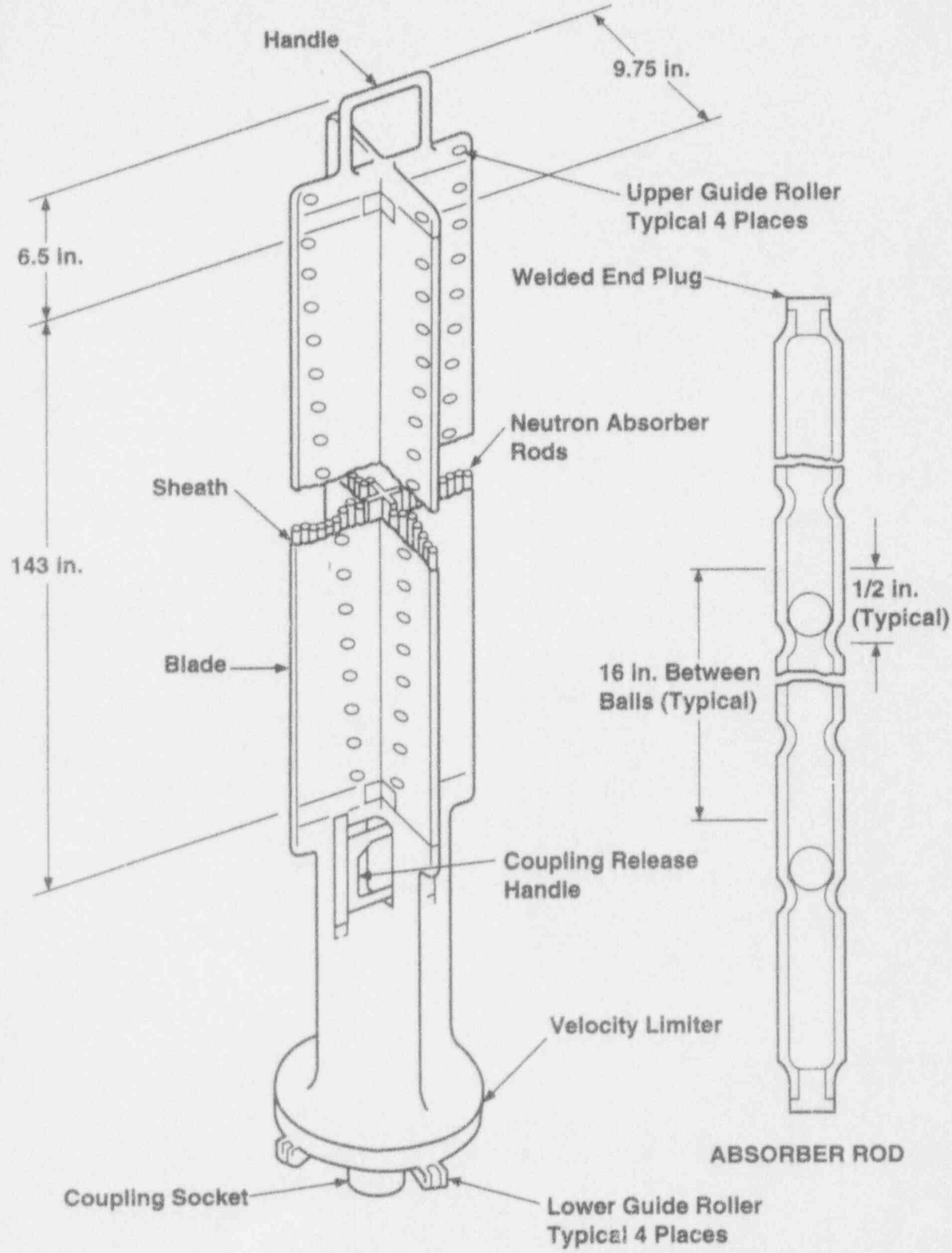


Figure 3.1-7 BWR control rod

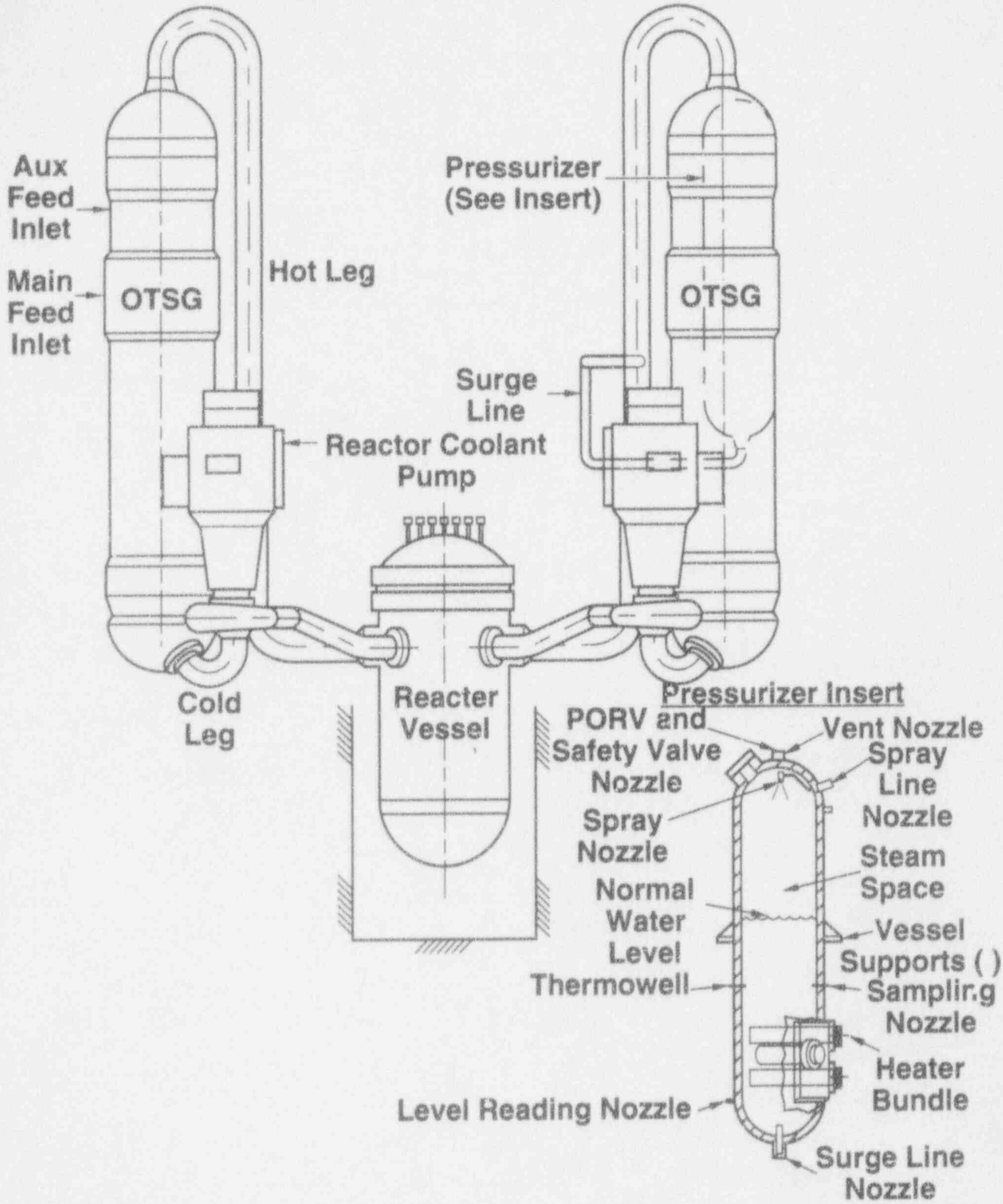


Figure 3.1-8 PWR reactor coolant system arrangement (B & W)

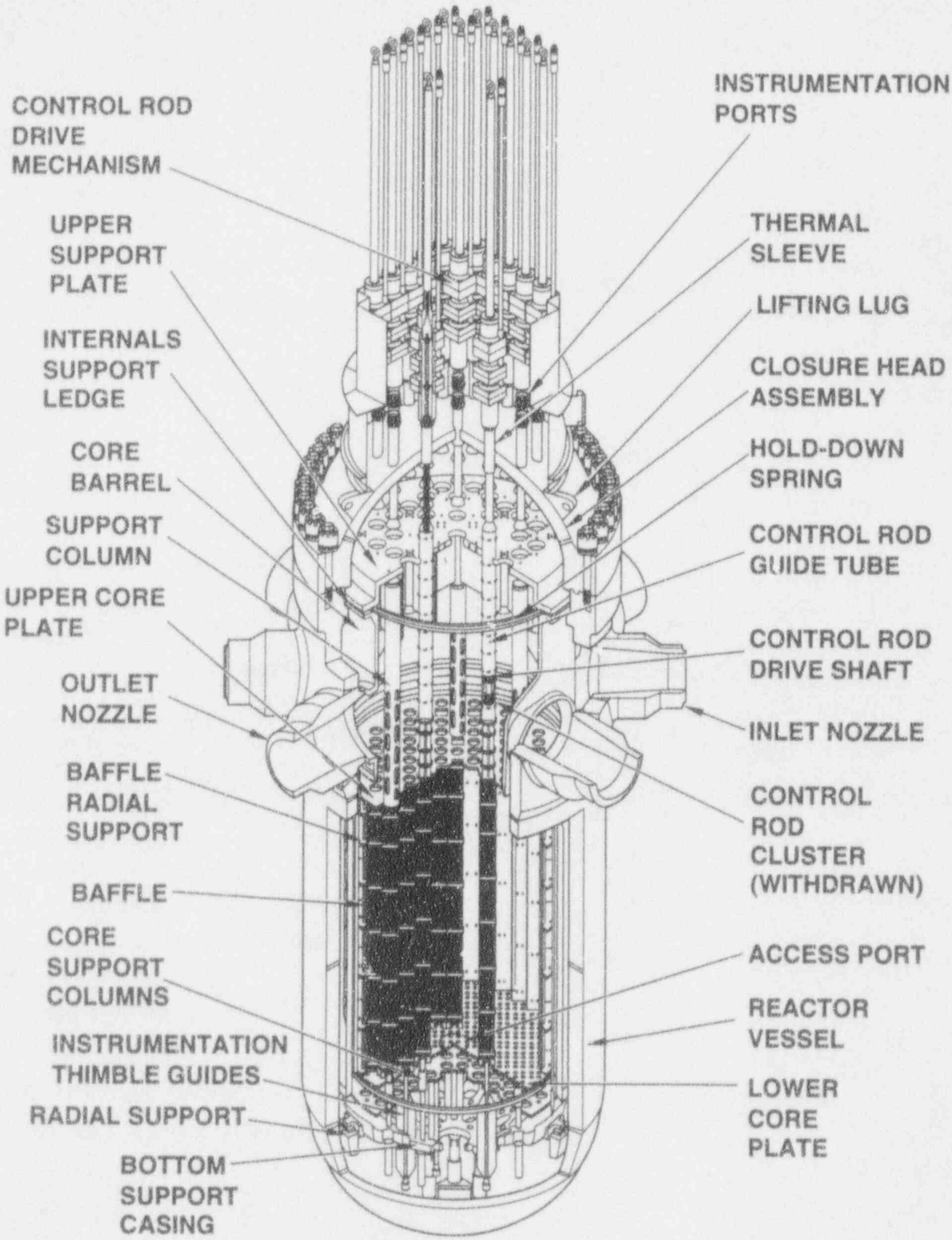


Figure 3.1-9 PWR reactor vessel internals (Westinghouse)

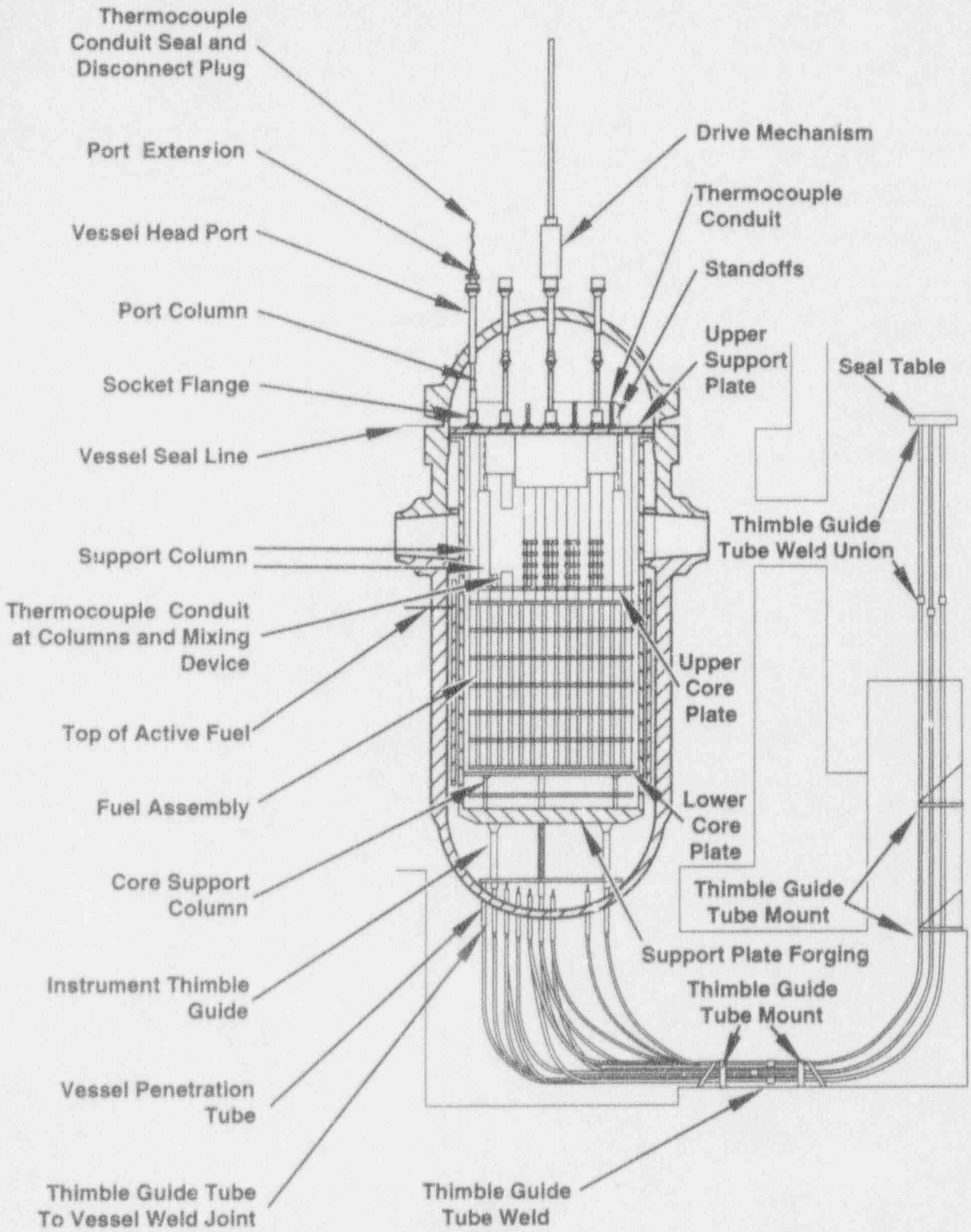


Figure 3.1-10 Typical PWR arrangement for in-core instrumentation (Westinghouse)

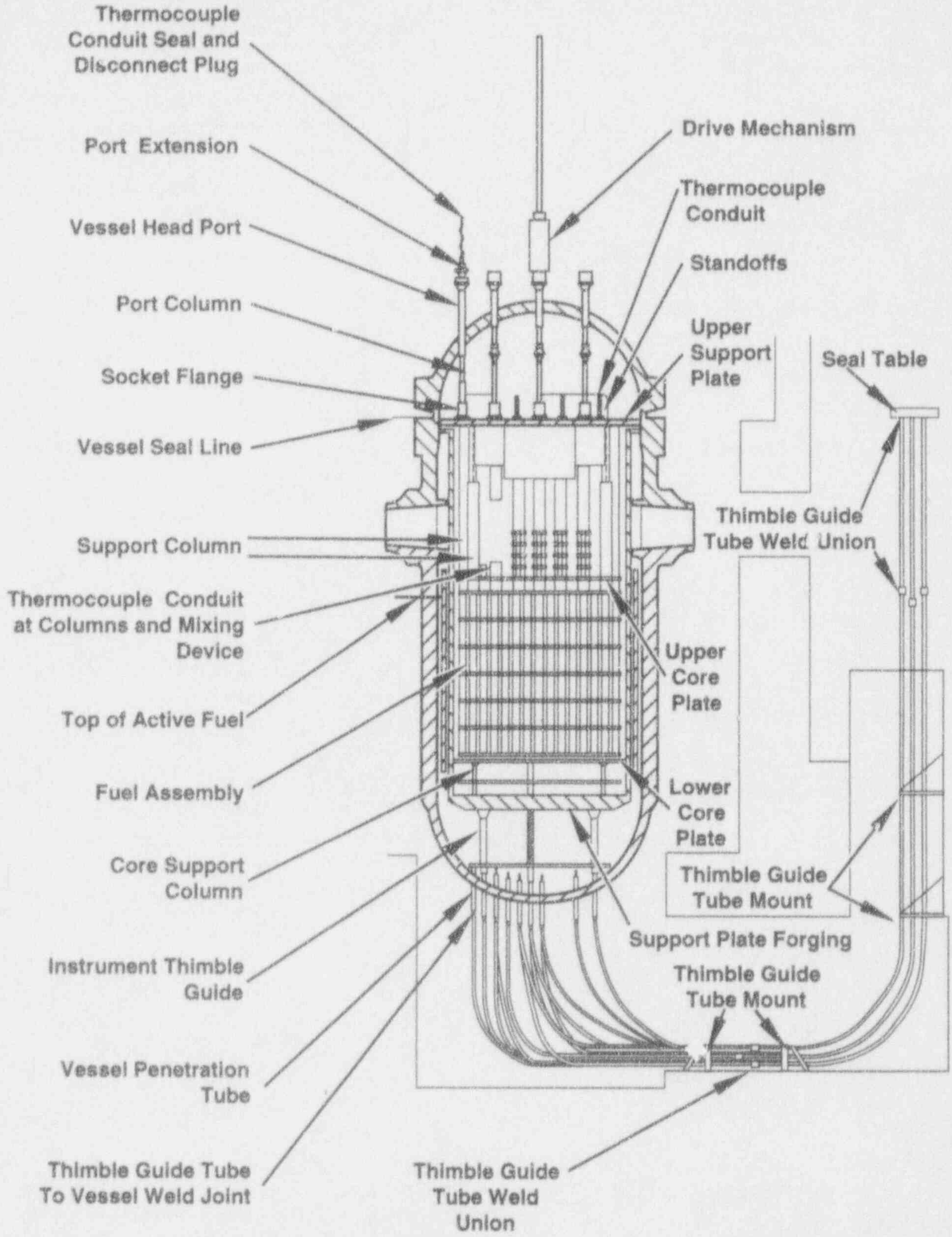


Figure 3.1-11 Typical PWR arrangement for in-core instrumentation (Westinghouse)

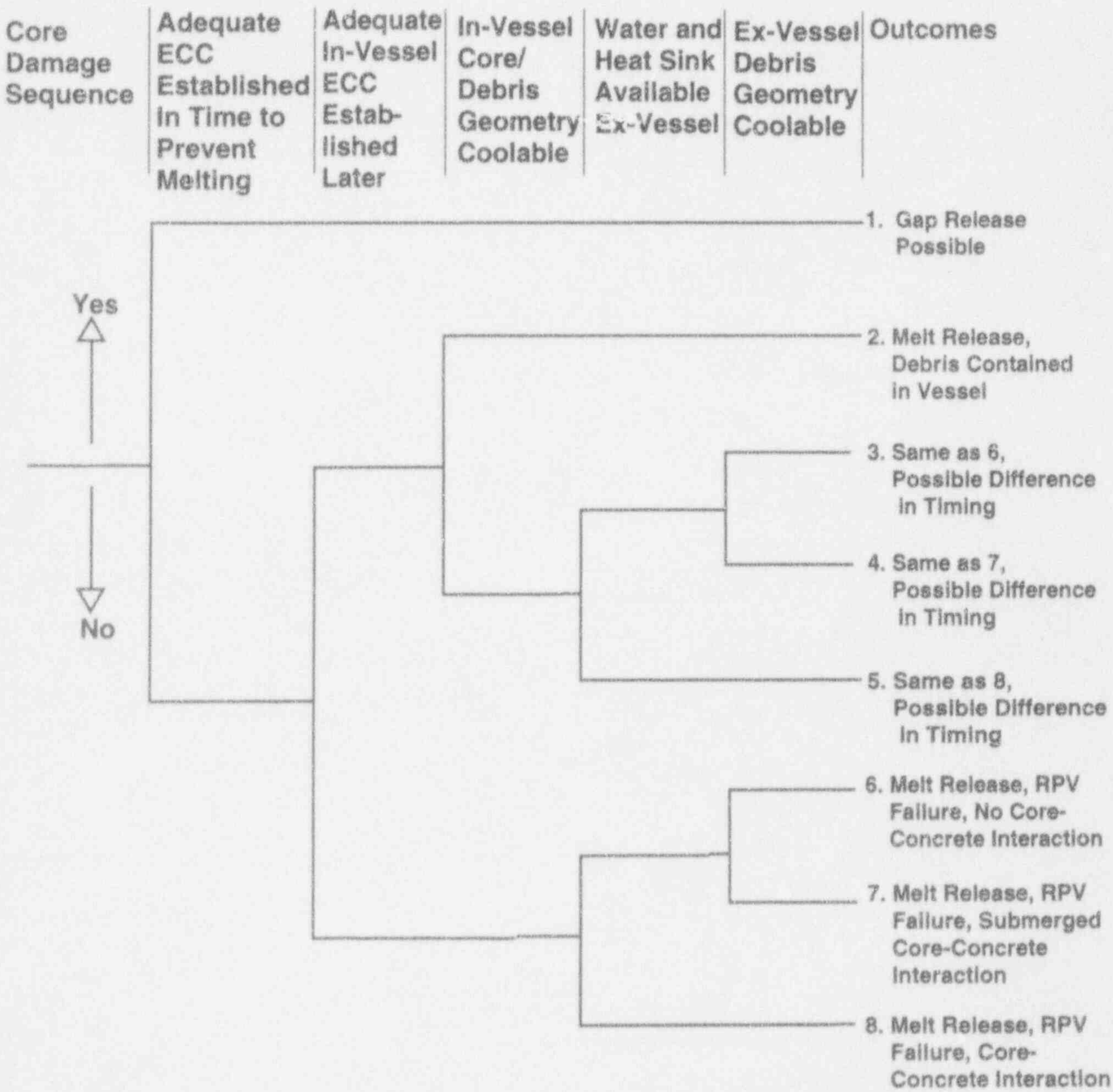


Figure 3.1-12 Core-damage event tree

References for Section 3.1

1. Hoffman, et al. "Reactor Core Materials Interactions." *Nuclear Technology*, Volume 87, August 1989, 147.

2. F.E. Haskin, J.L. Darby, W.B. Murfin, Analysis of Hypothetical Severe Case Core Damage Accidents for the Zion Pressurized Water Reactor, NUREG/CR-1989, SAND81-0504.

3.2 Core Uncovering and Heatup

Core heatup begins with the start of boiloff of water from the core region. Before this time fuel temperatures are close to the system saturation temperature because there is very little heat transfer resistance between the fuel and liquid reactor coolant. So long as fuel remains submerged, it is not expected to be damaged due to high temperature.

3.2.1 Boiloff of Water in Core Region

During the uncovering of the core the fraction of the core decay power that is utilized to vaporize water is reduced as the water level decreases. To a first approximation, all of the decay heat generated in the water covered region results in evaporation, and the water level decreases exponentially with time.[1] In a PWR, sustained core uncovering begins when the water level reaches the top of the active core, the exponentially decreasing water level depicted in Figure 3.2-1 follows from the equation

$$L(t) = L(0)\, e^{-t/\tau} \qquad (3.2\text{-}1)$$

where

$L(t)$= water level above bottom of active core region at time t since the onset of core uncovering,

$L(0)$= water level at the beginning of core uncovering, for a PWR this is the height of the active core region Z (12 ft.),

t = time since onset of core uncovering, and

τ = time constant for boiloff in core region, which is given by the equation

$$\tau = \frac{\rho A Z h_{fg}}{P_D} \qquad (3.2\text{-}2)$$

with

ρ = liquid density,

A = cross-sectional area of liquid in active core region,

h_{fg} = the energy required to evaporate a unit mass of saturated liquid, that is, the latent heat of vaporization, which decreases with increasing reactor coolant system pressure,

P_D = core decay power (approximated as constant during boiloff of water in the core region).

Given the exponentially decreasing water level associated with boiloff in the core region, it takes one time constant for the water level to decrease by a factor of e (from 12 to 4.4 ft) and another time constant for the water level to decrease by another factor of e (from 4.4 ft to 1.6 ft.). It should be noted that the decay constant for boiloff in the core region, τ, varies with the reactor coolant system pressure during boiloff since both the density ρ and latent heat of vaporization h_{fg} vary with saturation pressure. Figure 3.2-2 depicts the change in τ with pressure for the Zion PWR at the decay power (32.5 MW) used in the following example. The total time duration for Stage 2, core uncovering and heatup, is approximately 2τ or, as noted in Table 3.1-1, 5 to 35 minutes depending on the reactor coolant system pressure.

Example 3.2-1 - Time Required for Boiloff in Core Region

In the Zion station blackout accident sequence, steam is discharged from the primary system at the relief valve set point of 2500 psig.[2] The active core height is 12 ft. The area of the core occupied by water is 53.4 ft^2. The core decay power during boiloff is approximately 32.5 MW. Estimate the time required for the water level to decrease from the top of the active core to the core midplane.

Solution:

Solving Eq. (3.2-1) for t and using Eq. (3.2-2) for τ gives

$$t = \frac{\rho A Z h_{fg}}{P_D} \ln\left(\frac{L(0)}{L(t)}\right) \qquad (3.2\text{-}3)$$

From the steam tables, for saturated water at 2515 psia,

$$h_{fg} = 357.0 \ Btu/lb_m$$
$$\rho = 34.83 \ lb_m/ft^3$$

Substituting:

$$t = \frac{(34.83\frac{lb_m}{ft^3})\ (53.4\ ft^2)\ (12\ ft)\ (357.0\frac{Btu}{lb_m})}{(32.5\ \frac{J}{s})\ (\frac{Btu}{1055J})} \ln(\frac{12}{6})$$

$$t = 258.7 \ \ln(2) \ s = 179.3 \ s = 2.99 \ \text{min}$$

A detailed treatment of the axial power distribution, local heat transfer, two-phase mixture dynamics, and coupling with the rest of the reactor coolant system requires the use of complex computer models. Figure 3.2-1 compares the predictions based on Eq. (3.2-1) with code calculations for a Zion station blackout scenario compounded by failure of turbine-driven auxiliary feedwater (the so-called TMLB' scenario).[3] As indicated by the comparison, the exponentially decreasing function defined by Equations 3.2-1 and 3.3-2 is a reasonable approximation for the water level in the core region during this stage of the accident.

3.2.2 Initial Heatup of Uncovered Fuel

Because of low vapor flow rates, the cooling of fuel in the uncovered part of the core by the flow of steam generated during boiloff is relatively ineffective. The temperature rise in the uncovered fuel during the boiloff and initial core heatup stage can, therefore, be approximated as an adiabatic absorption of fission-product decay energy. Using this approximation, the temperature T(z,t) at uncovered elevation z and time t is

$$T(z,t) = T(z,0) + \frac{Z P_D(z)}{m C_p}(t - t_{L=z})$$

where

Z = height of active core region (ft)

mC_p = heat capacity of entire core, J/K (Btu/°F),

$P_D(z)$ = decay power per unit axial height at z above bottom of active core, MW/ft

$t_{L=z}$ = time at which the water level in the core region equals z, seconds

Figure 3.2-3 compares the results of an adiabatic heatup calculation with code calculated core temperatures. The adiabatic heatup approximation appears reasonable.

The simplifying assumptions used to develop the analytic approximations presented above break down near the start of the next stage, cladding oxidation, which occurs when the peak fuel temperature reaches about 1832°F (1000 °C or 1273 K).

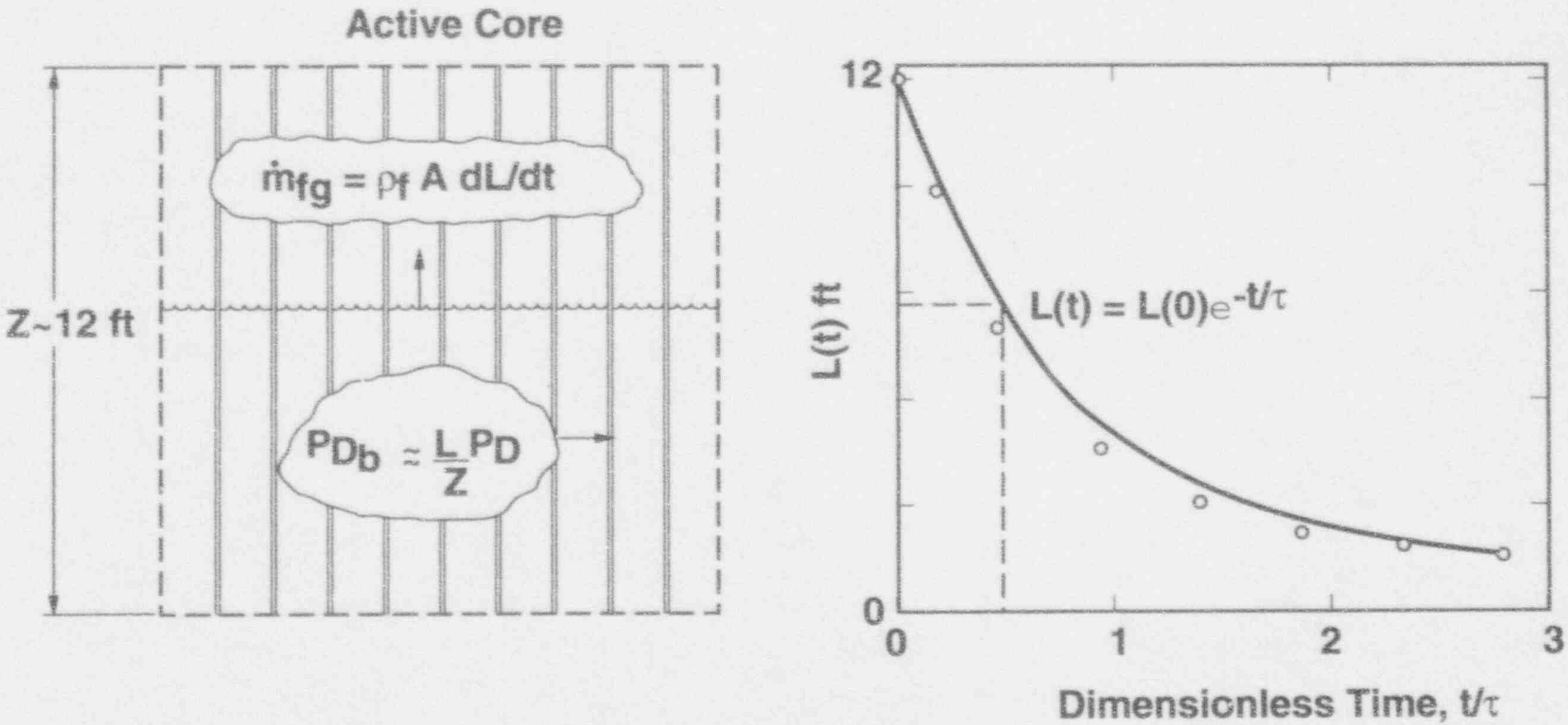


Figure 3.2-1 Exponentially decreasing water level

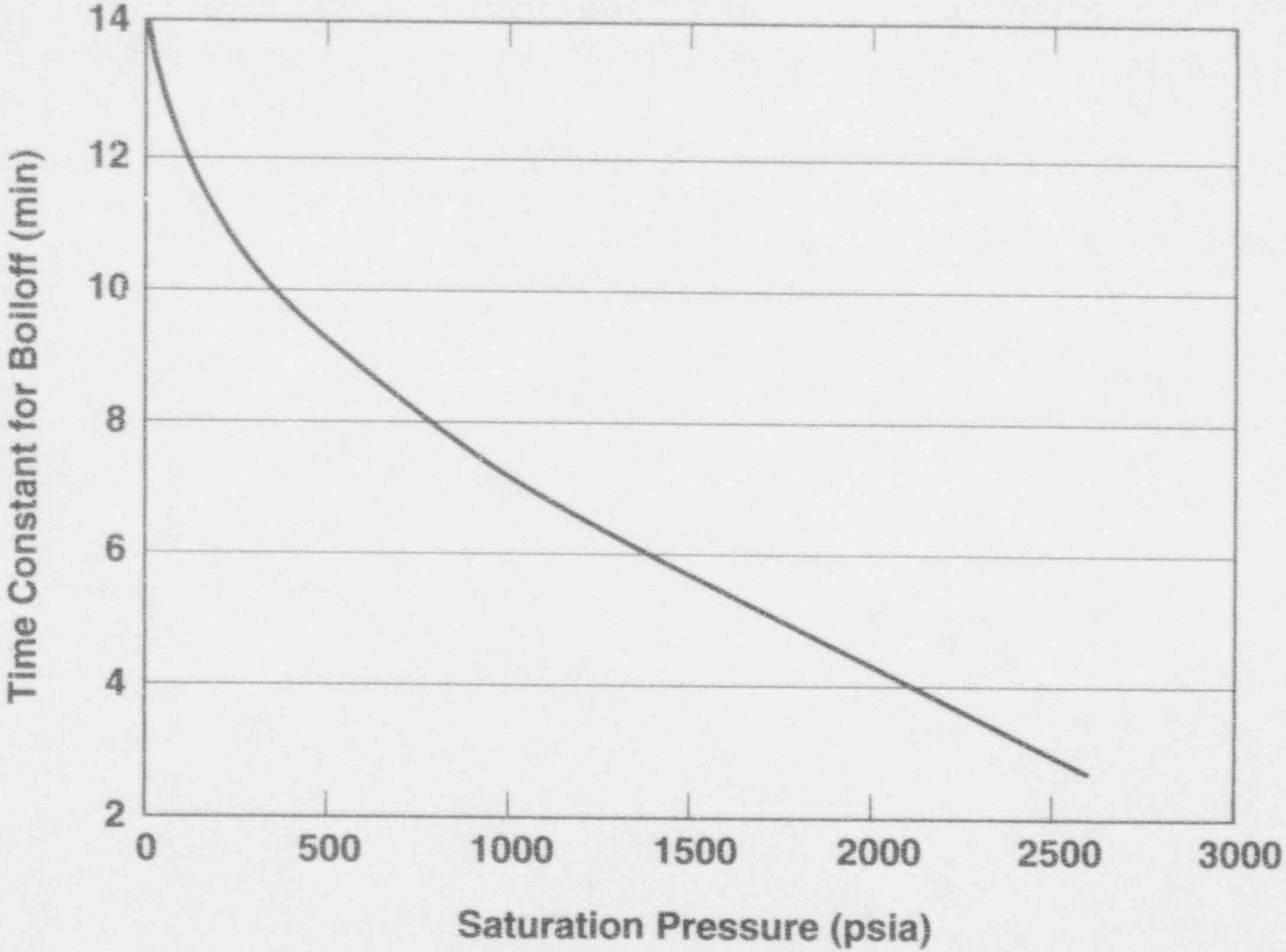


Figure 3.2-2 Variation of boiloff time constant with saturation pressure

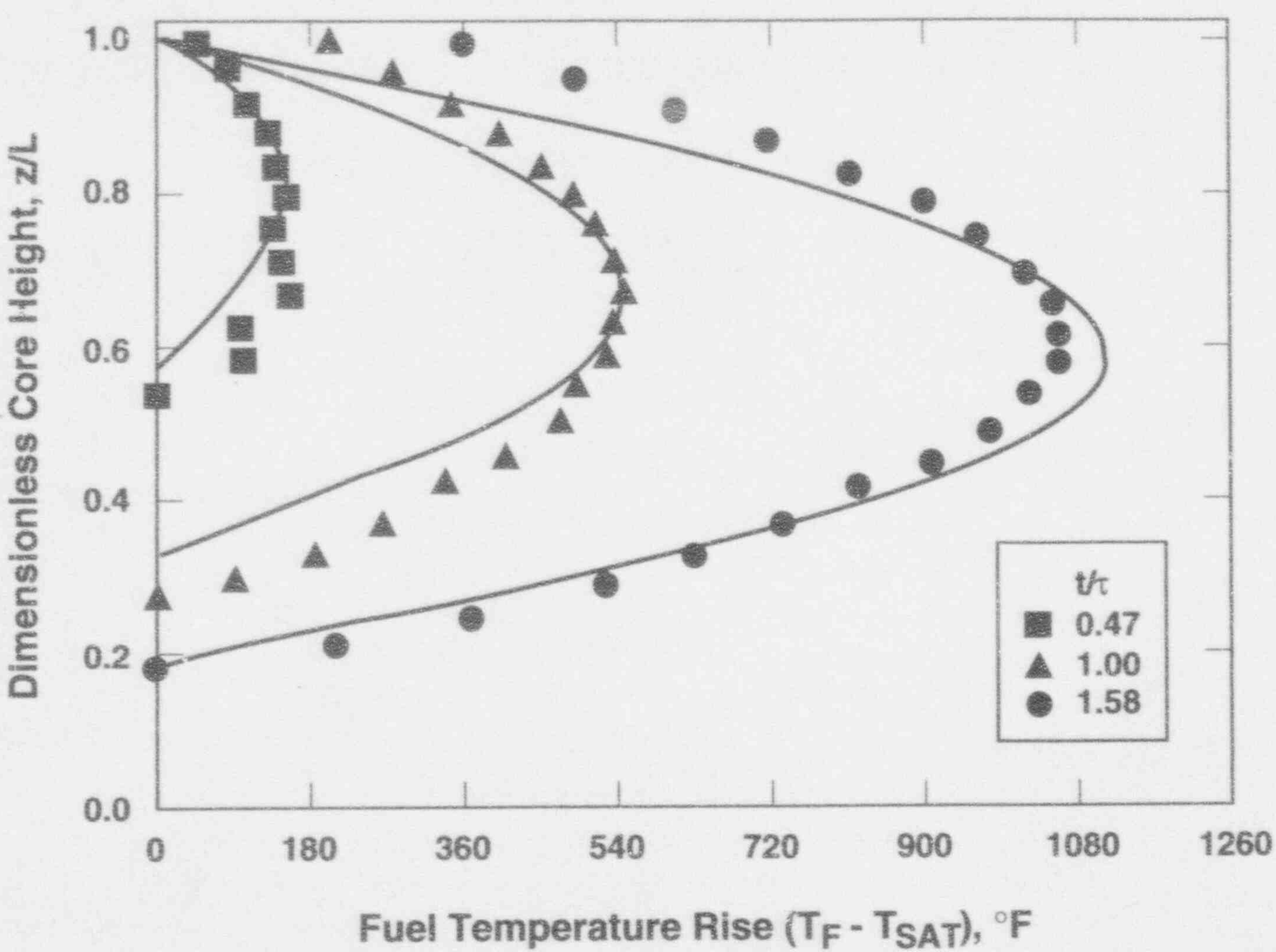


Figure 3.2-3 Approximate calculation of fuel temperature rise (curves) at three different times compared with code results

References for Section 3.2

1. B. Rivard and F. E. Haskin, "LWR Meltdown Analyses and Uncertainties," ANS/ENS Topical Meeting on Reactor Safety Aspects of Fuel Behavior, Sun Valley, ID, (August 2-6, 1981).

2. F. Eric Haskin, Walter B. Murfin, Joseph B. Rivard, John L. Darby, Analysis of a Hypothetical Core Meltdown Accident Initiated by Loss of Offsite Power for the Zion 1 Pressurized Water Reactor, NUREG/CR-1988, SAND81-0503 (November 1981).

3. J. B. Rivard et al, Interim Technical Assessment of the MARCH Code, NUREG/CR-2285, SAND81-1672 (February 1981).

3.3 Cladding Oxidation

The start of Stage 3 (Table 3.1-1) is marked by the initiation of significant cladding oxidation, which occurs when the peak fuel temperature reaches about 1832 °F (1000 °C).[1] The chemical reaction is

$$Zr + 2H_2O \rightarrow ZrO_2 + 2H_2 \quad (3.3\text{-}1)$$

This reaction is particularly important because it is highly exothermic (approximately 6.5 MJ/kg (280 BTU/lbm) of Zr reacted), the reaction rate increases strongly with cladding temperature, and the noncondensible gaseous reaction product is hydrogen.

3.3.1 Reaction Kinetics

A considerable amount of data on oxidation-reaction kinetics exists. If adequate steam is available, it is generally believed that the reaction is limited by oxygen diffusion through the ZrO_2 film and the underlying metal. In this case, the reaction rate is governed by parabolic kinetics; that is, $W^2=kt$ where W is the weight of metal reacted, t is the time, and k is the rate constant, which increases exponentially with temperature. The following equation can be used to estimate the mass of Zr oxidized at a particular temperature in a steam environment as a function of time.

$$W_{Zr} = \sqrt{A\ t\ e^{-B/RT}} \quad (3.3\text{-}2)$$

Where,

W_{Zr} = mass of Zr oxidized per unit area exposed to steam, kg_{Zr}/m^2 (lbm_{Zr}/ft^2).

t = exposure time, s,

T = temperature of surface, K, (°R),

R = universal gas constant, 8314.29 J/(kg-mole·K). (1.98583 BTU/lb-mole/°R)

Correlations with experimental data have provided several alternative estimates of the empirical constants A and B.[2,3,4] The values obtained by Cathcart are

A = 294 $kg^2/(s \cdot m^4)$ (12.3 $lbm^2/ft^4/s$),

B = 1.672 x 10^8 J/kg-mole (7.195 x 10^4 BTU/lb-mole),

Figure 3.3-1 shows the mass of hydrogen produced as a function of time for several temperatures. Figure 3.3-2 shows the mass Zr oxidized in 5 minutes at constant temperature as a function of temperature for surface area of 5400 m^2 (58000 ft^2), corresponding to a PWR core.

3.3.2 Oxidation Front

The preceding isothermal example is not realistic because the exothermic energy associated with the oxidation reaction would actually cause the cladding and fuel temperatures to increase rapidly. Reaction energy is removed from the surface by hydrogen and by inward and axial transfer to the metal substrate and then to the fuel. When the reaction zone attains temperatures above about 2420°F (1327°C =1600 K), the oxidation rate becomes so large that nearly all the available steam is reacted for typical boiloff sequences. This condition is referred to as steam limiting because the oxidation rate is limited by the amount of steam available to react with the cladding.

Example 3.3-2: Hydrogen Production Rate

a. What is the hydrogen production per unit surface area of Zr after 5 minutes exposure to steam at 2192 °F (1200 °C)?

b. If all of the cladding (5400 m², 26,940 lb_m) in the Zion PWR were exposed to such an environment in a severe accident, how much hydrogen (kg) would be produced?

c. Estimate the total energy release.

Solution:

a. Substituting into Eq (3.3-2) gives

$$W_{Zr} = \sqrt{\frac{294\ (kg_{Zr})^2}{m^4 \cdot s} \Big| \frac{5\ \text{min}}{} \Big| \frac{60\ s}{\text{min}} \exp\left(\frac{-1.672x10^8\ J}{kg\text{-}mole} \Big| \frac{kg\text{-}mole \cdot K}{8314.29J} \Big| \frac{}{1473.15\ K} \right)}$$

$$W_{Zr} = 0.322\ kg_{Zr}/m^2$$

Multiplying W_{Zr} by the surface area of 5400 m² gives the mass of Zr that could be oxidized according to the parabolic kinetics:

$$m_{Zr} \leq \frac{0.322\ kg\ Zr}{m^2} \Big| \frac{5400\ m^2}{} = 1{,}740\ kg\ Zr = 3.83x10^3\ lb_m\ Zr$$

This is 14.2% of the 26,940 lb_m Zr present.

b. By Equation (3.3-1), two moles of hydrogen are produced per mole of Zr reacted; hence, the number of moles of hydrogen released is

$$n_{H_2} = \frac{1{,}740\ kg\ Zr}{} \Big| \frac{kg\text{-}mole\ Zr}{91.22\ kg\ Zr} \Big| \frac{2\ kg\text{-}moleH_2}{kg\text{-}mole\ Zr} = 38.1\ kg\text{-}mole\ H_2$$

The corresponding mass of hydrogen is

$$m_{H_2} = \frac{38.1\ kg\text{-}mole\ H_2}{} \Big| \frac{2.016\ kg\text{-}H_2}{kg\text{-}mole\ H_2} = 76.9\ kg\ H_2$$

c. The total energy released is estimated as the mass of Zr reacted times 6.5 MJ/kg.

$$\Delta H_{rxn} = \frac{1{,}740\ kg\ Zr}{} \Big| \frac{6.5\ MJ}{kg\ Zr} \Big| \frac{GJ}{10^3\ MJ} = 11.3\ GJ$$

Figure 3.3-3 illustrates a calculation of the thermal behavior of fuel during the oxidation stage of core degradation.[5] The calculation is one dimensional, and does not account for the natural-circulation flow discussed later (see 3.3.5). The calculated behavior is characterized by smooth temperature profiles, which follow the axial power profile (see Eq. 3.2-1 and Fig. 3.3-2) until the onset of significant zircaloy oxidation. Significant oxidation occurs first near the location of maximum axial power. As oxidation continues, a sharp temperature profile develops, reflecting a distinct oxidation front. Oxidation increases rapidly near the front and then decreases with elevation due to steam depletion. The relatively short 5 minute duration in Table 3.1-1 for Stage 3 is based on calculations that indicate average temperature rise rates in excess of 3.6°F/s (2 K/s) in regions undergoing vigorous oxidation.[5]

Figures 3.3-4 and 3.3-5 illustrate the potential contribution of the zirconium oxidation energy to the overall energy release rate in the core region, as a function of oxidation temperature. Decay heat transfer to residual saturated water below the uncovered portion of the core results in a steam production rate that is proportional to the below-water portion of the decay heat power, P_{Db}. As indicated in Figure 3.3-5, at sufficiently low peak cladding temperature, the energy release rate due to oxidation is negligible compared to that due to decay power. However, as the cladding temperature in the uncovered core region increases to about 1832°F (1000°C = 1273 K), more and more of the vapor generated by evaporation of residual water participates in the zirconium oxidation reaction. At sufficiently high cladding temperatures, virtually all of the resulting vapor could participate in the zirconium oxidation reaction. In this so-called steam limited condition, the ratio of the energy release rate by the oxidation reaction to the decay power released below the water level, $P_{oxidation}/P_{Db}$, would at least equal the ratio of the oxidation energy Δh_{rxn} to the latent heat of vaporization h_{fg} (both normalized to a unit mass of steam). As indicated in Figure 3.3-5, this ratio varies from 6.3 at atmospheric pressure to 19 at 2500 psig. Even if P_{Db} were just 1/20 of the total decay heat power, the oxidation energy could be comparable to the decay heat power during Stage 3.

The preceding argument ignores potential energy transfer from the hot, uncovered core region downward to the residual water. As indicated in Figure 3.3-4, each unit of energy that is transferred downward to the saturated residual water results in the production of additional steam to fuel the oxidation reaction. With significant feedback, for example due to radiative heat transfer from the hot reaction zone to the residual water, the energy release rate from oxidation can easily and substantially exceed that from decay heat power. The acceleration of energy release rates from zircaloy oxidation with temperature, which is illustrated by Figure 3.3-5, has been observed experimentally.

3.3.3 Core Damage Due to Oxidation

Clad melting is excluded during Stage 3, which is by definition (Table 3.1-1) limited to temperatures of 3350°F (1843°C = 1570 K) or less. Nevertheless, several types of cladding damage can occur during Stage 2. The cladding is simultaneously subjected to thermal transients and, particularly if the reactor coolant system is depressurized, to stresses resulting from increased internal pressure of the initial fill gases and fission gases. At low reactor coolant system pressures, ballooning of the cladding is expected prior to rupture. The temperature and pressure at which ballooned Zircaloy-4 cladding bursts in a steam environment has been studied, and it has been found that, even at low (initial) internal pressures, cladding usually bursts at temperatures below 2192°F (1200°C = 1473 K).[6]

Zirconium-burning tests result in clouds of smoke issuing from the test chamber, indicating that large quantities of aerosols may be generated during the oxidation.[7] Such aerosols may have a tendency to accelerate the plateout of fission products within the reactor coolant system.

Embrittlement and spallation of ZrO_2 from the surface of the cladding as oxidation proceeds may weaken the fuel rods, expose more fresh Zirconium metal, and/or produce debris with the potential for blocking coolant flow channels. Increases in the cladding surface area exposed to steam can increase the oxidation rate if the reaction is not already steam starved.

Because low-melting-point silver-indium-cadmium alloys are often employed in PWR control rods, the possibility exists for formation of significant molten quantities of these materials at the temperatures attained during Phase 2. It is uncertain when, and how coherently, such melts might move through the core region, before contacting residual water or core support structures.

3.3.4 Reflooding During Stage 3

During a normal boiloff mechanisms for transferring energy from uncovered fuel to residual water are limited principally to radiative heat transfer. On the other hand, if water is reintroduced to the core zone (reflooding) during the oxidation (Stage 3), the core-damage processes may initially be accelerated (and hydrogen generation increased) due to cladding oxidation by the additional steam generated during the cooling of overheated fuel. Considerable fracturing of cladding embrittled during oxidation is expected during reflood, leading to the formation of fairly coarse rubble (fractured cladding, fuel, and control materials) within the central region of the core (as at TMI-2). It is possible that the rubble beds formed can be maintained in a cooled condition, terminating the accident during this stage. (At TMI-2 coolant was not permanently restored until the accident had progressed beyond Stage 3, yet the debris was ultimately cooled in-vessel.) However, cooling of a reflooded core that has undergone severe damage would have to be maintained long-term. Additional aspects of rubble-bed cooling are discussed in Section 3.5.

3.3.5 Natural Circulation During Core Degradation

In PWR accidents in which the reactor coolant system is not depressurized, as the core heats up, gas movement in the uncovered core and upper head regions begins to be driven by natural convection (buoyancy forces).[8] Heat and mass transfer from the core to the reactor coolant system structures are dominated by buoyancy-driven components of the flow field. Steam from the boiloff of residual in-vessel water and hydrogen from oxidation of fuel cladding rise from the hot central core region and lose heat and entrained fission products to relatively colder structures above the core. As depicted in Figure 3.3-6, the cooled gases recirculate downward through the colder regions of the uncovered core and are reheated again by flowing up through the hot central core region.

In BWRs, the fuel channels which enclose the rods of individual fuel assemblies impede in-core natural circulation. However, if the residual water level falls below the bottom of the BWR downcomer region while fuel is still heating up in the core region, a strong natural convection loop can be established from the core to the steam separators and dryers with return to the core inlet via the downcomers. This is depicted in Figure 3.3-7.

For some high-pressure PWR accidents (see Section 3.4.4), it has been suggested that the natural circulation flows in PWRs could transfer sufficient heat to the reactor coolant system pressure boundary to result in relatively early temperature-induced failures of the reactor coolant system pressure boundary.[9] The resulting depressurization of the primary system would alter the thermal-hydraulic progression of the accident. In particular, depressurization would preclude the potentially severe ramifications associated with high-pressure ejection of melt into the containment (see Section 3.5). It should be noted, however, that early temperature-induced failure did not occur at TMI-2. Nevertheless, codes capable of modeling natural circulation are currently being exercised in attempts to investigate the likelihood of such early temperature-induced failures in various PWR severe accident scenarios.

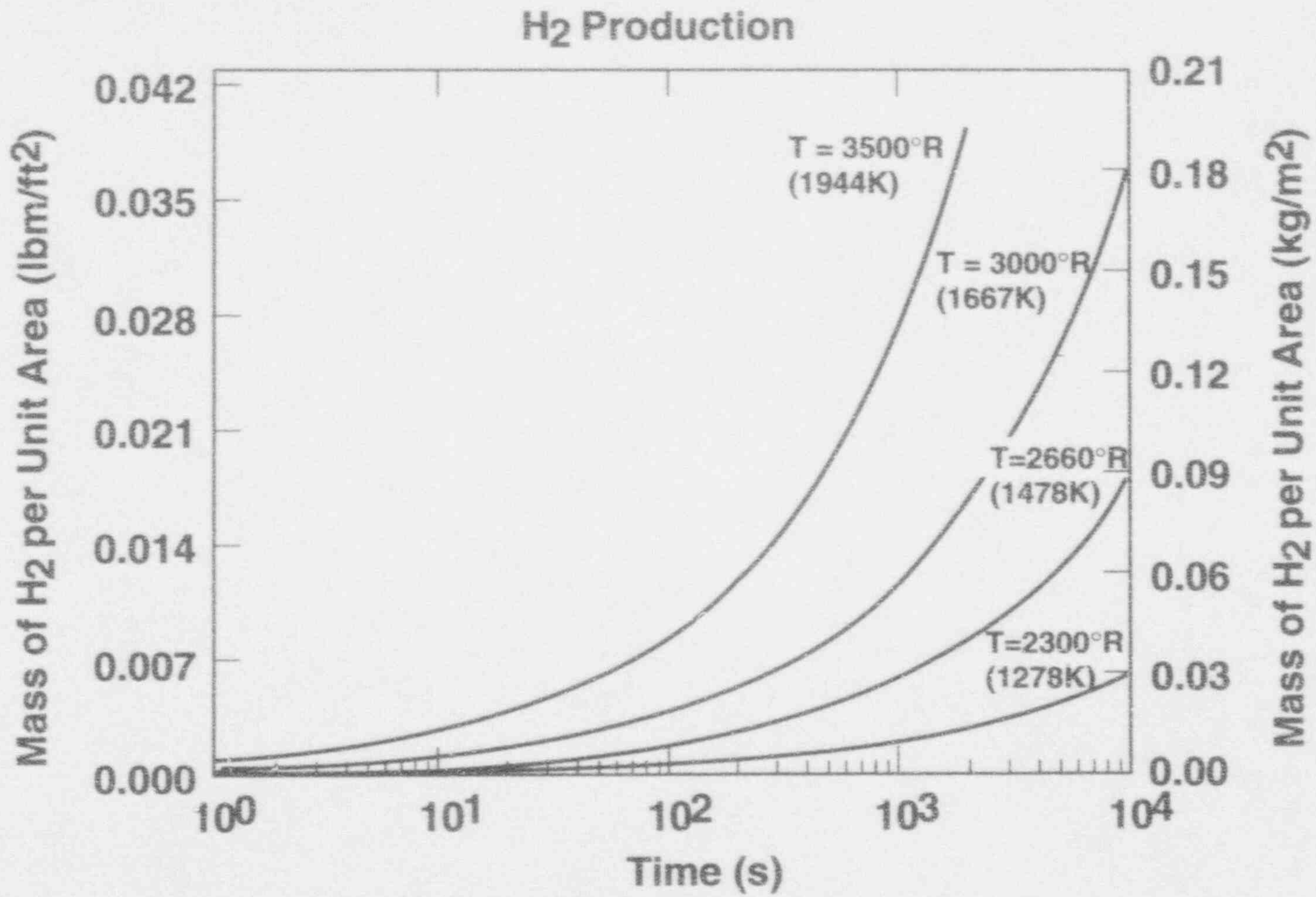


Figure 3.3-1 Hydrogen production per unit are from the Zr:H_2O reaction

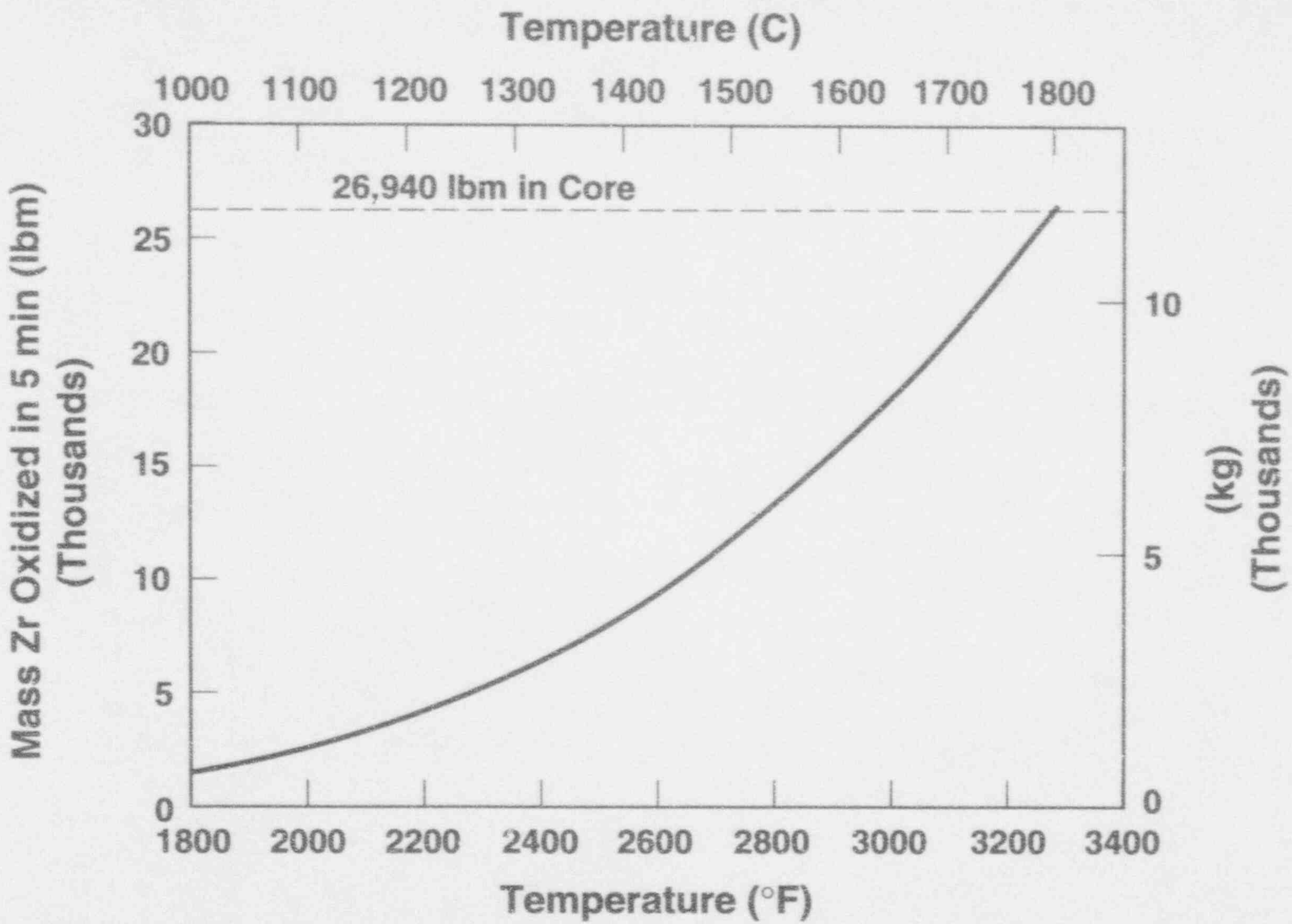


Figure 3.3-2 Mass of Zr oxidized in 5 minutes exposure of 5400 m^2 zircaloy

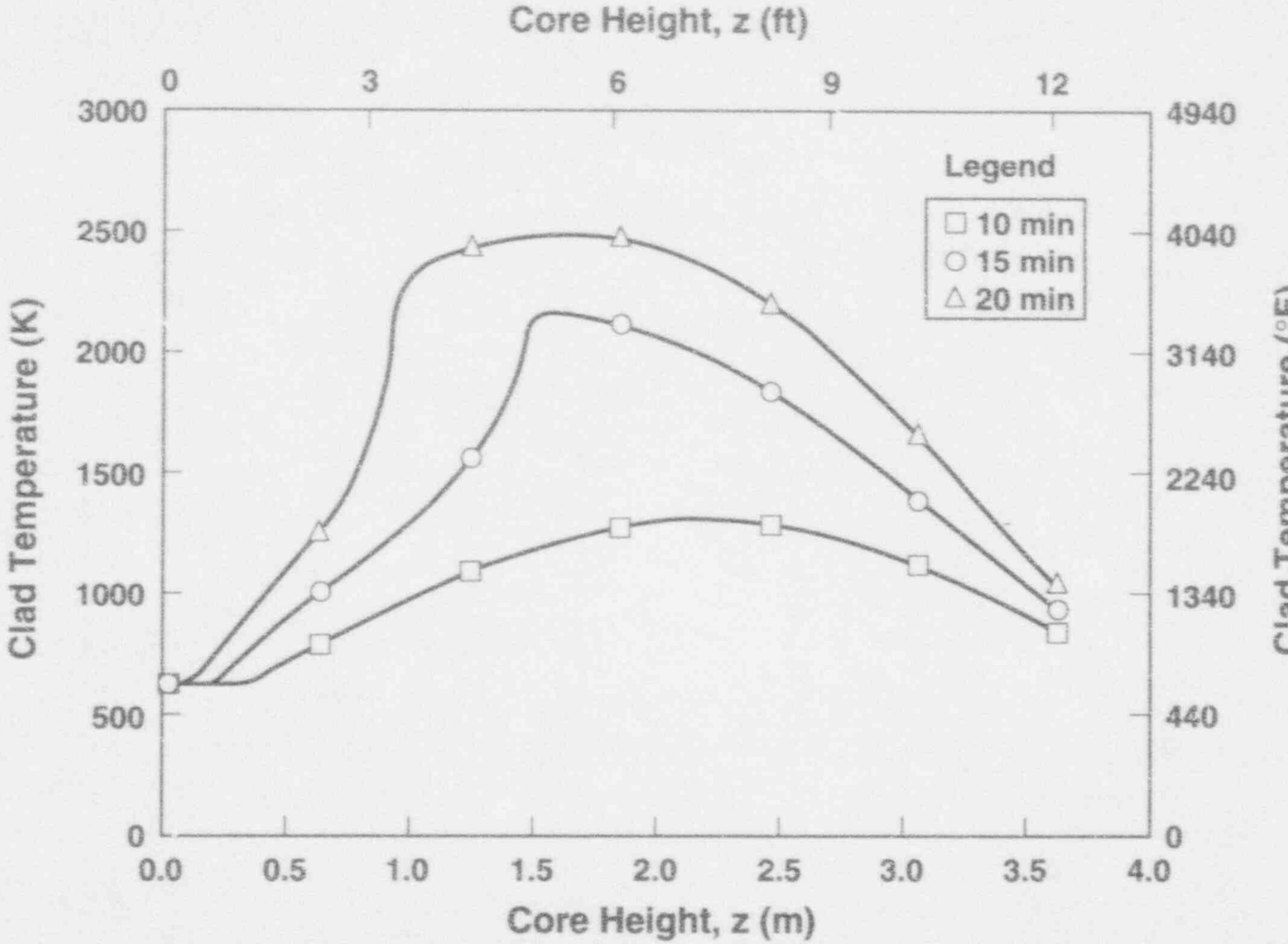


Figure 3.3-3 Calculated axial cladding temperatures at three different times following start of core uncovering for a PWR station blackout

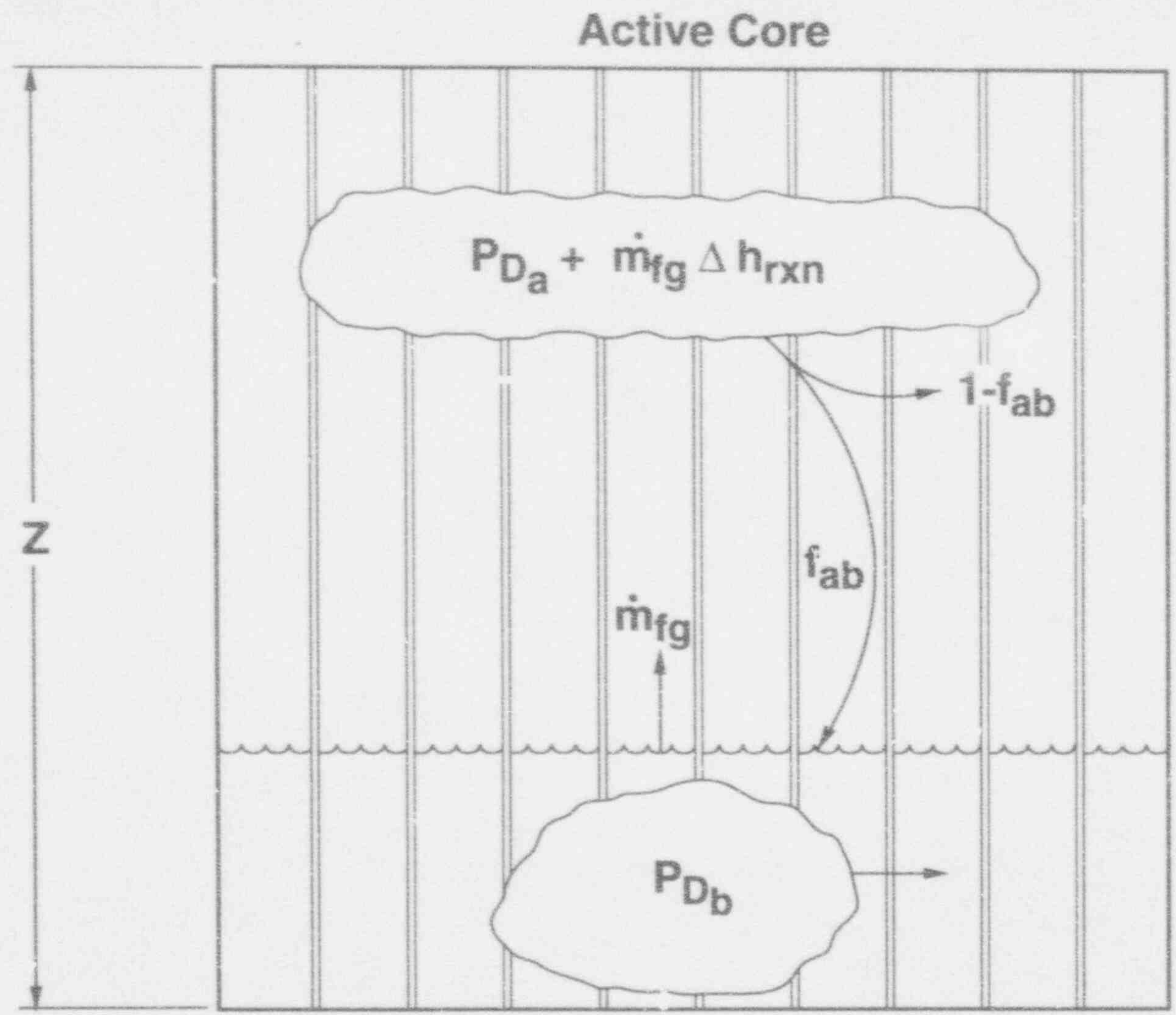


Figure 3.3-4 Heat balance between uncovered core and residual water

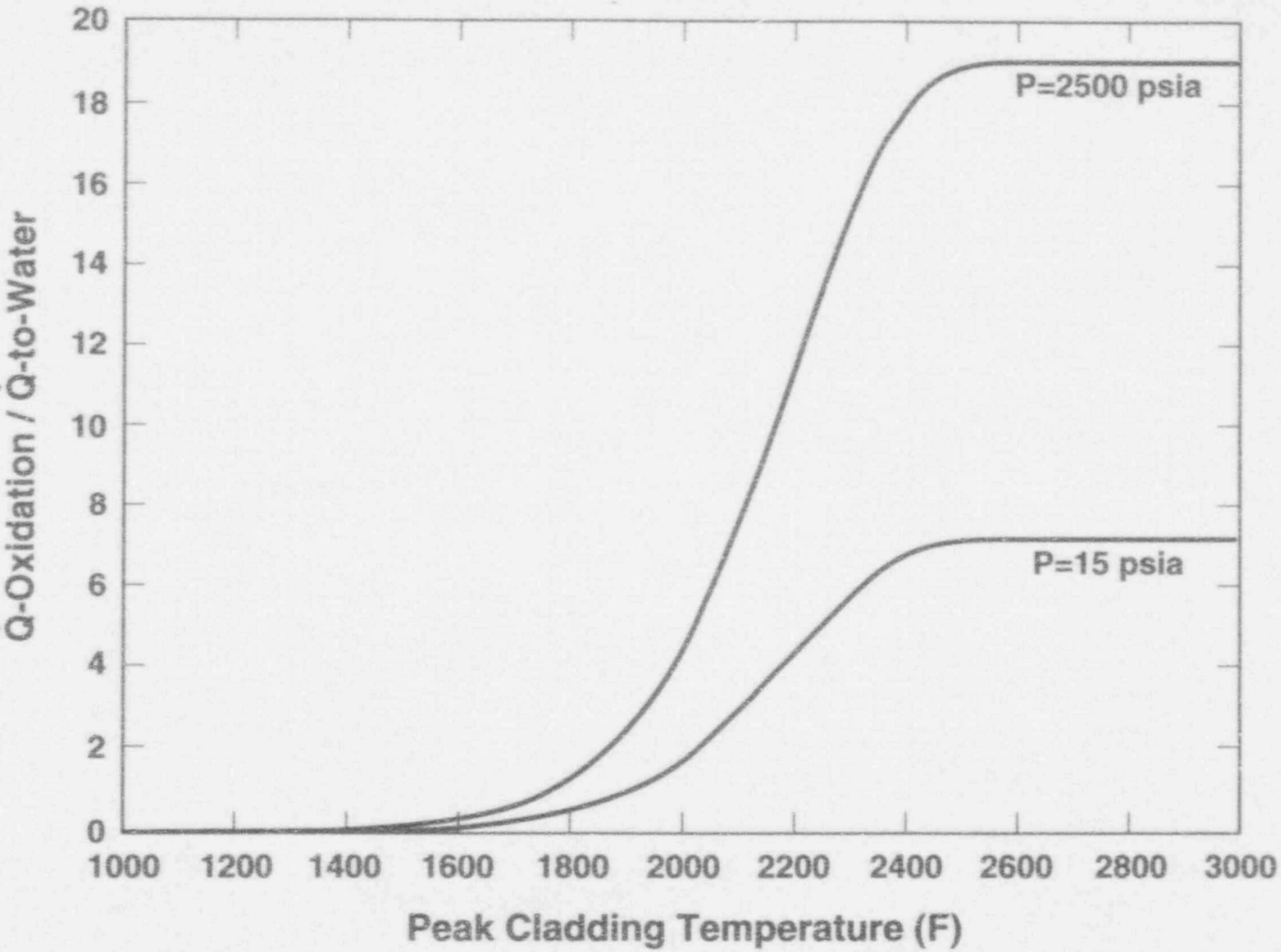


Figure 3.3-5 Ratio of heat release rate via oxidation to heat transfer rate to residual saturated water

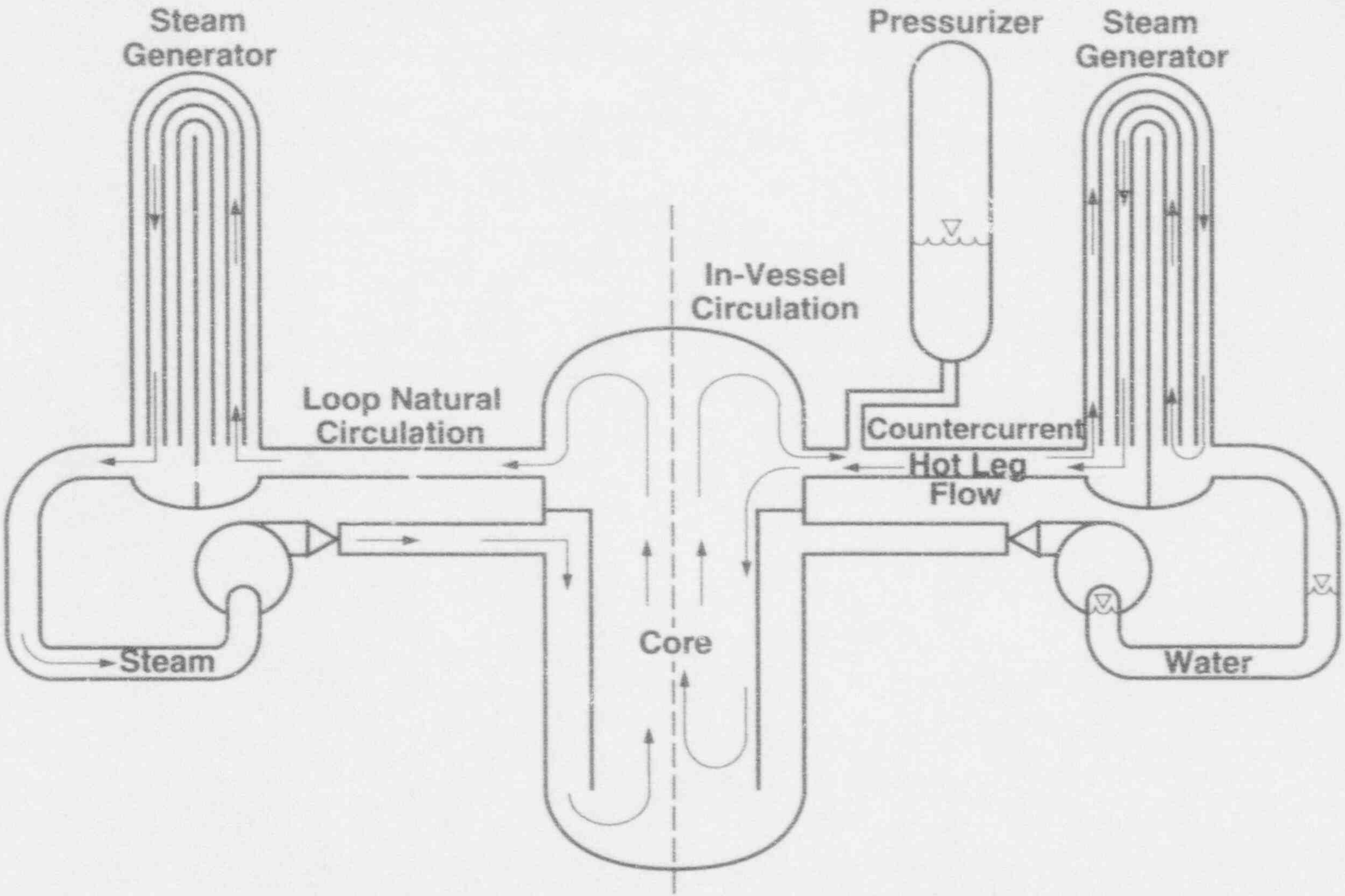


Figure 3.3-6 Severe accident natural circulation flows

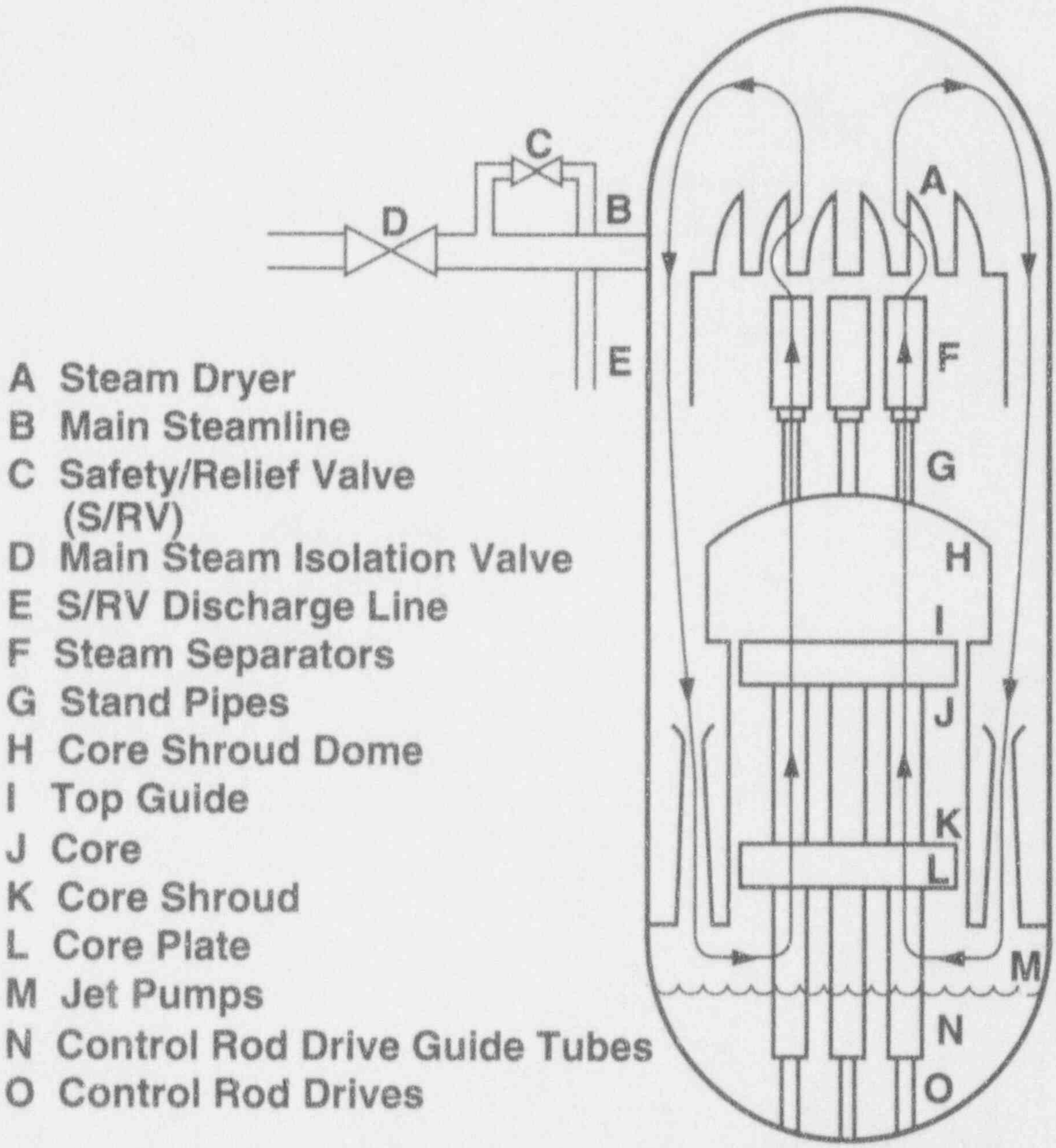


Figure 3.3-7 Schematic diagram of a BWR with internal circulation

References for Section 3.3

1. Baker, Jr., and R. O. Ivins, "Analyzing the Effects of a Zirconium-Water Reaction," Nucleonics, 23, 7, p. 70 (1965).

2. L. Baker, Jr. and L. C. Just, "Studies of Metal-Water Reactions at High Temperatures III, ANL-6548, Argonne National Laboratory, Argonne, IL (1962).

3. J. V. Cathcart, et al, Zirconium Metal-Water Oxidation Kinetics IV, Reaction Rate Studies, ORNL/NUREG-17, Oak Ridge National Laboratory, Oak Ridge, TN (August 1977).

4. V. F. Urbanic and T. R. Heidrick, "High Temperature Oxidation of Zircaloy-2 and Zircaloy-4 in Steam," J Nucl Materials, 75(2):251-61, 1978.

5. F. Briscoe, J. B. Rivard, and M. F. Young, "Fuel Rod Temperature Transients During LWR Degraded Core Accidents," Proceedings, International Meeting on Thermal Nuclear Reactor Safety, USNRC Conference Proceeding NUREG/CP-0027, Chicago, IL, (August 29 - September 2, 1982).

6. R. H. Chapman et al, "Zircaloy Cladding Deformation in a Steam Environment with Transient Heating," pp. 393-408 in Zirconium in the Nuclear Industry (Fourth Conference), ASTM STP 681, American Society for Testing and Materials, Philadelphia, PA (1979).

7. J. B. Rivard et al, Identification of Severe Accident Uncertainties, NUREG/CR-3440, SAND83-1689, Sandia National Laboratories, Albuquerque, NM, p. 3-8 (September 1979).

V. E. Denny and B. R. Sehgal, "Analytic Prediction of Core Heatup Liquefaction/Slumping," (Proc. Int. Mtg. on LWR Severe Accident Evaluation, Cambridge, MA, p5.4-1, 1983.

F. T. Harper et al, Evaluation of Severe Accident Risks: Quantification of Major Input Parameters, NUREG/CR-4551, SAND86-1309, Vol. 2, Rev. 1, Part 1, Issue 1 (December 1990).

3.4 Melting, Liquefaction, Holdup

3.4.1 Initial Melting

Stage 4 begins with the initial downward relocation of molten cladding material in the core region. As indicated in Section 3.2, the local decay-heat generation rate determines how rapidly a given uncovered region of the core would heat up. The decay-heat generation rate is proportional to the thermal power during operation. The thermal power distribution can therefore be used to provide a rough idea of the core regions most susceptible to the onset of rapid oxidation and subsequent melting. Figure 3.4-1 shows the power distribution in the TMI-2 core prior to the 1979 accident.[1,2] Less than half of the core by volume produces power at 25 kW/m or greater. Heat generation rates at the periphery of the core are markedly lower. This suggests that initial melting would occur first near the center of the core and might be restricted to the central region of the core. Some of the outermost fuel rods may not attain temperatures resulting in severe damage because of their low power levels and their location adjacent to surrounding structures. The degree of coherency in core damage affects both the course of the accident and the rate of release of fission products and aerosols from the core.

The melt temperature of zircaloy is 3350°F (1843°C = 2116 K);* however, the onset of Stage 4 may occur at lower temperatures if the core contains significant quantities of other metals with low melt temperatures. At TMI-2, a Ni-Zr eutectic was probably the first liquid formed as a result of interactions between the Inconel grid spacers and zircaloy cladding near the center of the core. The TMI-2 stainless steel control rod cladding melted at approximately 2600°F (1973°C = 1700 K) releasing molten Ag-In-Cd control material (melting point 1520°F = 1373°C = 1100 K) and allowing it to flow to the liquid steam interface with the Ni-Zr eutectic. Molten silver and iron form relatively low-temperature eutectics with zircaloy. Thus, the initial molten mixture probably contained significant zirconium upon reaching the steam/liquid interface. At the interface, the mixture froze to form a lower crust that blocked coolant channels between fuel rods. The postulated condition of the TMI-2 core shortly after the onset of Stage 4 (150 to 160 min into the accident) is shown in Figure 3.4-2.[3] Analyses indicate that the TMI-2 lower crust was a Zr-Ag-In-Fe-Ni metallic mixture surrounding standing columns of fuel pellets.

Stage 4 extends to the time that core material enters the lower plenum of the reactor vessel. Fuel damage during Stage 4 is extensive. It is driven both by decay power and by oxidation power. There is a strong forward coupling between fuel damage during this stage and the release, chemistry, and transport of fission products within the reactor coolant system.

3.4.2 Fuel Liquefaction

Early views of LWR core melt progression reflected in the 1975 Reactor Safety Study held that fuel melting did not occur until the UO_2 fuel material attained its melting temperature, 5180°F (2860°C = 3133 K). Research subsequent to the 1979 TMI-2 accident has demonstrated that UO_2 can be liquified far below its ceramic phase melting temperature. When the local temperature of the fuel reaches the zircaloy melting temperature, 3350°F (1843°C = 2116 K), flow of metallic cladding beneath the oxidized layer can occur. Interactions can then occur between molten zircaloy and solid UO_2 as indicated in Figure

*3. Core Meltdown Experimental Review, SAND74-0382, 1989, page 11-35.

3.4-3. In one series of laboratory experiments, UO_2 crucibles holding molten zircaloy at temperatures between 3272°F (1800°C = 2073 K) and 3632°F (2000°C = 2273 K) in an argon atmosphere were rapidly destroyed by the dissolution of solid UO_2 in molten zircaloy.[4] In another experiment, electrically-heated fuel-rod simulants in steam were massively liquefied and relocated when the oxidation-driven 9-rod-bundle temperature exceeded 3632°F (2000°C).* Similar behavior has been reported in several other experiments.

Apparently, zirconium reduces UO_2 preferentially along UO_2 grain boundaries near the UO_2-zircaloy interface. This produces a homogeneous U-Zr-O melt at low oxygen concentrations or a heterogeneous U-Zr-O melt containing UO_2 particles at high oxygen concentrations. In either case, the process is called fuel liquefaction.

In addition to destroying the UO_2 matrix, fuel liquefaction accelerates the release of fission products from the fuel.[5] However, minor alloying components or impurities can have large effects on such releases. For instance, tin, which is a 1% component of zircaloy, may act as a getter for tellurium resulting in significant holdup or retention of this fission product. Both fuel liquefaction and retention of tellurium in the presence of tin illustrate that chemical reactions are crucial to the understanding of severe accidents.

* S. J. Hagen, KfK/IT, private communication with J. B. Rivard regarding Experiment ESBU-1, July, 1982.

3.4.3 Flow Blockage Versus Streaming

The significant liquefaction of fuel that would occur at local temperatures between 3350°F (1843°C = 2116 K) and 3812°F (2100°C = 2373 K) would result in downward flow of liquid U-Zr-O. Even in the absence of a blockage formed by the refreezing of lower melting temperature eutectics (as occurred at TMI-2), molten U-Zr-O could refreeze on the surfaces of fuel rods or fuel assembly rod spacers in lower regions of the core where temperatures were cooler (Figures 3.4-4 through 3.4-10). Calculations indicate that, without additional oxidation, the liquefied fuel would rapidly freeze producing a significant core blockage. This is true even if freezing requires the transfer of the full UO_2 latent heat of fusion (270 kJ/kg). A latent heat of fusion more appropriate for the U-Zr-O mixture would require less heat transfer (about 50 kJ/kg)[5] making freezing even more likely.

On the other hand, the high temperature of the liquified U-Zr-O would favor high oxidation rates per unit area exposed, and energy addition by oxidation as the liquid flowed downward could preclude its refreezing. If the water level during the meltdown were below the bottom of the active core, the melt would stream into the lower plenum if not halted by freezing on cooler surfaces in the lower core regions. Quenching of melt that streamed into residual water in the lower plenum could provide the additional steam required to maintain the streaming process. The question of blockage versus streaming is important because it affects the magnitude of resulting melt-water interactions and the timing and mode of eventual bottom head failure (Section 3.5). Most current analyses predict the formation of a blockage in the core region even if the residual water level is below the bottom of the active fuel.

A central blockage would redirect steam flow outward in an open lattice (PWR) core. This is depicted in Figures 3.4-4 and 3.4-5 for residual water levels in and below the active core region respectively. The diversion of steam flow to the outer regions of the core could result in two possible alternatives. If the fuel rods have not yet attained temperatures capable of supporting rapid oxidation, they may be cooled by the additional flow, but if the rods are hot enough, they may rapidly oxidize.

Figure 3.4-6 shows the core condition postulated at TMI-2 at 173 min, just prior to the brief restart of reactor coolant pump 2B.[4] The process of zircaloy oxidation, melting of core metallic components, UO_2 dissolution, and relocation of molten material downward to freeze and block coolant flow channels at or near the steam/liquid interface is postulated to have progressed to the point where the blockage was nearly complete with only the outermost fuel assemblies undamaged. The bowl-like shape of the lower crust or crucible may have been caused by the flow blockage diverting steam flow to the core periphery. Steam diversion to the core periphery increases steam flow rates and thus heat transfer at the periphery of the damage zone. This results in freezing the downward relocating melt at elevations above the water level as shown in Figure 3.4-6. A second explanation for the shape of the lower crust is that core temperatures near the core periphery were primarily controlled by decay heat. Thus, the freezing isotherm for the molten metallics would increase in elevation as core damage progressed radially outward into the lower power regions of the core.

Above the lower crust, a region of at least partially molten metallics and ceramics would form as depicted in Figure 3.4-6 for TMI-2. At the time indicated (just prior to the restart of reactor coolant pump 2B) core heatup calculations indicate that peak temperatures within this region of consolidated core materials may have reached fuel melting (5180°F = 2860°C = 3133 K). The average temperature of the material was probably between 4220°F (2873°C = 2600 K) and 4580°F (3073°C = 2800 K).

Undamaged rod stubs below the bottom crust at TMI-2 indicate that coolant levels were held 20 inches (0.5 m) or more above the bottom of the active core at TMI-2. Water covering the bottom of the core assured that the lower supporting crust was cooled. This almost certainly helped maintain the structural stability of the crust.

3.4.4 Quenching During Stage 4 at TMI-2

To this point scenarios in which there is no injection of core coolant have been discussed before considering alternatives (such as TMI-2) which involve partial injection and reflooding. It is convenient at this point, however, to complete the discussion of Stage 4 events at TMI-2. The differences that could arise in other core melt accidents are discussed in the Sections 3.4.5 through 3.4.7.

Activation of reactor coolant pump 2B at ~174 min resulted in the first significant addition of coolant to the TMI-2 reactor vessel following the shutdown of the loop A reactor coolant pumps at ~100 min. Reactor coolant pump 2B operated for ~19 min; however, significant flow in the loop B hotleg was only measured during the first 15 s. Approximately 1000 ft^3 (28 m^3) of water was pumped into the reactor vessel from the loop B cold leg.

As discussed in Section 2.4, the reactor coolant pressure increased rapidly when pump 2B was turned on. This pressure increase was caused by steam generated when the water contacted hot surfaces in the core region, and by hydrogen generated by the rapid oxidation of metallic zircaloy in the top half of the core. The hydrogen also degraded the limited heat transfer that was occurring in the loop B steam generator.

The thermal-mechanical forces resulting from partial quenching of the oxidized fuel rod remnants in the top half of the core fragmented the oxidized cladding and fuel pellets to form a debris bed. The configuration postulated for the core just after the pump 2B restart is shown in Figure 3.4-7. As indicated in the figure, the upper support grid was damaged. Selected areas of the bottom of the upper grid were oxidized, melted, or ablated thermally. There was, however, no damage to the upper plenum structures above the core. Thus, stored energy of the core was not efficiently transferred to the upper plenum structures.

From ~180 min to ~200 min, the TMI-2 core liquid level decreased as decay heat from the degraded core boiled liquid from the reactor vessel. The liquid level at ~200 min stood 79 inches (2 m) above the bottom of the active core. The low thermal diffusivity of the large consolidated region of primarily ceramic core debris above the bottom crust prevented the interior of this region from cooling even when the reactor vessel was subsequently filled with water. Calculations indicate that a pool of molten material formed in the center of the consolidated region and increased in size during this period.

At 200 minutes the high pressure injection system was actuated and cooling water was injected for the next 17 minutes. Analyses indicate that the core region was refilled with water by 207 min. As the cooling water filled the reactor vessel, water began to penetrate the debris bed above the consolidated region. By about 230 min debris in this bed was fully quenched. The consolidated region continued to heat up even though the core region was filled with water. The postulated condition of the core debris at 224 min is depicted in Figure 3.4-8. Water covered the core region, and the debris bed above the core region was quenched, but most of the consolidated region between the upper and lower crusts was predominately molten.

Relocation of approximately 20 tonnes of molten core material into the lower plenum of the reactor vessel occurred at approximately 224 min. This is confirmed by increases in the reactor coolant pressure and temperatures and by changes in the out-of-core source range neutron detector readings. Rapid steam production occurred in the lower plenum as a result of heat transfer from the molten core material to water in the bottom head. Nothing in the recorded data or post accident core conditions suggests an energetic steam explosion (see Section 3.5) occurred as the tons of molten core material relocated into the lower plenum with the reactor vessel nearly full of water.

The hypothesized configuration during relocation is depicted in Figure 3.4-9. The crust failure appears to have been in the upper half of the consolidated region near the core periphery. Material apparently flowed downward into the lower plenum through both the upper core support assembly and the peripheral fuel assemblies. Two mechanisms have been postulated for crust failure. First, continued heating of the molten pool could have led to melting of the supporting crust, which was thinnest on the top (1 cm versus ~6 cm on the bottom) where heat transfer was greater. Second, at ~220 minutes the pressurizer block valve was opened resulting in a decrease in the reactor coolant pressure of 70 psi (0.5 MPa) between 220 and 240 min.

The molten core material settled onto the reactor vessel bottom head and was not cooled significantly by water during the relocation. Thermal analyses indicated that lower-head temperatures exceeding 1520°F (1373°C = 1100 K) would have occurred if the molten material had settled onto the lower head as a cohesive, nonporous structure. The lower head would have failed due to creep rupture at such temperatures. Since this did not occur, the debris on the lower head must have had substantial porosity, which permitted more rapid quenching. The challenge to TMI-2 vessel integrity posed by local failures (e.g. meltthrough of in-core instrument penetrations) is still being studied.

3.4.5 Alternative for Melt Flow Scenarios

In core melt scenarios involving the formation of blockage in the core region, configurations similar to that at TMI-2 are postulated. The formation of a molten pool contained within a crucible-like bottom crust is envisioned with unmelted ceramic (UO_2) and metallic material either adding to the pool from above or forming a rubble bed above an upper crust as at TMI-2.

The size of the molten region would grow due to continued addition of decay heat (reduced by fission products lost during liquefaction). With a total loss of coolant injection, the residual water level could drop below the bottom of the active core and structures supporting the mass of the crust and melt could weaken as depicted in Figure 3.4-10. Given a failure of the core support structures or a breakthrough of suspended melt as occurred at TMI-2, substantial quantities of melt could suddenly plunge into the residual water in the lower plenum as occurred at TMI-2.

On the other hand, for the streaming scenario in which a crust does not form in the core region, the maximum liquid flow rate from a single PWR fuel assembly is about 940 kg/s.[6] Based on the above, melt might flow from the core region in three possible modes:

(1) In a narrow discontinuous stream, or streams, distributed over the duration of the core meltdown;

(2) In a narrow continuous pour over a period of fractions of minutes to several minutes; or

(3) In a relatively massive, coherent pour occupying a few seconds or less.

The third mode is likely to be broken up in BWRs by the massive BWR core supports and bottom-head-entry control rod drive housings.

The timing of discharge from the vessel is related to the three modes listed and to the level of damage achieved (fraction of core liquefied). This is true because the rate of formation of liquefied fuel is slow compared to all but the very slowest discharge rates. Thus, if a large fraction of the core is liquefied at the onset of discharge, a larger amount might be discharged. Conversely, if only a small fraction is liquefied at the onset of discharge, a smaller amount might be discharged (corresponding to mode 1 or 2 above).

3.4.6 Natural Circulation During Core Melting

In PWR accidents, even if the steam generator secondary-side inventory is depleted at the time of core damage, gaseous natural convection between the vessel and the primary side of U-tube steam generators is favored. Because of potential loop seal and downcomer blockage, the convection would most likely be required to traverse the hot leg piping, displacing cooler steam/hydrogen in the generator tubes by warmer steam-hydrogen from the core, Figure 3.3-6. The great height of the steam generator tubes (18 m) provides a large driving force.

To the extent that the convection is effective, it will provide a sink for fission products. Based on a 3260-tube generator with 18 m of upflow, the 22-mm-tube diameter with 1-mm wall, the generators in the Surry plant, for example, contain about 1.3 x 10^5 kg of "effective" steel. Assuming that the total Cs + Te + I core inventory is uniformly deposited throughout the tubes, the heat flux resulting from the deposited fission products would be approximately 0.5 KW/m^2. In the absence of water on the secondary side, this heat flux would result in a steady increase in the temperature of the steam generator tubes. The lumped tube heating rates corresponding to a 0.5 kW/m^2 deposited heat flux would be about 0.18°F/s (0.1 K/s). This overestimates the heating effect because heat would be lost by thermal radiation and convective heat transfer to cooler components, and by gamma rays not captured within the tube walls. Nevertheless, the effectiveness of the steam generators as a heat sink would decrease strongly as the tubes heat up. It has been estimated that halving the ΔT between hot gases and steam generator tubes reduces the convective heat flux by 40%.[6]

Thus, given dry steam generators (anticipated for transient-initiated accidents), effective natural convection would be inhibited when structures acting as heat sinks attained elevated temperatures. On the other hand, as discussed in Section 3.3.5, because the strength of steel decreases rapidly above 1832°F (1000°C), reactor coolant system structures such as the hot legs could weaken and fail at sufficiently elevated temperatures. Such temperature-induced boundary failures would depressurize the reactor coolant system and preclude large containment pressures and temperatures that might otherwise result from high-pressure melt ejection due to reactor vessel bottom head failure (Section 3.5.2.5 and Module 4).

3.4.7 Reflood During Stage 4

As explained for Stage 3 in Section 3.3.4 and for TMI-2 in Section 3.4.4, if water is reintroduced into the core during Stage 4, acceleration of cladding oxidation may occur, because

- the quantity of unoxidized cladding may be relatively large due to the slow rate of steam evolution from boiloff prior to reflooding,
- a large fraction of the unoxidized cladding could have achieved elevated temperatures,
- quenching of hot fuel upon reflooding the lower part of the core would produce copious amounts of additional steam, and
- there could be relatively uninhibited access of steam to unoxidized cladding.

Acceleration of oxidation associated with reintroduced coolant might, given these assumptions, add tens of gigajoules (GJ) of energy to the system in a short time and evolve large quantities of hydrogen, because of the rapid oxidation kinetics at temperatures characteristic of Stage 4, and the modest energy used to increase the coolant temperature and vaporize it. Because the energy required to destroy the entire core geometry at these temperatures may be as little as 6 GJ,[6] a significant redistribution of core materials in a very short time following the reintroduction of water is possible.[6] An attendant possibility is one or more steam explosions caused when hot, liquified fuel falls into the pool of reflooding water. (Steam explosions are discussed in Subsection 3.5.) The actual scenario is quite uncertain, producing significant uncertainty in all subsequent events and processes that are affected.

If much of the steam generated is not reacted, the reintroduction of sufficient water should halt the heatup and result in a cooling of the core. This requires, in addition to the initial quench, either reestablished loop flow (forced or natural convection in the primary system) or local bed convection. Cooling by local convection in the bed, as well as by reestablished loop flow, depends upon the size and characteristics of the rubble and the coolant-volume fraction, and requires that a long-term heat sink be available for the energy removed from the bed. Rubble bed cooling is discussed further in Section 3.5.

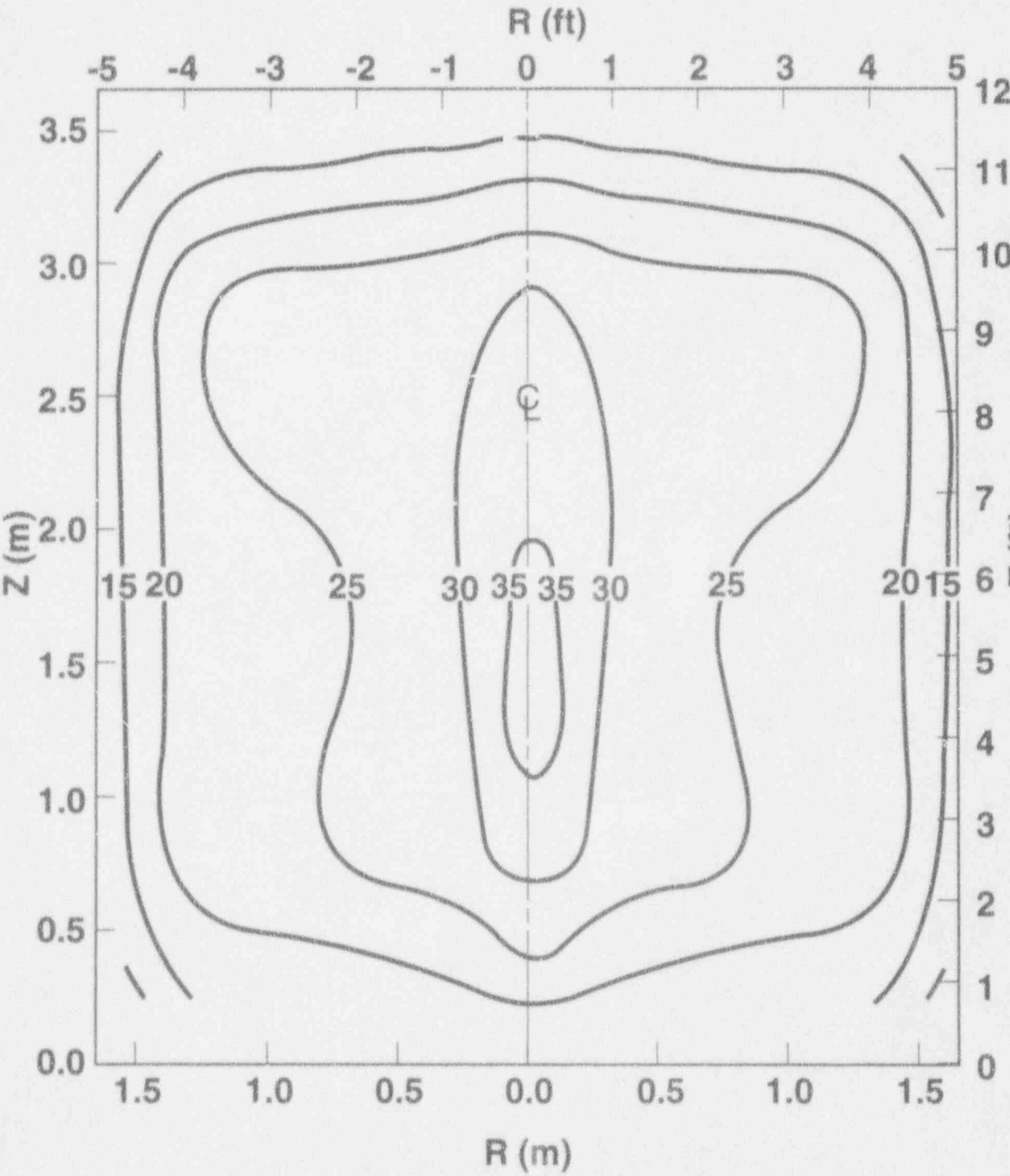
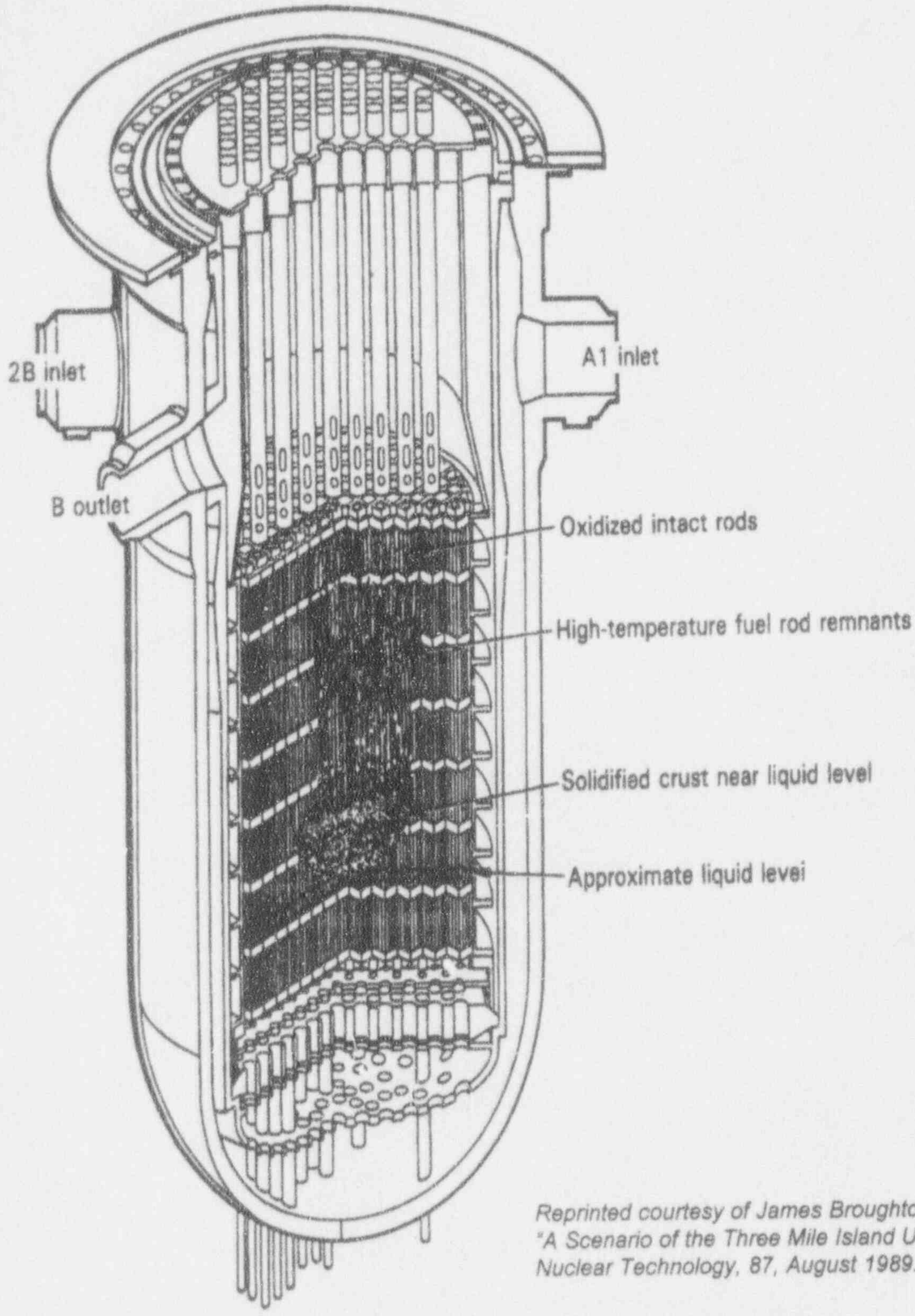


Figure 3.4-1 Distribution of fuel rod rating in kW/m in the TMI-2 core



Reprinted courtesy of James Broughton et al., "A Scenario of the Three Mile Island Unit 2 Accident," Nuclear Technology, 87, August 1989.

Figure 3.4-2 Hypothesized TMI-2 core condition between 150 and 160 min.

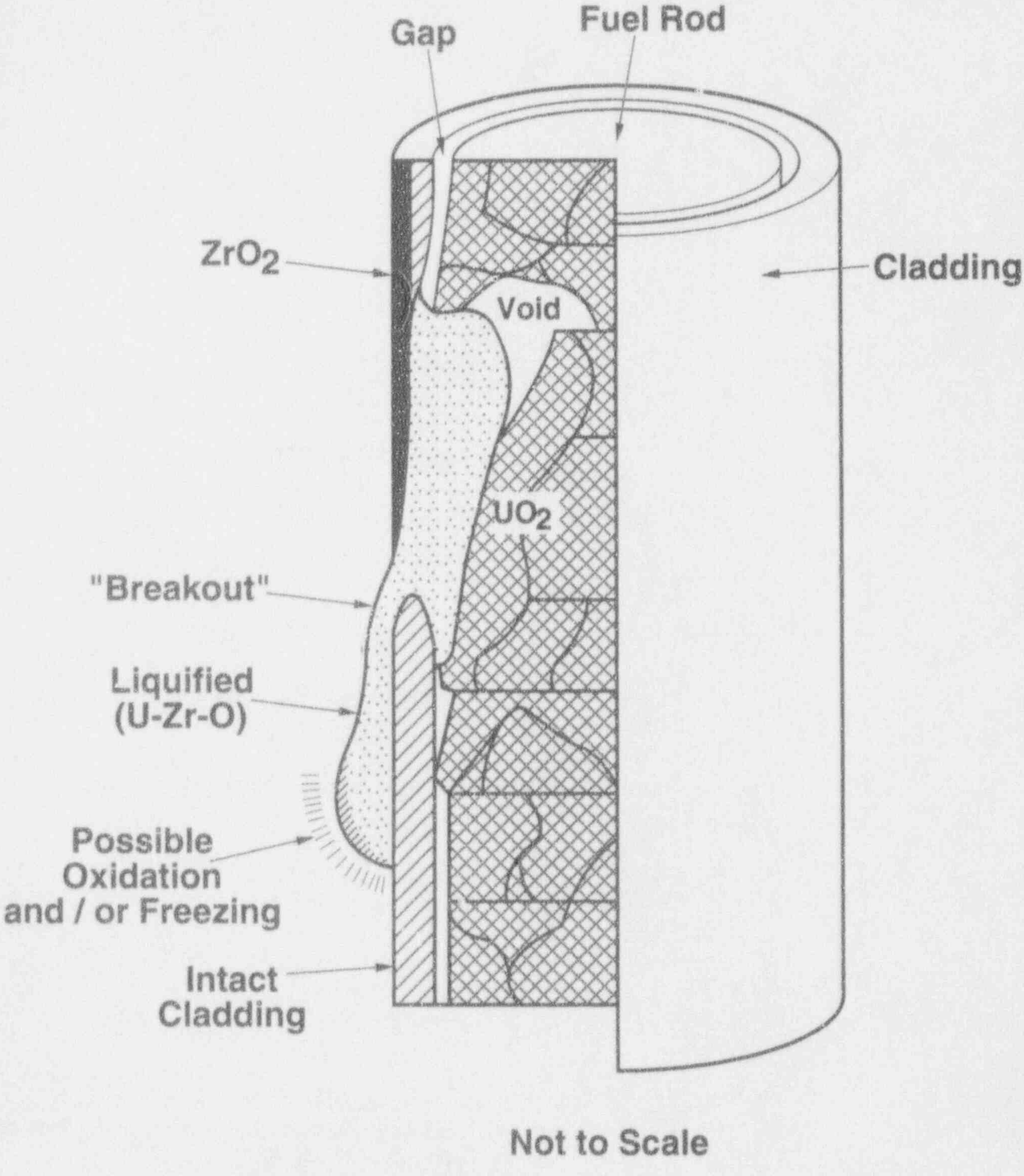


Figure 3.4-3 Schematic representation of possible mode of initial fuel liquefaction and downward flow

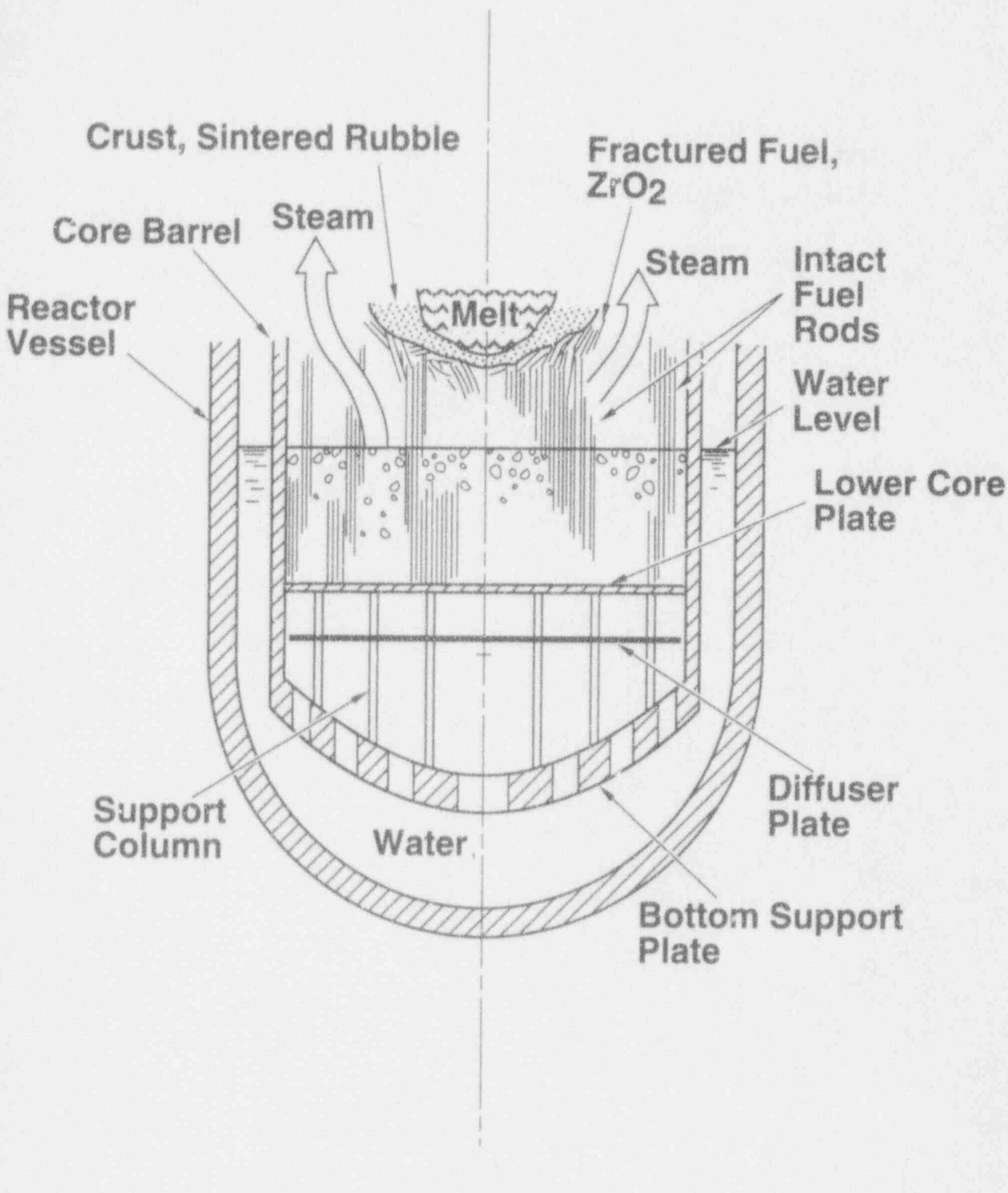


Figure 3.4-4 Initial core degradation in a PWR

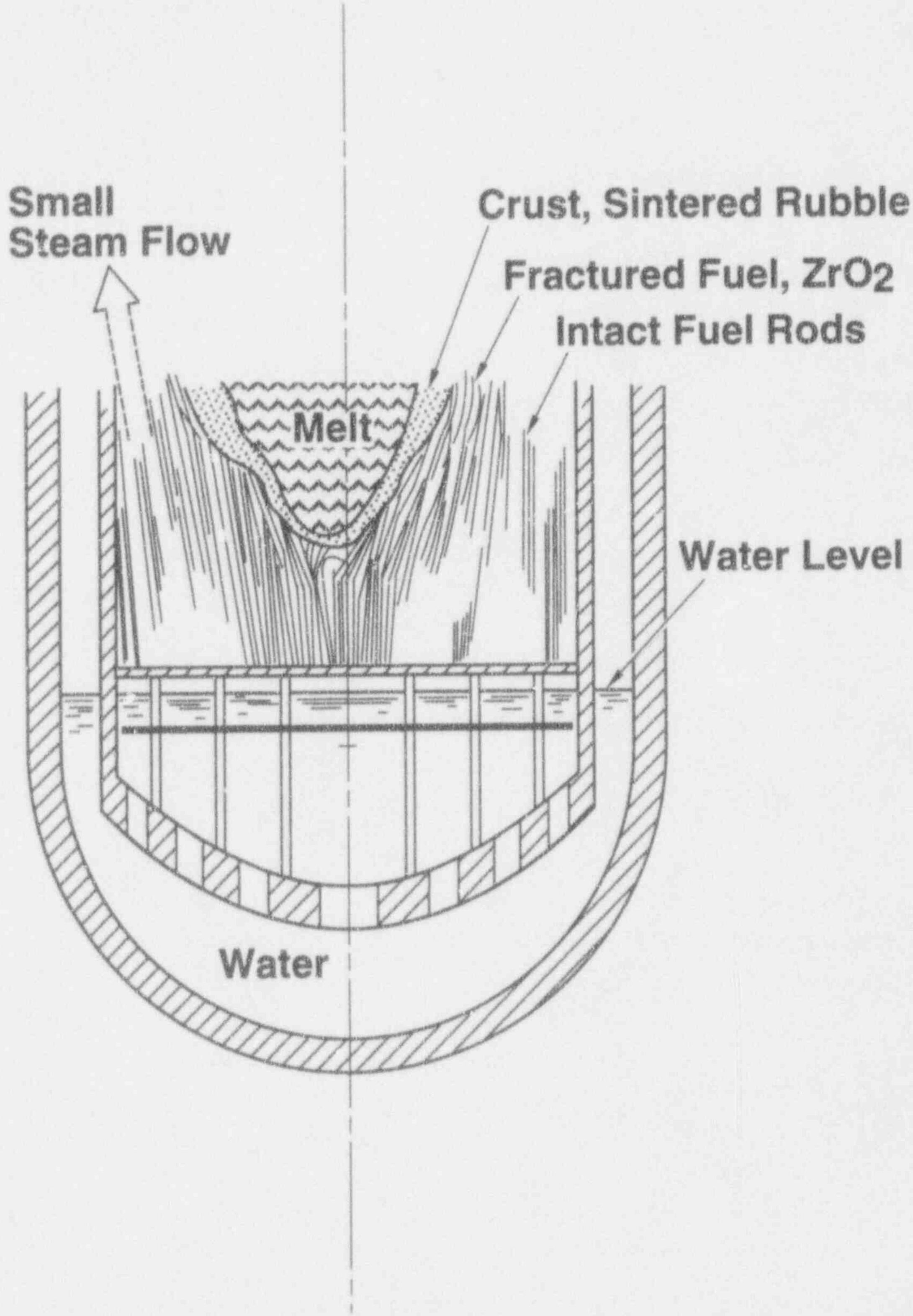
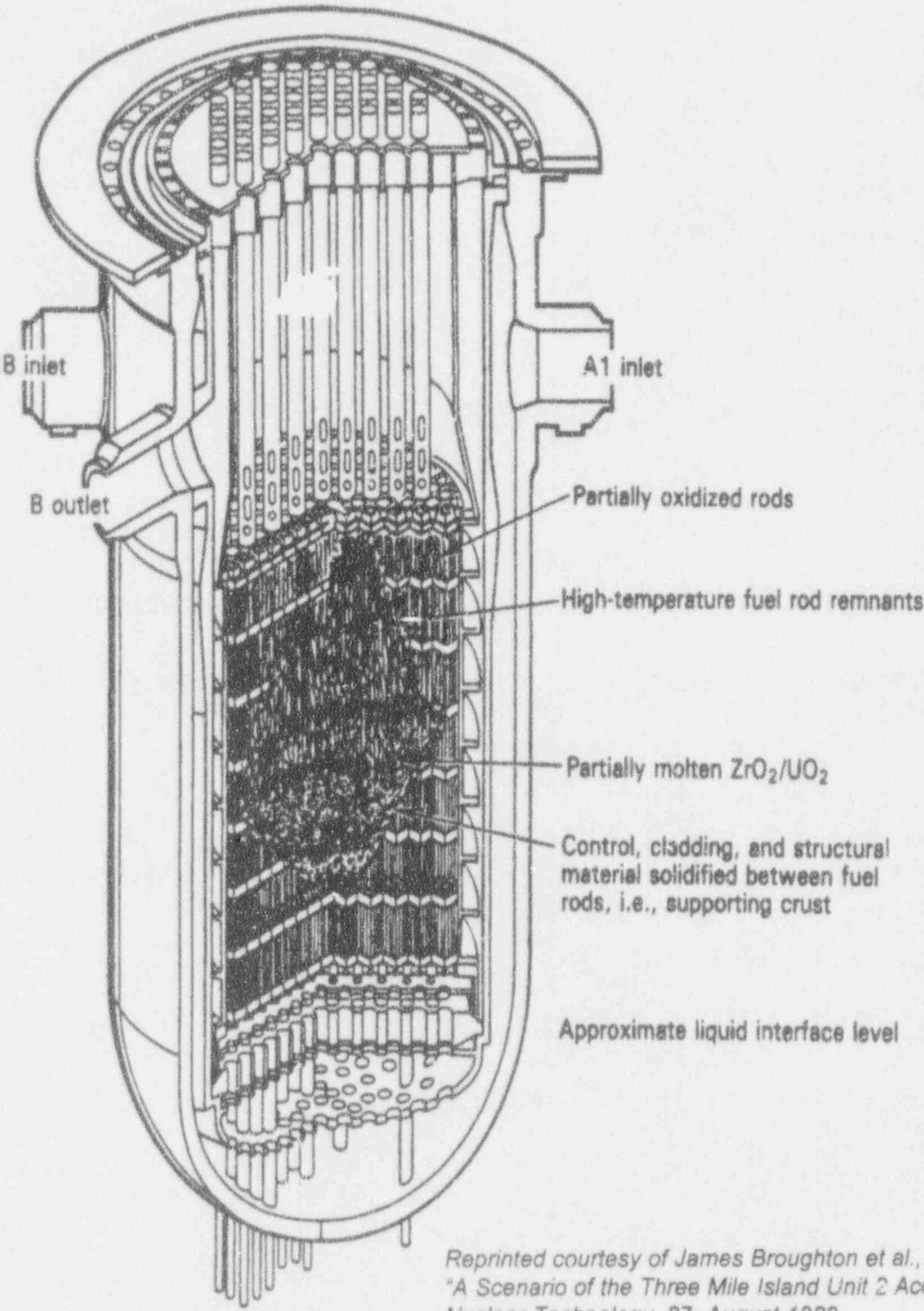
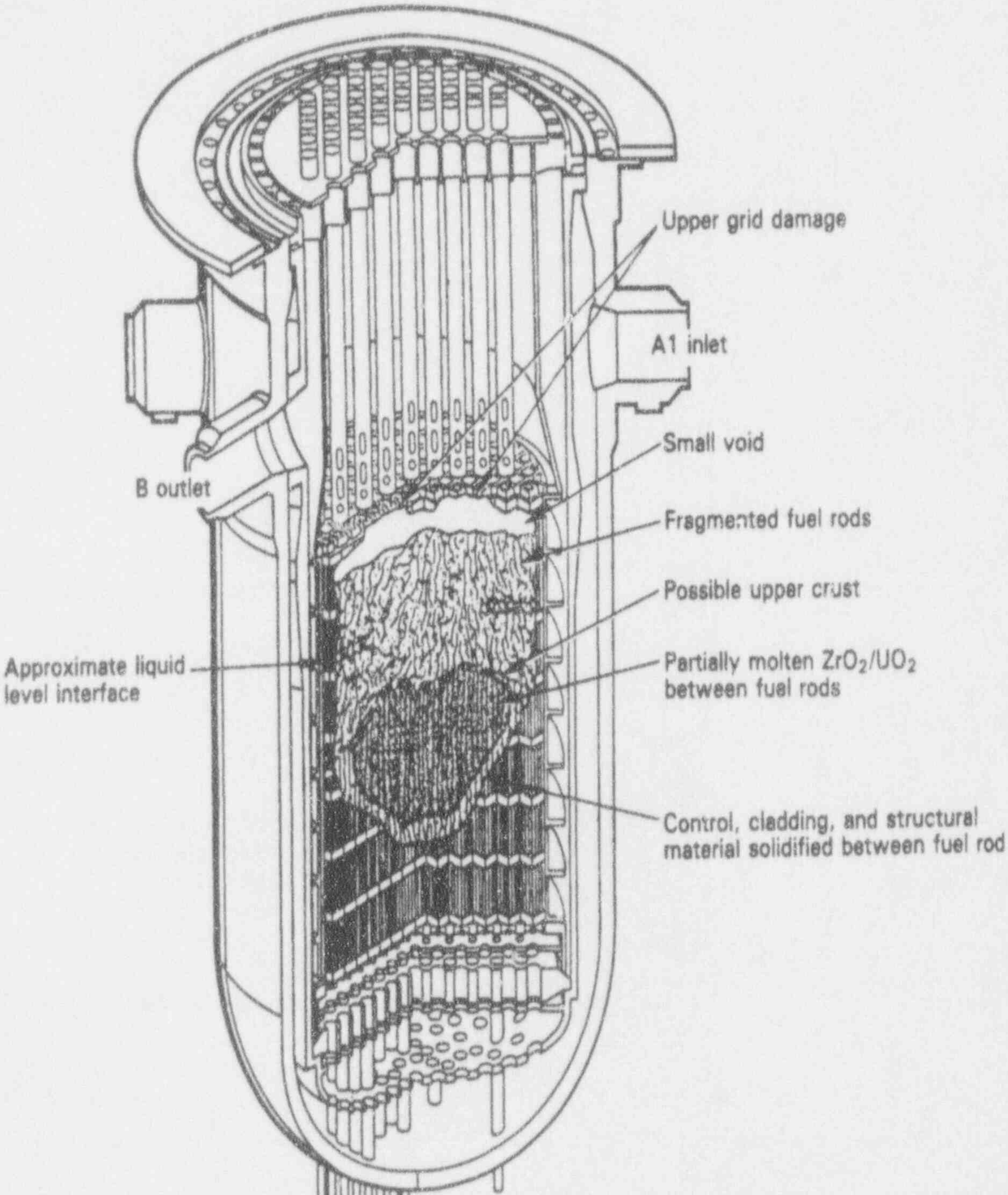


Figure 3.4-5 Structures and features of meltdown in a PWR



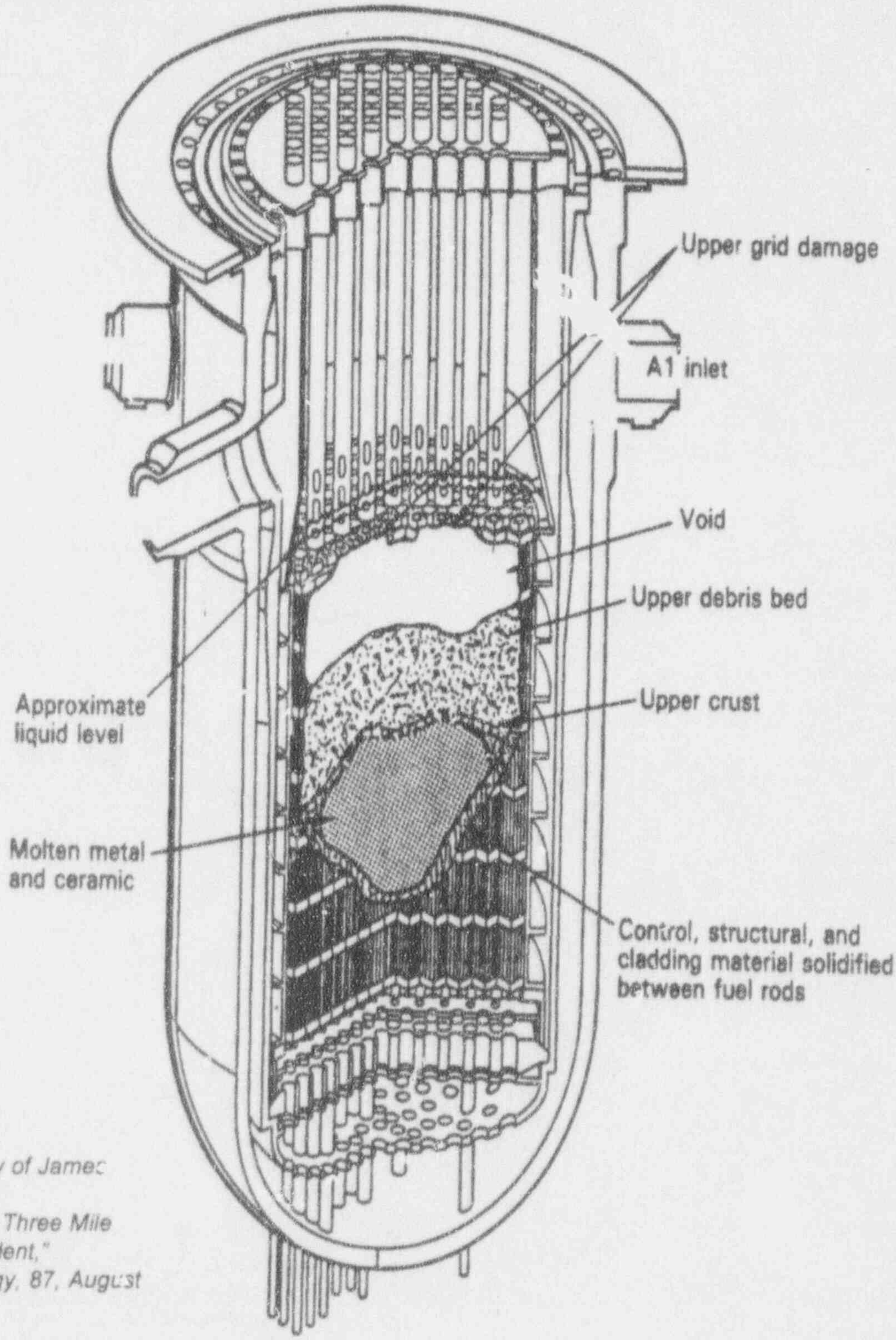
Reprinted courtesy of James Broughton et al., "A Scenario of the Three Mile Island Unit 2 Accident," Nuclear Technology, 87, August 1989.

Figure 3.4-6 Hypothesized TMI-2 core configuration at 173 min.



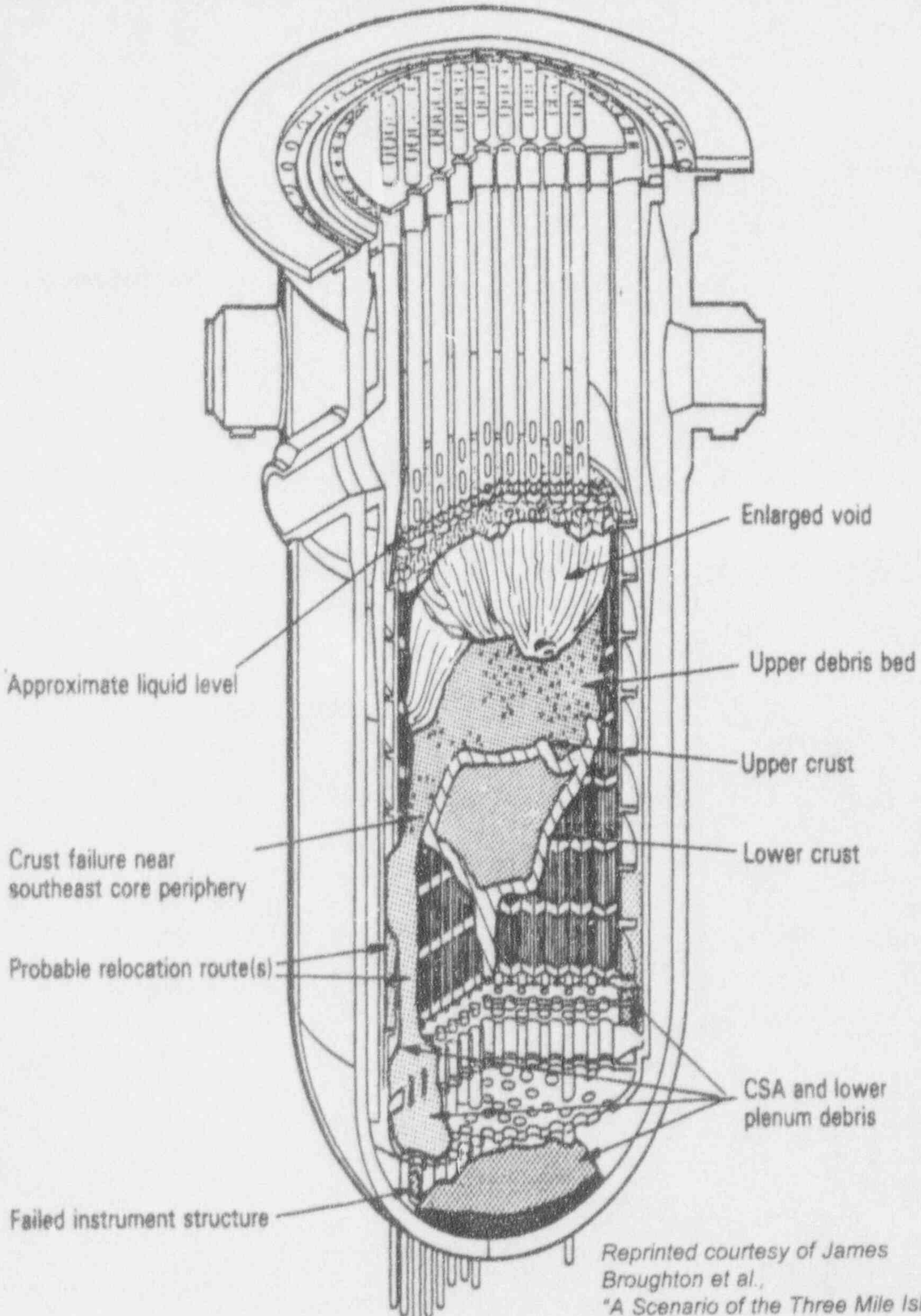
Reprinted courtesy of James Broughton et al., "A Scenario of the Three Mile Island Unit 2 Accident," Nuclear Technology, 87, August 1989.

Figure 3.4-7 Hypothesized TMI-2 configuration between 174 and 180 min.



Reprinted courtesy of James Broughton et al., "A Scenario of the Three Mile Island Unit 2 Accident," Nuclear Technology, 87, August 1989.

Figure 3.4-8 Hypothesized configuration of TMI-2 core at 224 min (just prior to major core relocation).



Reprinted courtesy of James Broughton et al., "A Scenario of the Three Mile Island Unit 2 Accident," Nuclear Technology, 87, August 1989.

Figure 3.4-9 Hypothesized TMI-2 core configuration during relocation.

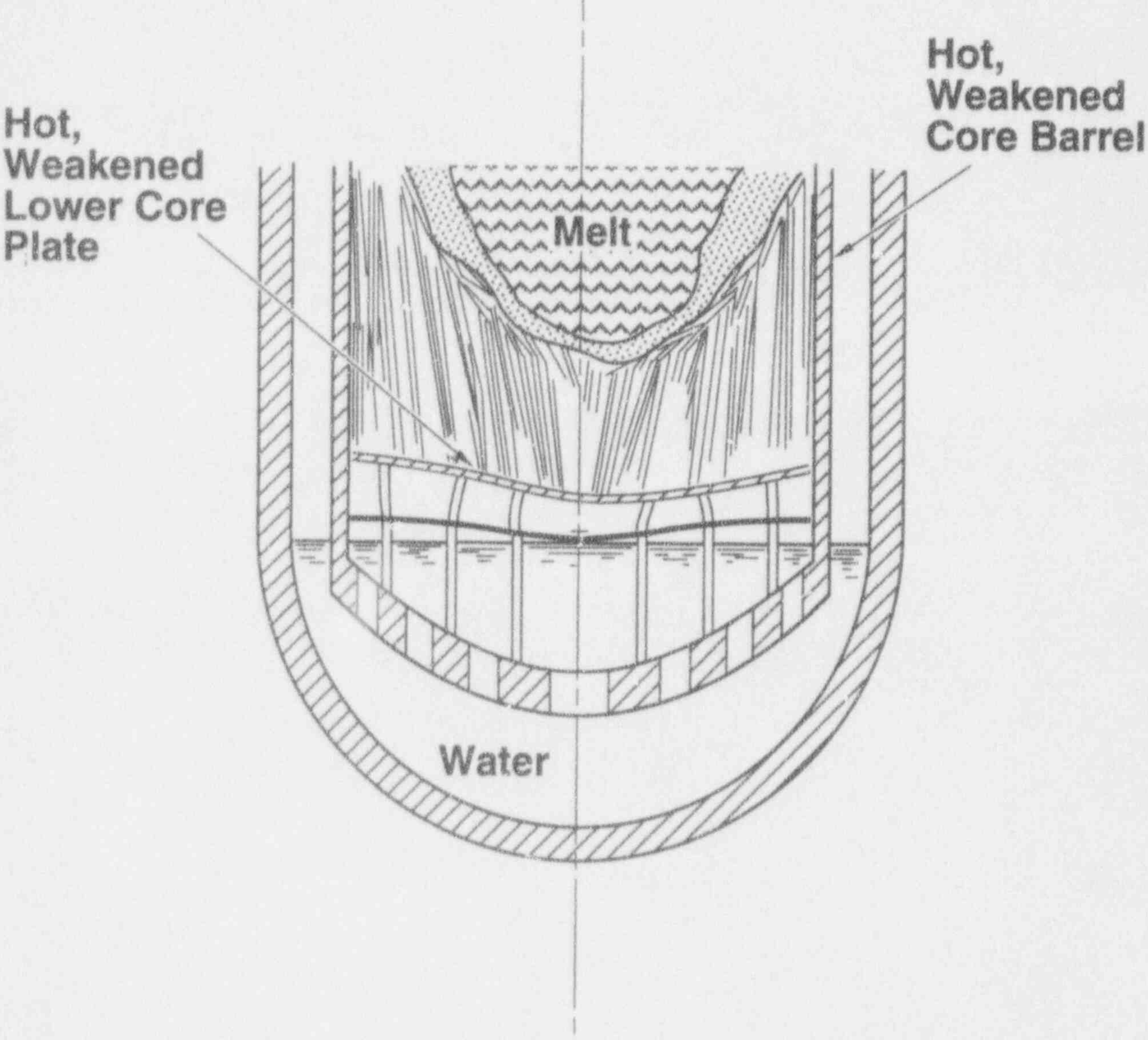


Figure 3.4-10 Visualization of the downward progress of a coherent molten mass as the below-core structures weaken

REFERENCES FOR SECTION 3.4

1. K. H. Ardron and D. G. Cain, TMI-2 Accident Core Heat-Up Analysis, NSAC-24, Electric Power Research Institute, Palo Alto, CA, 1981.

2. K. H. Ardron and D. G. Cain, "Core Temperature Transient in the Early Phase of Core Uncovering at TMI-2," Progress in Nuclear Energy 7:197-228, 1981.

3. J. M. Broughton et al, "A Scenario of the Three Mile Island Unit 2 Accident, *Nuclear Technology*, Vol. 87, August 1989.

4. P. Hofmann, D. Gerwin Peck, and P. Nikolopoulos, Physical and Chemical Phenomena Associated with the Dissolution of Solid UO_2 by Molten Zircaloy-4, 06.01.06p10c, PNS-NR.675/82 (Karlsruhe, Federal Republic of Germany: Kernforschungszentrum Karlsruhe, GmbH, 1982).

5. J. B. Rivard, et al, Identification of Severe Accident Uncertainties, NUREG/CR-3440, SAND83-1689, p. 3-12, September, 1989.

6. K. Bracht, "Orienting Analysis on Core Melt Slump During A Core Meltdown Accident," Gesellschaft fur Reaktorsicherheit (GRS) mbH, GRS-A-490 (NRC Translation 1069), May 1982.

3.5 Core Slumping, Quenching, Reheating

Stage 5 begins as molten material flows out of the core region and into the lower plenum. It ends with the breach of the reactor vessel and the accompanying discharge of core materials into containment.

Based upon the Stage 4 description, the melt might flow from the core region in three possible modes:

1. in a narrow discontinuous stream, or streams, distributed over the duration of the core meltdown

2. in a narrow continuous pour over a period of fractions of minutes to several minutes, or

3. in a relatively massive, coherent pour occupying a few seconds or less.

The third mode is likely to be broken up in BWRs by the massive BWR core supports and bottom-head-entry control rod drive housings.

The rate of formation of liquefied fuel is slow compared to all but the very slowest discharge rates. Thus, if a large fraction of the core is liquified at the onset of discharge, a larger amount might be discharged; conversely, if only a small fraction is liquefied at the onset of discharge, a smaller amount might be discharged (corresponding to Mode 1 or 2 above).

If there is no residual water in the lower plenum, a possibility for some accident sequences, the melt would directly attack the lower head (see Section 3.5.2). However, the progression treated here postulates the more complex case in which residual water exists in the lower plenum.

3.5.1 Fuel-Coolant Interactions (FCIs)

When molten core material (fuel) comes into contact with liquid water (coolant), a variety of different fuel-coolant interactions (FCIs) can occur. The FCIs can range from quiescent boiling to explosive fragmentation of the fuel with rapid steam generation. An explosion caused by the rapid fragmentation of fuel and vaporization of water due to heat transfer from the fragmented fuel is called a steam explosion. If the hot liquid contains unoxidized metals, exothermic metal-water reactions can accompany the FCI, resulting in enhanced energy release and the generation of hydrogen. The nature of the FCI determines the rates of steam and hydrogen production and the potential for damaging the reactor vessel or containment building. Much theoretical and experimental research has been devoted to FCIs over the last three decades.[1,2] Although significant progress has been made, many questions remain unresolved.

3.5.1.1 Steam Explosions

Steam explosions occur when heat is transferred from the melt to water on a very short time scale (approximately 1 ms). Steam explosions have occurred ever since man began to work with molten metals. The first known written record of such an explosion appears in the Canterbury Tales of the 14th century.[3] Destructive steam explosions have occurred in aluminum, steel, and copper foundries; arc-melting facilities; paper mills; granulation plants; and Chernobyl.[4,5,6,7,8]

The four major stages of a steam explosion are:

1. Initial *coarse mixing* of melt and water during which heat transfer is generally characterized by stable film boiling (Figure 3.5-1).

2. A *triggering* event that causes local destabilization of film boiling and local fragmentation of melt into small drops, on the order of 0.01 to 0.1 mm in diameter.

3. *Propagation* of the region of rapid heat transfer through the coarse mixture, and

4. Explosive *expansion* driven by steam at high pressure.

In the absence of a triggering event, a nonexplosive FCI would occur. Coarse mixing would result in some quenching of the melt with associated steam and hydrogen production.

3.5.1.2 Conditions Affecting Steam Explosions

The probability and magnitude of steam explosions depend on various initial and boundary conditions including:

- mass, composition, and temperature of the molten material
- water mass, depth, and temperature
- vessel geometry, degree of confinement, and the presence and nature of flow restrictions and other structures,
- fuel-coolant contact mode, in particular, for melts poured into water, the melt entry velocity and pour diameter,
- the ambient pressure,
- the timing and strength of any externally applied trigger (in an experiment, not postulated for reactor accidents).

Intermediate conditions that strongly influence the probability and magnitude of steam explosions include

- the extent of coarse mixing (drop sizes and surface areas),
- the rate of heat production by the exothermic oxidation of molten metals and partially oxidized materials by the surrounding coolant, and
- the occurrence, timing, and strength of a spontaneous trigger (see below).

During mixing, some of the drops may spontaneously fragment into much smaller drops, on the order of 0.01 to 0.1 mm in diameter. This local fragmentation event is generally called a trigger. It may be produced by natural oscillations in the vapor film about the drop leading to fuel-coolant contact, or it may be induced by shock waves from falling objects, contact of the fuel with the bottom surface, entrance of the fuel into a region of colder water, or by turbulence generated in part of the mixing region. If the fragmentation is rapid enough, local shock waves can be produced, which can cause neighboring drops to fragment. If such a chain reaction escalates, a steam explosion can result.

Steam explosions can occur for a variety of high-temperature molten materials including uranium and its oxides. Spontaneous steam explosions have been observed for all possible contact modes including fuel pours, stratified water over fuel, and reflooding. High ambient pressure and saturated or only slightly subcooled water have been shown to reduce the probability of spontaneous steam explosions at experimental scales; however, explosions can still occur if the necessary triggers are available. The existing data base (fuel masses from 50 mg to 50 kg) implies that explosion strength tends to increase with increasing ambient pressure and increasing water temperature. Experimentally measured conversion ratios (the work done divided by the thermal energy available) range from zero to values approaching the thermodynamic maxima. Explosion pressures have been measured over the range of tens of bars to 2 kilobars. Steam explosion computer codes have predicted that pressures of many kilobars are possible for strong steam explosions.

Significant rates of hydrogen production have been observed for both explosive and nonexplosive FCIs. Much finer fragments produced in explosive FCIs can potentially lead to more rapid production of steam and hydrogen. The actual hydrogen production rate, however, is a result of two competing processes. The large surface-to volume ratio of the molten drop tends to increase the rate of heat transfer from the drop to water, but it also tends to increase the rate of exothermic oxidation, which adds energy to the drop and hot hydrogen gas to the vapor film surrounding the drop. The occurrence of a steam explosion as opposed to a nonexplosive FCI is generally thought to favor increased hydrogen production, especially when the melt is metallic as in foundries.

3.5.1.3 Limitations on In-Vessel FCIs

A rough estimate of the potential for energy release from in-vessel FCIs (excluding Zr oxidation) can easily be computed by calculating the energy that would have to be transferred to water in order to quench the entire core. For example, a typical PWR core might contain 10^5 kg of UO_2 and $2x10^4$ kg Zr. Assume that all of this material (plus 10^4 kg Fe to allow for structural material in the melt) is liquified at 4532°F (2500°C), below the UO_2 melt temperature of 5180°F (2860°C = 3133 K). The decrease in sensible and latent heat required to quench this melt to 212°F (100°C), saturation temperature for water at atmospheric pressure) is approximately 170 GJ. This requires the evaporation of approximately 75,000 kg or 75 m^3 of saturated water at atmospheric pressure.

In reality, the energy transferred from core materials to residual water would be less than 170 GJ for two reasons:

1. The volume of residual in-vessel water would be limited, in the absence of ECC restoration, and

2. Lower melt temperatures and/or higher in-vessel pressures, which would be anticipated in most severe accident scenarios, would reduce the temperature difference between molten core materials and residual in-vessel water.

Figure 3.5-2 illustrates the limited capacity for in-vessel FCI energy releases at various pressures in a PWR if the residual water is limited to 30 m^3, which is approximately the volume below the lower core plate. Table 3.5-1 shows the corresponding limitations of the mass of core material that could be quenched.[9]

Reactor vessel lower plenums, particularly in BWRs, contain significant quantities of structural materials as illustrated in Figures 3.5-3 and 3.5-4. Such structures could, at least temporarily, provide surfaces upon which molten debris could refreeze thereby restricting the volumes of melt and/or water participating in FCIs at a given time. For example, if melt flows into the lower plenum of a Westinghouse PWR by downward penetration through the lower core plate, as depicted in Figure 3.5-5, continued downward progress of melt into residual water in the lower plenum could depend upon the sequential failures of the diffuser plate and the massive bottom support forging, which is welded to the core barrel. If not failed by loads associated with explosive FCIs, each of these structural elements would fail by weakening soon after its cover of residual water boiled away, thus allowing melt to flow unimpeded into the water below. Table 3.5-2 provides some data on features and geometry that characterize these flow restrictions.[10]

Finally, it should be noted that the preceding estimates ignore the potential contribution to FCI energy releases associated with oxidizing metallic Zr contained in the melt. As noted in Subsection 3.3, quantities of unoxidized zirconium are likely to be involved in the core-liquefaction processes. Mixing of this metallic phase at high temperatures with the water in the lower plenum would promote rapid oxidation of the zirconium, depending primarily upon the degree to which fragmentation of the melt provides large increases in the interfacial surface area. The heat of reaction for Zr oxidation is approximately 6.5 MJ/kg of Zr reacted. If only 1% of the Zr typically contained in a PWR core ($2x10^4$ kg) were oxidized during in-vessel FCIs, an additional 1.3 GJ would be released. Regardless of the exact outcome, the addition of reaction energy and liberation of a quantity of hydrogen by the oxidation of zirconium during the melt-water interaction phase seems likely.

3.5.1.4 In-Vessel FCI Scenarios

In assessing the impact of in-vessel FCIs on accident progression, three alternative scenarios can be postulated:

1. No steam explosion but violent boiling, which may partially or totally quench the core debris, depending on the quantity of water available and the agglomeration of the debris;
2. One or more relatively low-yield steam explosions and nonexplosive quenching until the whole molten mass of fuel has been fragmented or all of the water evaporates;
3. A large steam explosion involving a significant fraction of the melt, triggered either spontaneously or by a low-yield steam explosion.

Because of the resultant disruption (and possible dispersal) of internal structures and residual core materials, the occurrence of even a relatively low-yield steam explosion could significantly alter the subsequent progression of damage.

3.5.1.5 Alpha Mode Containment Failure

Energetically, it is possible that a large in-vessel steam explosion could cause (a) breach of the reactor vessel,[11] or (b) breach of the reactor vessel and generation of containment-failing missiles.[12] Either event would completely alter the course of the accident by causing the immediate ejection of fuel and fission products from the reactor vessel. The second would result in nearly simultaneous venting of the containment. The possibility of these events accounts for the nil minimum duration for Stage 5 given in Table 3.1-1.

The Reactor Safety Study (RSS) identified the possibility that a large-scale in-vessel steam explosion could result in containment failure. This is commonly referred to as the alpha mode of containment failure. The RSS took the alpha mode failure probability (conditional on the occurrence of a core meltdown accident) to be 0.01, although the uncertainty in this probability was acknowledged by also providing a pessimistic estimate of 0.1.[12] Since the RSS, there has been considerable experimental research performed on fuel-coolant interactions at small to intermediate scales (<50 kg). A

1984 study concluded that for a significant containment failure probability due to in-vessel steam explosions

> *either a significant probability of (energy) conversion ratios higher than currently measured (5.3%) or a significant probability of large masses of molten core actively participating in an explosion would be needed.*[13]

The study showed that conversion ratios less than 5.3% and masses of actively participating molten core less that 5000 kg, as suggested by several mixing models,[14,15,16] imply an alpha mode failure probability of 0.0001 or less. However, some argue that the possibility of larger conversion ratios or larger masses actively participating can not be excluded and that the uncertainty in the alpha-mode containment failure probability is, therefore, large.[17]

In 1985, the NRC-sponsored Steam Explosion Review Group (SERG) reassessed the conditional probability of alpha mode failure.[18] The SERG pessimistic failure probability was 0.1, unchanged from the pessimistic estimate of the RSS. The NUREG-1150 α-mode failure probabilities are listed in Table 3.5-3.

3.5.2 Modes of Vessel Breach

Four modes of discharge of core materials from the vessel can be postulated:

1. massive failure of the vessel by an in-vessel steam explosion,
2. a pressure-driven melt jet,
3. gravity-driven pour of a large molten mass,
4. continuous dripping of core materials not involved in the initial release.

These modes of melt discharge are depicted in Figures 3.5-6 through 3.5-9 and discussed below.

3.5.2.1 Vessel Breach by an In-Vessel Steam Explosion

The steam-explosion kinetic energy required to fail the bottom head of a PWR has been estimated to be between 1 GJ and 1.5 GJ. Figure 3.5-2 and Table 3.5-2 indicate that a steam explosion need not involve large quantities of melt or water in order to yield such energies. In one study of PWR in-vessel steam explosions, failing the bottom head by an in-vessel steam explosion was found to be much more likely (probability of 0.2 versus 0.0001) than α-mode failure. Figure 3.5-6 illustrates this mode of vessel breach, which has the potential for driving particulate debris from the reactor cavity, resuspending radioactive aerosols previously plated out within the reactor coolant system, and forming additional aerosols during the explosion.

3.5.2.2 Quenching and Reheating of Debris in Bottom Head

In the event that the vessel is not breached by a steam explosion, a fraction of the core melt may be quenched. For core fractions equaling or exceeding the values in Table 3.5-1 (or smaller fractions for less water), the quenching would vaporize all of the water in the lower plenum. If excess melt over that which can be quenched is deposited in the plenum, it would begin heating the reactor vessel wall immediately. The quenched melt would subsequently begin reheating, but would require 20 to 40 minutes to attain temperatures that would augment the attack on the pressure vessel. Table 3.5-1 indicates the limited capacity for the formation of quenched debris in the lower plenum. The capacity is further reduced if the inventory of residual water is reduced below 29 m^3, which was assumed in developing Table 3.5-1.

Depending upon the extent of the core that becomes molten during Stage 4 and the fraction of this melt that is quenched by FCIs at the beginning of Stage 5, it is possible that the resulting bed of core rubble might be coolable. Accident termination during Stage 5 would, in addition to a coolable debris bed, require a supply of water to keep the debris submerged and a transport path and heat sink to remove decay heat from the system on a continuing basis. This is not unlike the situation that developed at TMI-2 as depicted in Figure 3.5-10, when the vessel was reflooded after molten debris had flowed into the lower plenum.

A large data base exists for debris bed coolability and a variety of models have been developed to explain the thermal and hydraulic processes that occur in a debris bed.[19] The key factors affecting the coolability of a debris bed are the bed power, its configuration, and its particle sizes. The higher the power generated in a bed, the more difficult the bed is to cool. The bed power at which some part of a flooded bed drys out is called the dryout power. If flooded from above, deeper debris beds tend to be less coolable than shallow debris beds of the same volume. Beds of smaller particles are less porous, the surface area for heat transfer is larger, and therefore, the vapor generation rates are increased relative to water ingress rates. Many particle sizes are possible during a severe accident, ranging from fractions of millimeters up to centimeter size and larger. There is no one exact particle size that defines a threshold for coolability. However particle sizes of a few millimeters and smaller, which could result from steam explosions, are most likely to be noncoolable. For example, Figure 3.5-11 shows the impact of particle size on the dryout heat flux (dryout power divided by top surface area of the bed) for beds flooded from above.[20]

A deep bed, sufficiently small or stratified particle sizes, and/or a small coolant fraction could produce dryout in the bed even after it is initially quenched.* Forced circulation of coolant through some possible configurations of in-vessel debris bed would be required to prevent dryout. Maintaining forced circulation was considered to be of paramount importance once it was re-established at TMI-2.

* E.D. Bergeron et al., "LWR Severe Core-Damage Phenomenology Program, LWR Degraded Core Coolability Program, Vol 2," SAND82-1115, Sandia National Laboratories, Albuquerque, NM.

3.5.2.3 Debris Reheating in Bottom Head

Even with forced circulation, melting in the interior of a debris bed can occur, and quenched or partially quenched debris beds could remelt even with forced circulation. Natural processes (such as capillary flow) tend to cause a melting debris bed to crumble. That is, melt flows through the open porosity toward the debris bed boundary where it freezes and forms a crust. If the crust is a poor conductor (e.g., an oxide), then very little of the energy is transferred out of the bed. A molten pool would form and very high temperatures could be attained in the melt. This could increase fission product releases. Furthermore, the quantity of retained fission products at the time of debris bed formation will influence the heat generation in the bed, and hence, its coolability. Models that describe the molten pool formation have been developed.[21]

3.5.2.4 Temperature-Induced Failure of the Bottom Head

Natural convection in the molten pool causes the energy transport to be a multi-dimensional. Experiments have shown that most of the energy is transported upward and radially, and very little is transported downward (a few percent).[22,23,24] This means that the heating of the lower head will slow. Hence, head failure is likely to be delayed relative to melt formation in the debris bed.

Failure of the bottom head would occur when the temperature of the steel increased to the point where the stress level exceeded the material's strength. Figure 3.5-12 shows that the strength of steel decreases rapidly as its temperature exceeds 1832°F (1000°C), which is far less than the nominal melting point of 304 stainless steel, 2550-2600°F (1399-1427°C or 1672-1700 K).

Early investigators focused on weakening of the entire bottom head. Estimates of the time required for such failures vary, typically from 22 minutes to 40 minutes, depending on whether the vessel is pressurized or not.[25] In pressurized accidents, the vessel would contain residual water and the lowest part of the bottom head might be the last location of such water. Bottom head failure could occur further up the sides of the hemisphere, where the vessel would tend to be heated earlier. Since pressure relief can occur through a small opening, initial failure was presumed to be by a relatively small crack or split in the vessel wall, which would reduce the stress substantially. Following this initial failure in a pressurized accident, or, as the primary failure mode in an unpressurized accident (e.g. a large-break LOCA), failure was originally expected to occur by the mechanism of combined melting and high temperature weakening accompanied by large plastic deformation of the entire bottom head, resulting in the bulk of the core materials in the bottom head falling into the reactor cavity.[10]

In a 1981 PRA performed for the Zion plant, an alternative mechanism for bottom head failure was identified.[26] Local meltthrough was postulated to occur at an in-core instrument tube penetration. The time to failure identified for this mode is typically 5 to 7 minutes, independent of relative pressure.

The 80 minute maximum duration given in Table 3.3-1 for Stage 5 results from combining the maximum estimated time-to-breach for the reactor vessel (40 minutes) with a scenario in which the core material deposited in the lower plenum is initially quenched (without a vessel-failing steam explosion), and must subsequently reheat to produce vessel failure.

3.5.2.5 Impact of Melt Discharge from Vessel

The mode of vessel breach can strongly influence the timing and nature of potential loads imposed on containment. In 1984, the NRC-sponsored Containment Loads Working Group identified the fact that pressurized dispersal of high-temperature melt into containment at the time of vessel breach (Figure 3.5-7) could result in rapid direct heating and exothermic chemical reactions within the containment atmosphere and pose a severe threat to containment integrity. On the other hand, if the vessel is depressurized, molten material would simply flow into the reactor cavity by gravity (Figure 3.5-8); although, if water were present in the reactor cavity, significant loads on containment could result from ex-vessel fuel coolant interactions (Figure 3.5-9) or from the additional hydrogen generated in such interactions. The initial geometry and potential for cooling of ex-vessel debris, as well as the nature of interactions between core materials and concrete, are strongly influenced by the mode of vessel breach. The mode of melt discharge into containment also has a strong influence on the subsequent concentrations of fission products, particularly in aerosol form, in the containment. Ex-vessel phenomena are discussed in Module 4.

3.5.2.6 Long-Term Melt Releases to Containment

Following either a pressurized ejection or a gravity-driven pour of melt from the vessel, a significant fraction of core materials may remain unmelted in the core region. Without coolant, much of this material may subsequently melt and drop out of the vessel in small amounts over a period of hours. This mode of discharge is illustrated in Figure 3.5-9. If there is water below the vessel, the dripping mass may prolong ex-vessel fuel-coolant or core-concrete interactions. If the hotleg or surge line had failed earlier, natural circulation could be established with flow from the reactor cavity up through the reactor vessel and out the failed pipe. All such possibilities would affect the magnitude of the radiological release given late containment failure.

Table 3.5-1 Fractions of core mixture* that can be quenched in below-core water**

	Saturated Water Pressure			
	Atmospheric	800 psia (5.5 MPa)	1595 psia (11 MPa)	2465 psi (17 MPa)
ΔT = 2700°F (1500°C)	0.79	0.44	0.31	0.17
ΔT = 3600°F (2000°C)	0.59	0.33	0.23	0.13
ΔT = 4500°F (2500°C)	0.37	0.21	0.14	0.08

*10^5 kg UO_2 + $2x10^4$ kg Zr + 10^4 kg steel
**in 29 m^3 of water

Table 3.5-2 Lower Plenum Features

Feature	Approx. Thickness (mm)	Water Volume to Next Feature (m^3)	Energy to Evaporate Water (GJ)**
Lower Core Plate	50	6.6	4.6
Diffuser Plate	37	14.1*	9.8
Bottom Support Plate	220	7.7*	5.4
Reactor Vessel Bottom	132	0	--

*Ratio of these two volumes approximate; sum (21.8 m^3) is volume of lower hemisphere.
** Based on a pressure of 2500 psia (17.2 MPa).

Table 3.5-3 NUREG-1150 Alpha Mode Failure Probabilities
Conditional on the Occurrence of Core Meltdown

	Plant	System Pressure	Lower Bound	Mean	Upper Bound
BWRs	Grand Gulf	High	0	1.0E-3	0.1
		Low	0	1.0E-2	1.0
	Peach Bottom	High	1.0E-8	1.0E-3	1.0E-1
		Low	1.0E-7	1.0E-2	1.0
PWRs	Sequoyah	High	0	8.5E-4	0.1
		Low	0	8.5E-3	1.0
	Surry	High	0	9.1E-4	0.1
		Low	0	9.1E-3	1.0

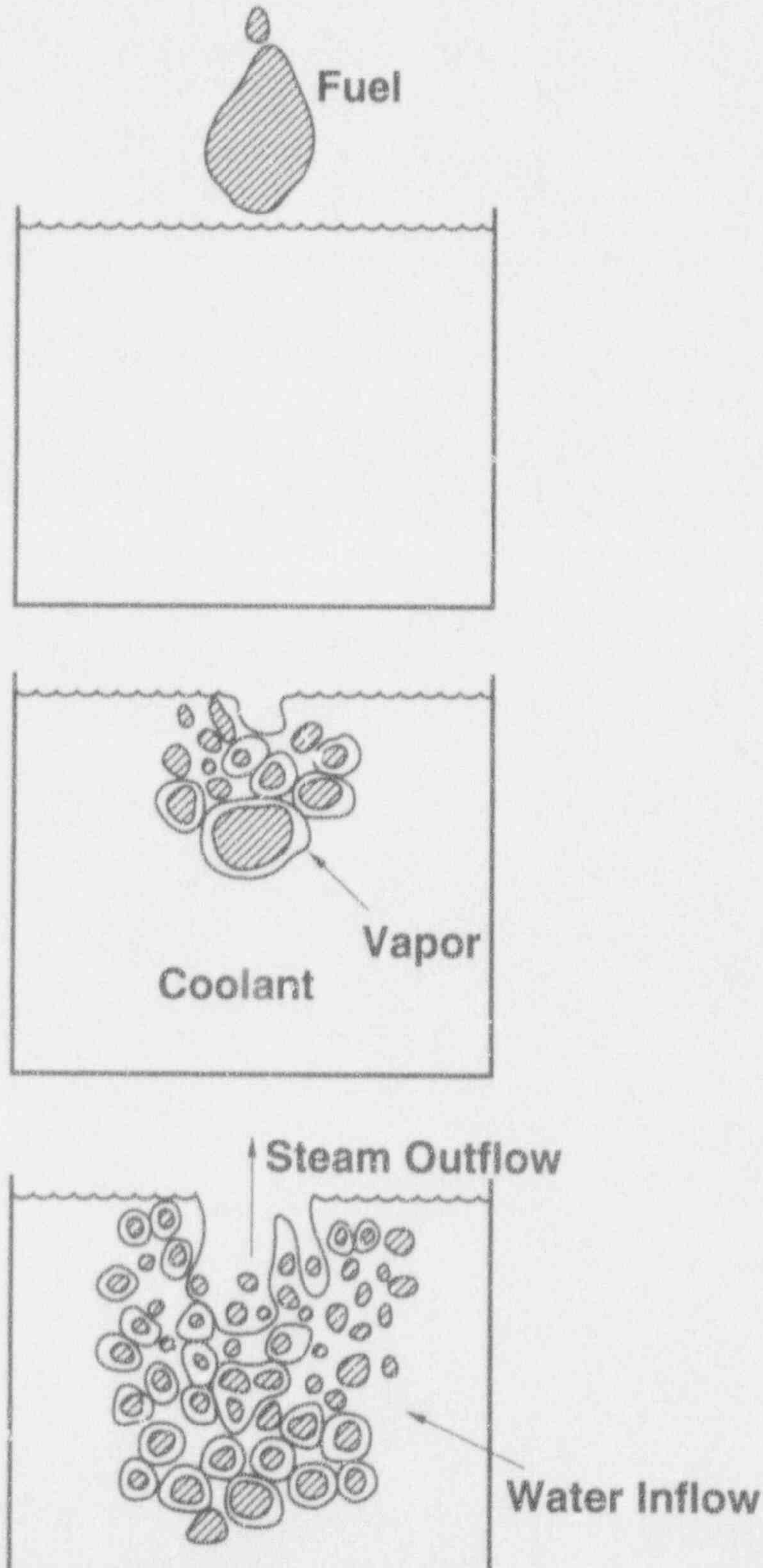


Figure 3.5-1 Progression of fuel-coolant mixing

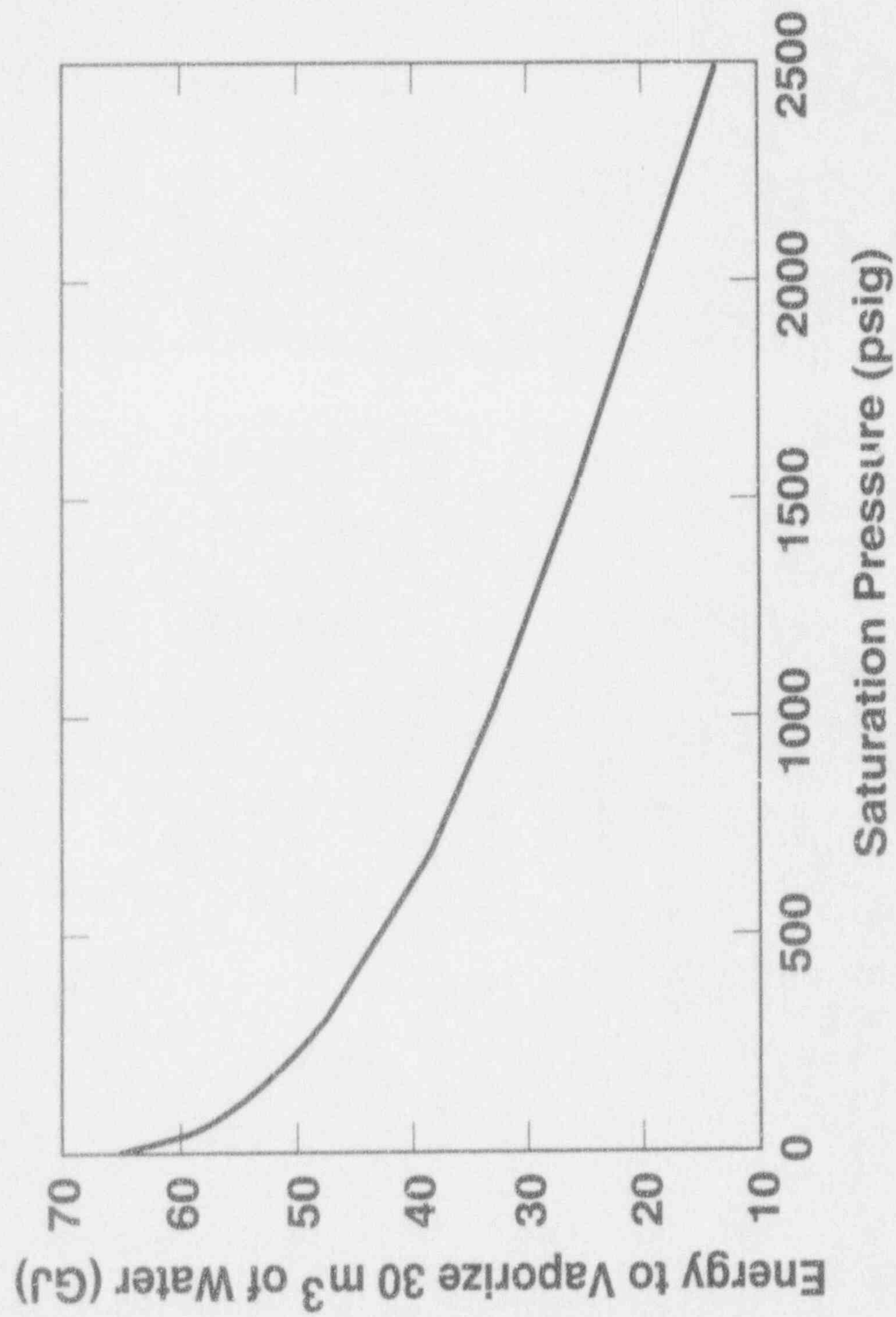


Figure 3.5-2 Energy required to vaporize 30 m^3 of water versus saturation pressure

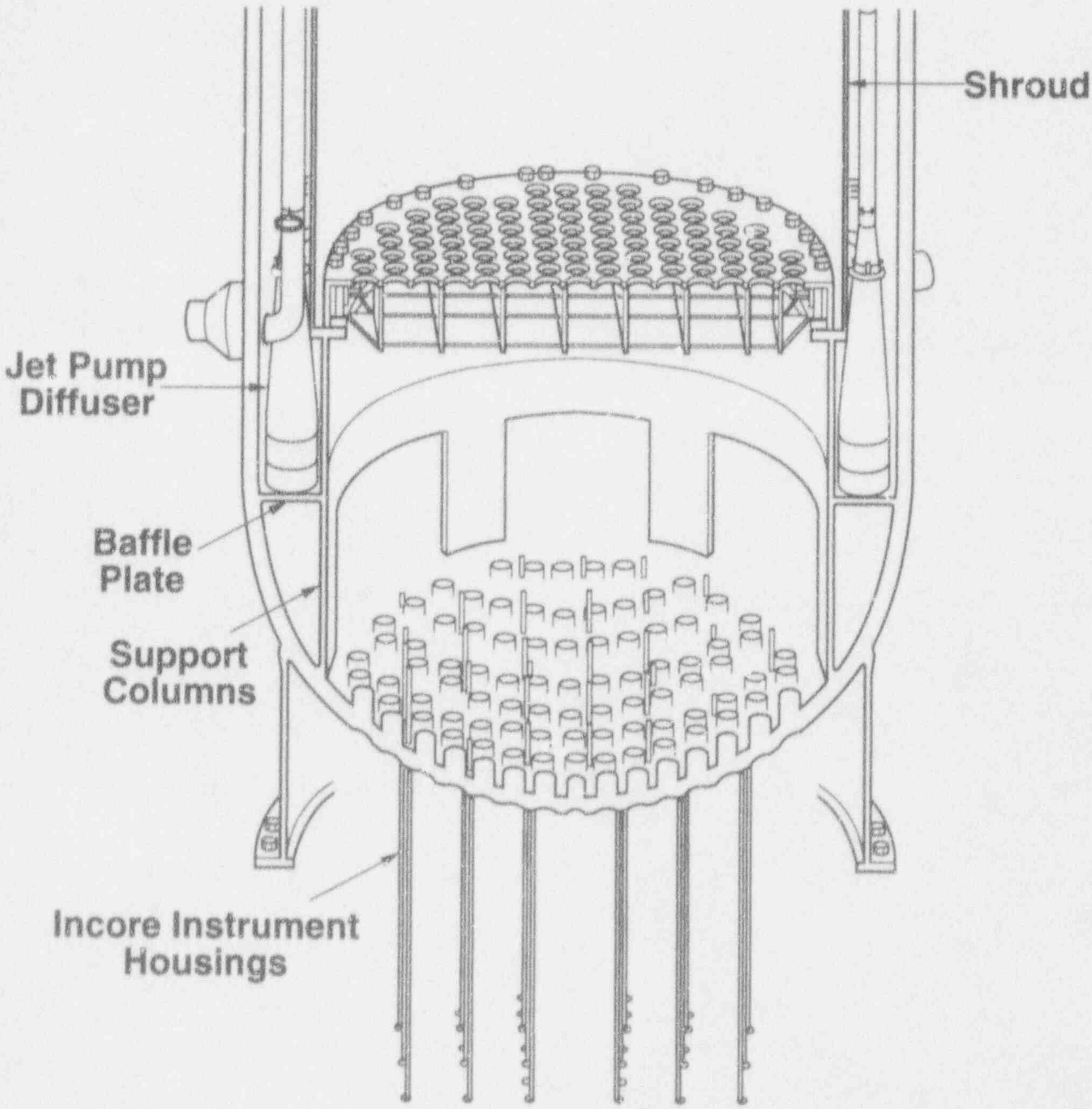


Figure 3.5-3 BWR reactor vessel lower plenum region components

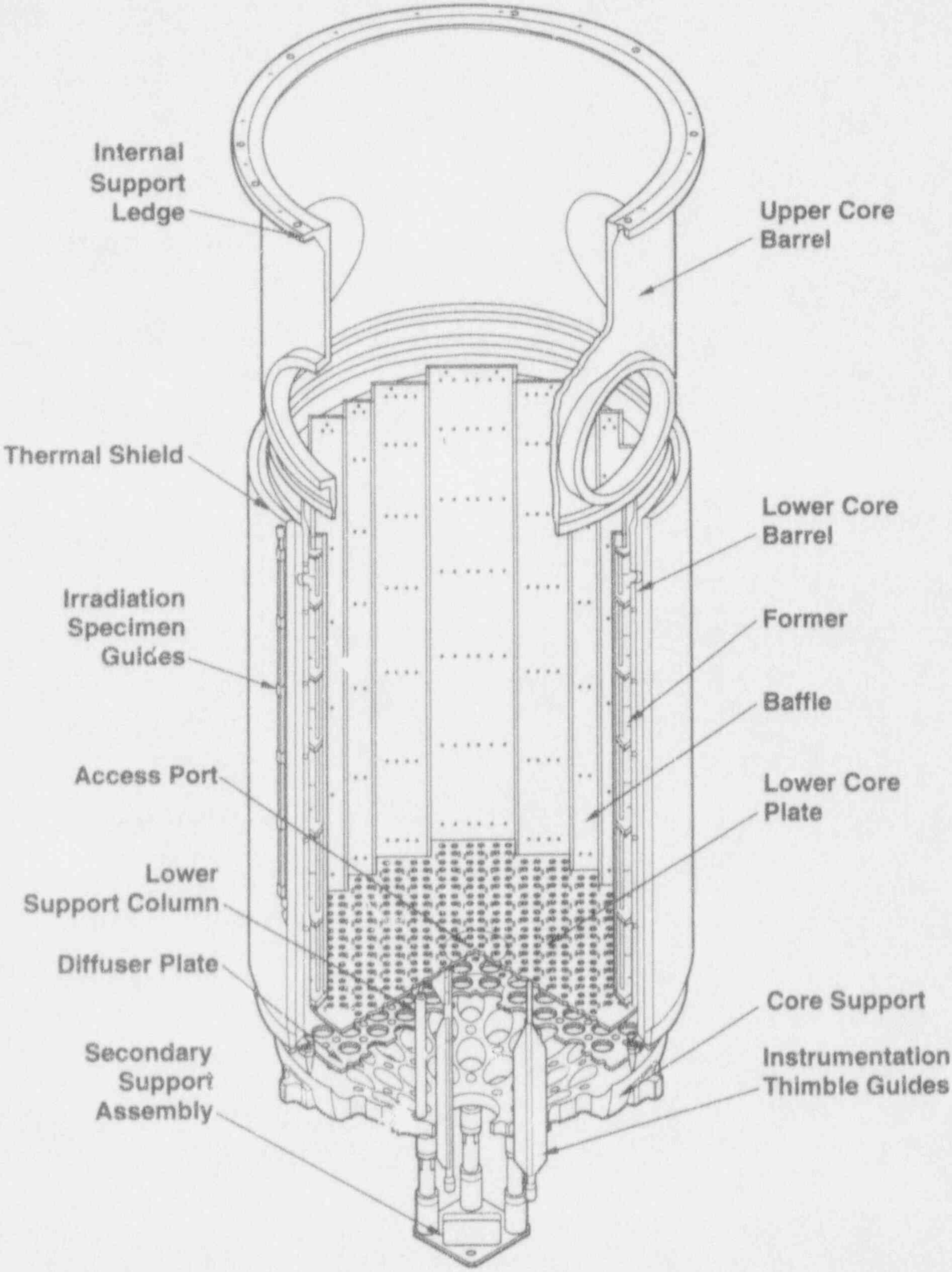


Figure 3.5-4 PWR lower core support structure

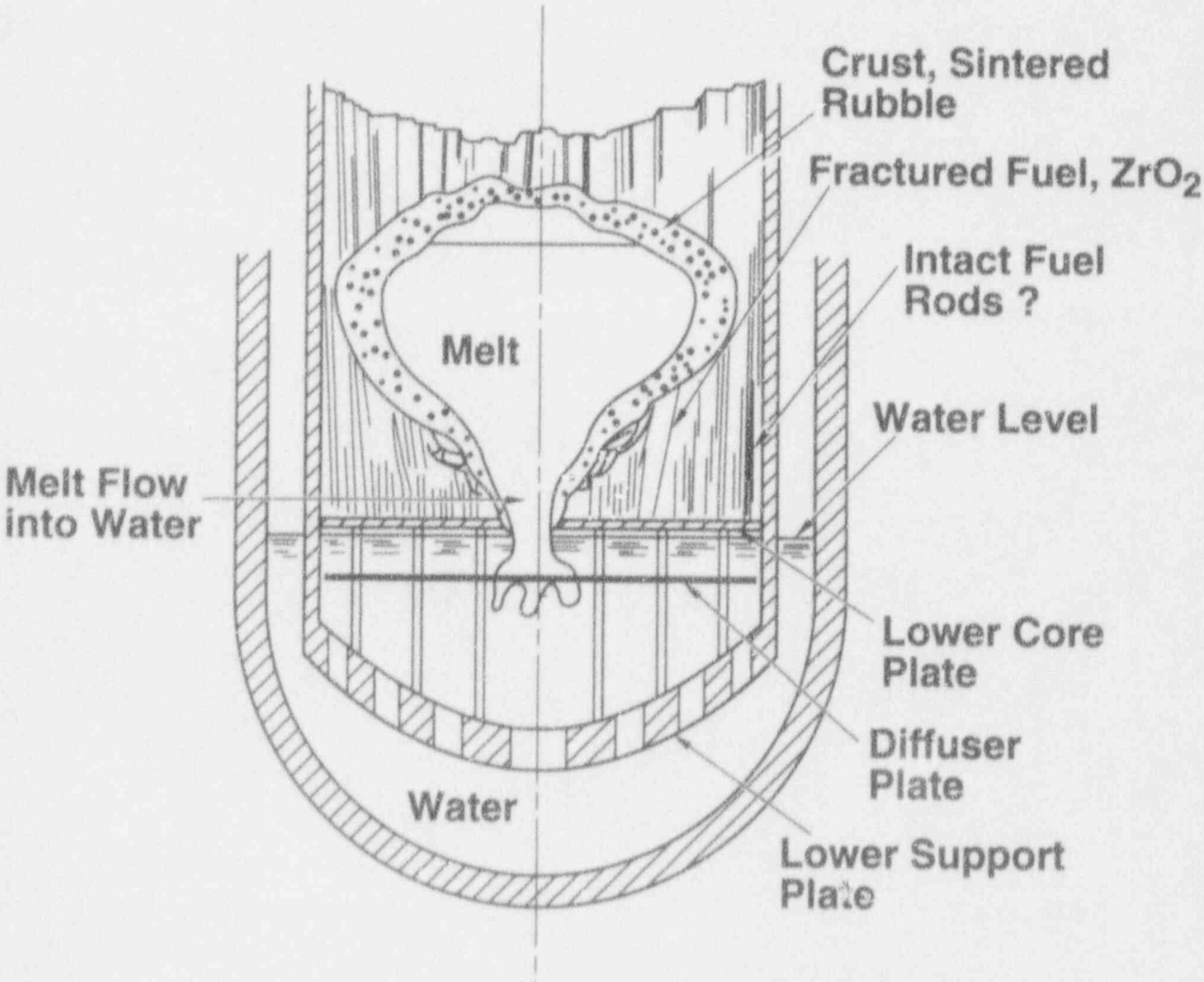


Figure 3.5-5 Melt pour into lower plenum by failure of the lower core plate

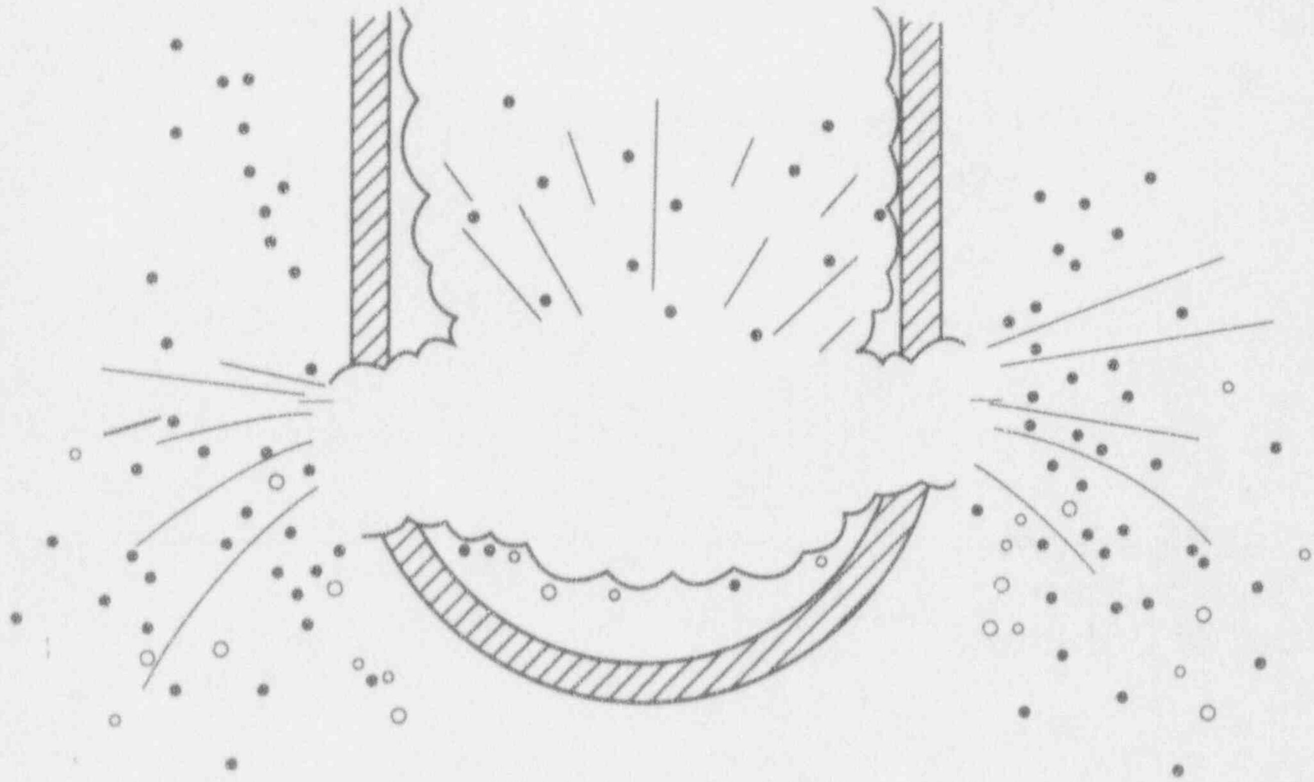


Figure 3.5-6 Vessel failure from steam explosion

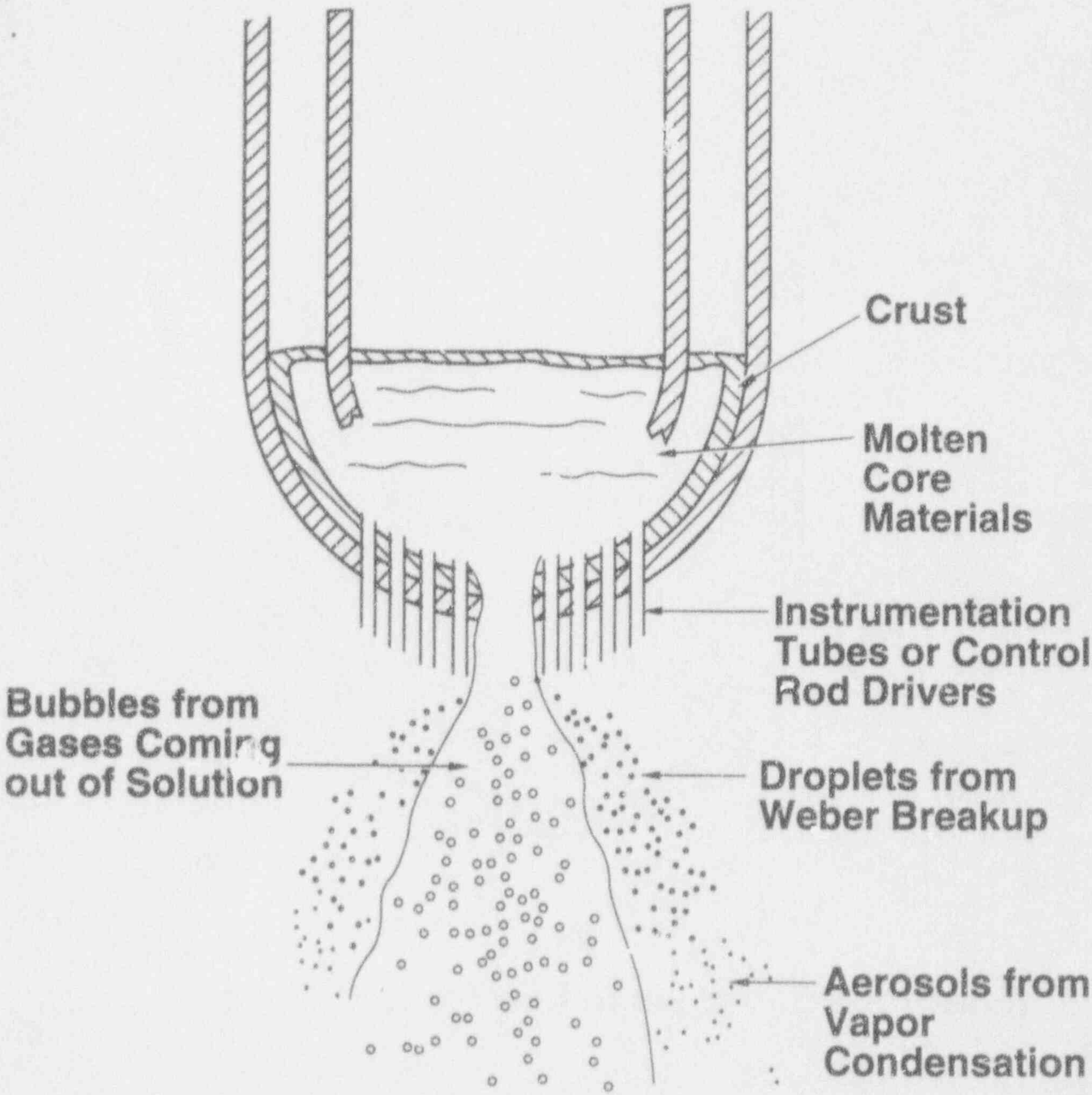


Figure 3.5-7 High-pressure melt release from bottomof reactor vessel

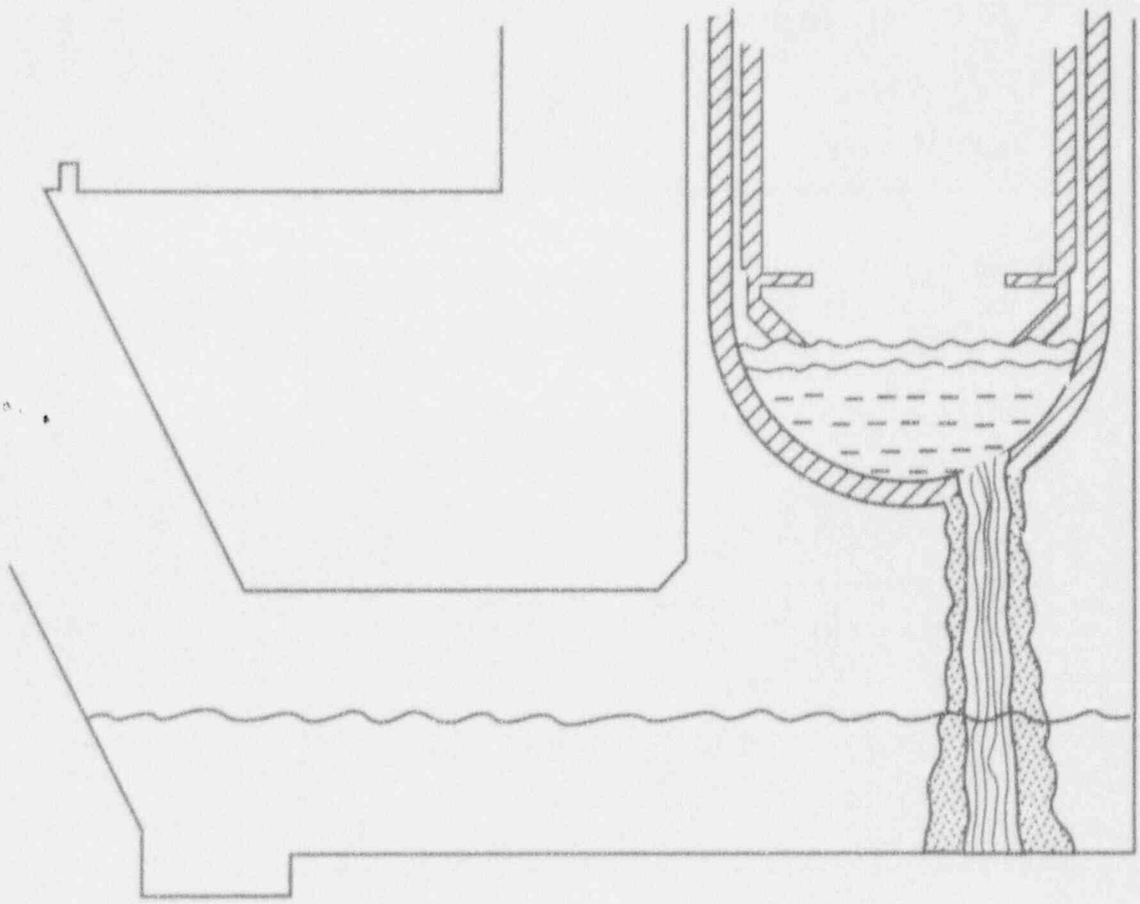


Figure 3.5-8 Low-pressure melt release from bottom of pressure vessel

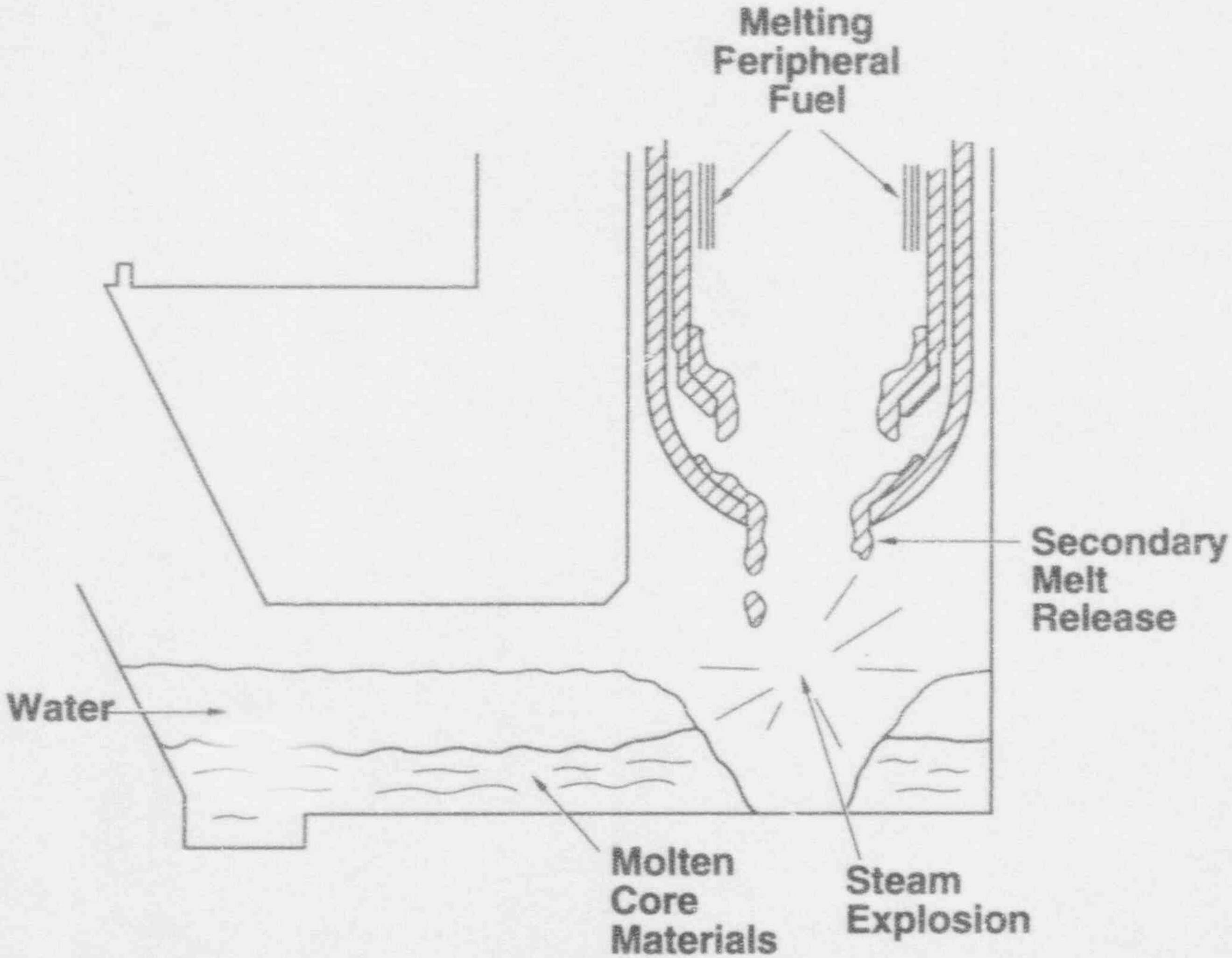


Figure 3.5-9 Secondary melt release in a Zion-type PWR reactor cavity

1

IMAGE EVALUATION TEST TARGET (MT-3)

150mm

6"

1

IMAGE EVALUATION TEST TARGET (MT-3)

150mm

6"

1

IMAGE EVALUATION TEST TARGET (MT-3)

150mm

6"

1

IMAGE EVALUATION
TEST TARGET (MT-3)

150mm

6"

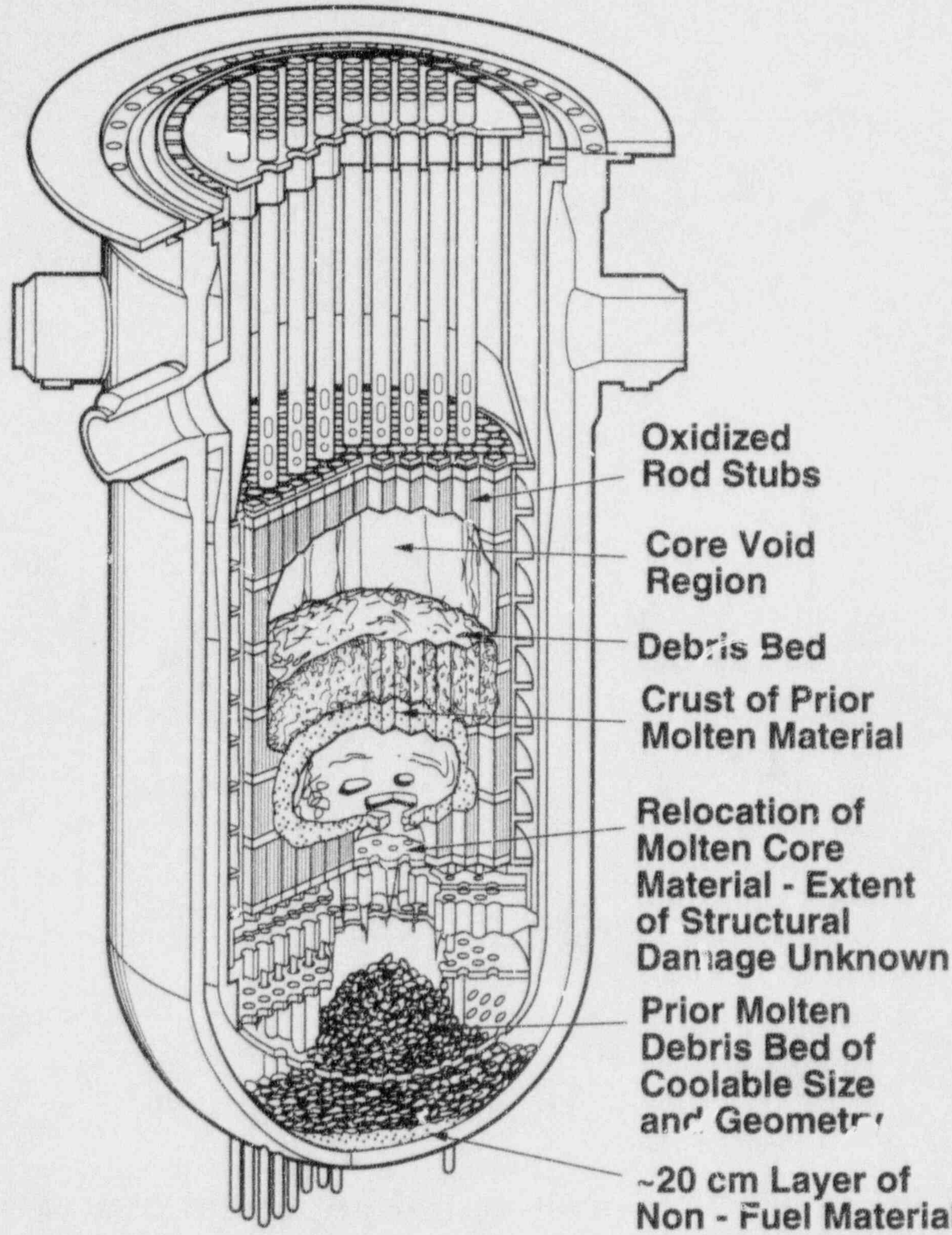


Figure 3.5-10 Condition of TMI-2 core after molten debris relocated to the lower plenum

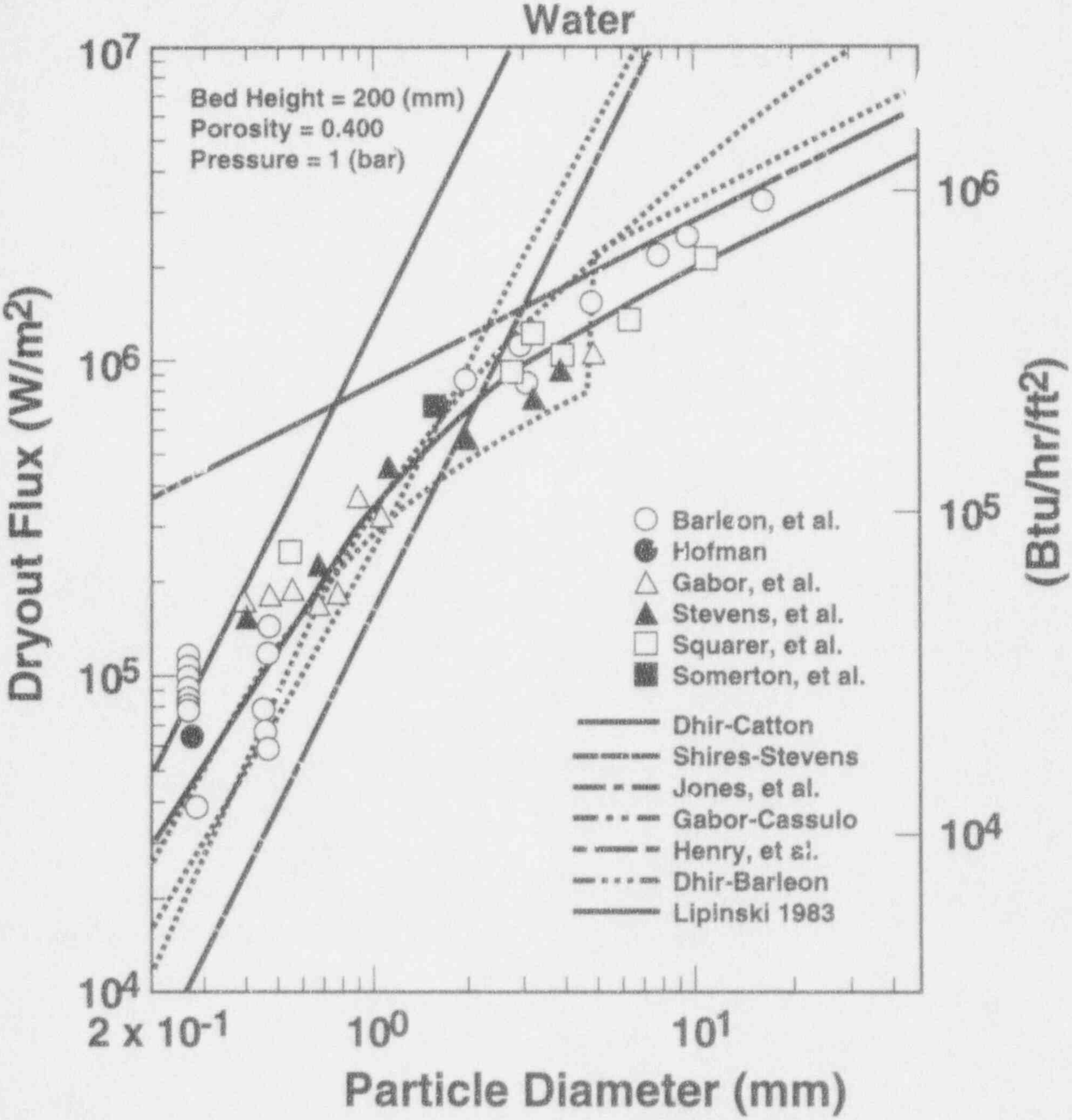


Figure 3.5-11 Debris bed dryout heat flux versus particle diameter for water

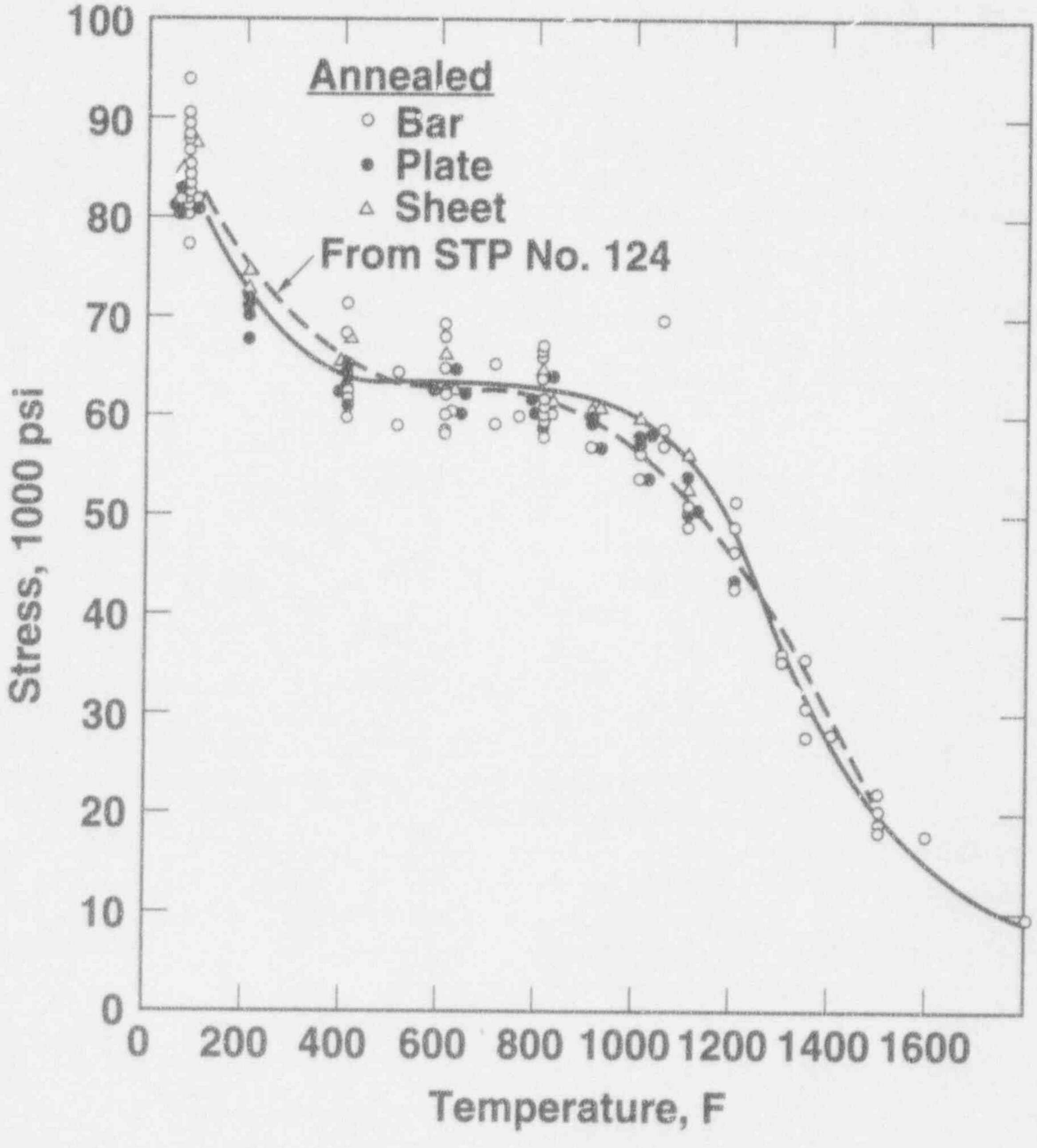


Figure 3.5-12 Tensile strength, type 304 stainless steel

References for Section 3.5

1. R. C. Reid, "Rapid Phase Transitions from Liquid to Vapor," **Advances in Chemical Engineering**, **12**, pp 105-208, 1983.

2. M. L. Corradini, B. J. Kim, and M. D. Oh, "Vapor Explosions in Light Water Reactors: A Review of Theory and Modelling," **Progress in Nuclear Energy**, **22**, 1, pp 1-117, 1988.

3. G. Chaucer, "The Canon's Yeoman's Tale," in **Canterbury Tales**, Garden City Publishing Company, Inc., Garden City, NY, 1934.

4. M. Berman, "Thermodynamic and Fluid-Dynamic Modelling of Two-Phase Propagating Explosions," Workshop on the Causes and Prevention of Melt-Water Interactions, Sandia National Laboratories, Albuquerque, NM, July 29, 1988.

5. M. Berman et al., Discussions of Steam Explosions at Chernobyl, in "Chernobyl: Where Do We Go From Here," **Proceedings of the Conference-by-Computer, Nuclear Publications**, McGraw-Hill, New York, NY, September 29-October 17, 1986.

6. W. Sweet, "Chernobyl, What Really Happened," **Technology Review**, pp 43-52, July, 1989.

7. F. Reisch, "Chernobyl - the Initiating Event?," **Nuclear News**, December 1987.

8. A. W. Cronenberg, "Recent Developments in the Understanding of Energetic Molten Fuel-Coolant Interactions," **Nuclear Safety, 22, 3**, May-June 1980, pp319-337.

9. J. B. Rivard et al, Identification of Severe Accident Uncertainties, NUREG/CR-3440, SAND83-1689, Sandia National Laboratories, Albuquerque, NM, September 1984.

10. Joseph B. Rivard, Review of In-Vessel Meltdown Models, NUREG/CR-1493, SAND80-0455, Sandia National Laboratories, Albuquerque, NM, July 1980.

11. J. H. Gittus et al, PWR Degraded Core Analysis, ND-R-610(S), United Kingdom Atomic Energy Authority, Springfields, UK, 1982.

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

13. M. Berman, D. V. Swenson, and A. J. Wickett, An Uncertainty Study of PWR Steam Explosions, NUREG/CR-3369, SAND83-1438, Sandia National Laboratories, Albuquerque, NM, 1984.

14. R. E. Henry, H. K. Fauske, "Required Initial Conditions for Energetic Steam Explosions," **Proc. ASME Winter Meeting**, Washington, DC, November 1981.

15. T. G. Theofanous and M. Saito, "An Assessment of Class 9 (Core-Melt) Accidents for PWR Dry Containment Systems," **Nucl. Eng. Des.** 1981, pp.301-332.

16. M. L. Corradini and G. A. Moses, "A Dynamic Model for Fuel-Coolant Mixing," **Proc. Int. Mtg. on LWR Severe Accident Evaluation**, Cambridge, MA, August 1983.

17. M. Berman, "Molten-Core Coolant Interactions Program," **Proc. 12th Water Reactor Safety Research Information Meeting**, 1984.

18. NUREG-1116, A Review f the Current Understanding of the Potential for Containment Failure Arising from In-Vessel Steam Explosions, 1985.

19. R. J. Lipinski, "A Coolability Model for Postaccident Nuclear Reactor Debris," **Nuclear Technology**, **65**, pp. 53-66, 1980.

20. R. Lipinski, "Debris Bed Dryout," Appendix 3.2-B of Thermal-Hydraulic Process Modeling in Risk Analysis: An Assessment of the Relevant Systems, Structures, and Phenomena, NUREG/CR-3986, SAND84-1219, Sandia National Laboratories, Albuquerque, NM, August 1984.

21. S. S. Dosanjh, On the Melting and Refreezing of Porous Media, NUREG/CR-5028, SAND87-1976, Sandia National Laboratories, Albuquerque, NM, 1987.

22. J. T. Hitchcock and J. E. Kelly, The DC-1 and DC-2 Debris Coolability and Melt Dynamics Experiments, NUREG/CR-4060, SAND84-1367, Sandia National Laboratories, Albuquerque, NM, 1985.

23. C. P. Fryer and T. J. Hitchcock, The Post-Irradiation Examination of the DC Melt Dynamics Experiments, NUREG/CR-4625, SAND86-1102, Sandia National Laboratories, Albuquerque, NM, 1988.

24. F. A. Kulacki and Goldstein, "Thermal Convection in a Horizontal Fluid Layer With Uniform Volumetric Energy Source," **J. Fluid Mech.**, 55, pp. 271-287, 1972.

25. F. A. Kulacki, Estimates of Failure Time for LWR and LMFBR Vessels Following a Core Meltdown Accident, Ohio State University, Department of Mechanical Engineering, USNRC contract AT-(49-24)-0149 Report, February 1976.

26. Commonwealth Edison Company, "Zion Probabilistic Safety Study," Chicago, IL, 1981.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ILLUSTRATIONS (Continued)

LIST OF ILLUSTRATIONS (Continued)

4.0 ACCIDENT PROGRESSION IN THE CONTAINMENT

4.0.1 Introduction and Background

As discussed in Module 1, containments began to evolve when designers realized that remote siting would not be practical in all cases. The first containments were provided for the Knolls Atomic Power Laboratory and Shippingport experimental reactors in order to allow them to be sited in more populated areas. Containments for large power reactors evolved during the 1960s, representing a key element of the defense-in-depth strategy. In the event of a design-basis accident, containments are designed to minimize leakage and keep offsite doses well below the 10 CFR 100 limits.

Two basic strategies are used in U.S. containments. The passive pressure suppression approach, used in all General Electric Boiling Water Reactors and Westinghouse Pressurized Water Reactor Ice Condenser Containments, involves the use of an energy absorbing medium to absorb most of the energy released during a design-basis loss-of-coolant accident. For BWRs the medium is a water-filled suppression pool, and for ice condenser containments, the medium consists of numerous columns of ice. The second approach, used in most PWRs, is simply to design a large, strong volume to receive the energy. All containments also contain active cooling systems, such as sprays and fan coolers, to provide additional cooling and pressure suppression during a design basis accident. These active systems do not act quickly enough to affect the initial blowdown during a large-break loss-of-coolant accident, but limit further pressure increases and are beneficial during slower developing accidents.

Containments are designed to cope with the accidents specified in Chapter 15 of the Safety Analysis Report, as discussed in Section 2.1. Generally, the most limiting design-basis accident leading to the highest pressure rise in the containment is a double-ended guillotine break in a pump discharge line in the reactor coolant system. The design-basis accident leading to the highest containment temperatures is usually a double-ended guillotine break in a main steam line. As described in Section 4.1, containments are designed to survive such accidents with considerable margin.

The China Syndrome and the Reactor Safety Study began to cast doubt on the ability of containments to survive all possible accidents, and it became clear that risk to the public is usually dominated by those accidents in which the containment fails or is bypassed. In a severe accident, there are sources of energy and phenomena that can cause a greater threat to containment than the design-basis loss-of-coolant accident. The hydrogen burn at Three Mile Island highlighted the potential threats from severe accident phenomena, even though the containment survived that particular event. The remainder of this module describes different containment designs and the potential threats to those designs.

4.0.2 Module 4 Learning Objectives

At the end of this module, the student should be able to:

1. Describe the six basic containment types and associated engineered safety features.

2. Identify which containment types are less susceptible to isolation failures.

3. Contrast the potential failure mechanisms for steel and concrete containments.

4. Describe the following causes of containment failure. For each cause, indicate when failure could occur.

   a. Direct containment heating

b. Fuel-coolant interactions
c. Local liner meltthrough
d. Combustion
e. Long-term overpressure

5. Describe a BWR accident scenario in which venting of a Mark I or Mark II containment might be appropriate.

6. List at least one concern regarding the containment if AC power is restored late in a station blackout accident.

7. Explain the different hydrogen control measures used in BWR Mark I, II, and III and PWR ice condenser containment designs.

8. Characterize the usefulness of hydrogen recombiners during severe accidents.

4.1 Containment Characteristics and Design Bases

4.1.1 Containment Types

There are six basic containment types used for U.S. Light Water Reactors (LWRs). Four of those designs primarily use the passive pressure suppression concept, and two rely primarily on large, strong volumes. All of these containments are constructed of either steel or concrete with a steel liner for leak tightness. Boiling Water Reactor (BWR) designs, which have evolved from the Mark I to the Mark III design, all use a pressure suppression pool. A few Westinghouse PWRs have ice-condenser (pressure suppression) containments, but most PWRs have large, dry containments or a subatmospheric variation of the large, dry containment. Table 4.1-1 lists the number of containments of each type.[1] Figure 4.1-1 shows a comparison of the containment volumes and design pressures for typical containments.[2] The design pressures for containments are based on a very conservative design process. If all isolation features work properly, it is likely that containments will not fail until the design pressures have been greatly exceeded. Figure 4.1-2 compares the design pressures with realistic estimates of ultimate failure pressures for six typical containments.[3,4]

The next six subsections describe the six containment types in more detail. It is important to note that there are plant-specific variations within each containment type, and these discussions do not delineate all of these design differences.

4.1.1.1 Large Dry Containments

A typical large dry containment is shown in Figure 4.1-3. A large dry containment is designed to contain the blowdown mass and energy from a large break Loss-of-Coolant Accident (LOCA), assuming any single active failure in the containment heat removal systems. These systems may include containment sprays and/or fan coolers, depending on the particular design. Large dry containments can be of either concrete or steel construction. Concrete containments have steel liners to assure leak tightness. Large dry (and all other) containments have a large, thick basemat that provides seismic capability, supports the structures, and may serve to contain molten material during a severe accident.

During an accident, most of the water introduced into containment through a pipe break or relief valves collects in the sump. The water can include the initial reactor coolant inventory plus additional sources injected into the reactor coolant system. Water may enter containment as vapor, liquid, or a two phase mixture. The liquid portion drains quickly into the sump and the vapor portion may condense (on structures or containment spray drops or coolers) and then drain into the sump. Once water storage tanks have been depleted, water in the sump is recirculated to the vessel and/or the containment sprays using recirculation systems to provide long-term heat removal. It is important that the sumps be kept clear of debris that could inhibit this recirculation Large dry containments are not as susceptible to hydrogen combustion as other, smaller containments. No systems are provided for short term hydrogen control during a severe accident (see Section 4.6). However, hydrogen recombiners are provided to allow long-term hydrogen control.

4.1.1.2 Subatmospheric Containments

Subatmospheric containments are very similar to large dry containments, as shown in Figure 4.1-4. The major difference is that the containment is maintained at a negative pressure (~ 5 psi or 35 kPa) with respect to the outside atmosphere. This negative pressure means that leakage during normal operation is into the containment rather than to the atmosphere.

Further, this negative pressure provides additional margin for response to design basis accidents, and therefore, the design pressure and/or volume can be reduced accordingly. Keeping the containment at a subatmospheric pressure also means that any significant containment leaks will be readily detected, when maintaining the negative pressure becomes more difficult.

4.1.1.3 Ice Condenser Containments

Figure 4.1-5 shows the layout of an ice condenser containment and Figure 4.1-6 shows the ice condenser in more detail. Ice condenser containments are constructed of either concrete or steel. Ice condenser containments are the only PWR containments that rely primarily on passive pressure suppression. The containment consists of an upper and a lower compartment connected through an ice bed. In the event of a design-basis loss-of-coolant accident, steam flows from the break, into the lower compartment, and up into the ice beds where most of the steam is condensed. Return air fans maintain a forced circulation from the upper to lower compartments, enhancing flow through the ice beds. One-way doors are present at the entrance and exit of the ice bed region. These doors open upon slight pressure from the lower compartment, but close if air flow occurs in the reverse direction.

The ice beds are more than adequate to limit the peak pressure from a design-basis loss-of-coolant accident. However, in a long-term accident, the ice will eventually melt and containment heat removal will be required. Thus, containment sprays are provided in the upper compartment of the containment. Water from the sprays drains through sump drain lines down into the lower compartment sump, where it can be recirculated for long-term heat removal. It is noteworthy that, because of the melting ice, there will be more water in the lower compartment during many accidents than would be present in a large dry containment. The effect of this additional water upon severe accident phenomena will be discussed in later sections.

Because of their smaller volume, ice condenser containments are more susceptible to combustion events than large dry containments. In fact, a combustion event involving the same quantity of hydrogen that was burned at TMI-2 might have led to containment failure in an ice condenser containment. Therefore, specific hydrogen control requirements have been placed on ice condenser containments. These requirements are examined in Section 4.6.

4.1.1.4 BWR Mark I Containments

Mark I containments are provided for most of the older BWR plants, 24 in number. The Mark I is a pressure suppression containment, which allows the containment to be smaller in volume. The basic design is shown in Figure 4.1-7. The containment is divided into the drywell containing the reactor vessel and the wetwell (torus) containing the suppression pool. The containment may be constructed of either concrete or steel. The water in the suppression pool acts as an energy absorbing medium in the event of an accident. If a loss-of-coolant accident occurs, steam flows from the drywell through a set of downcomers into the suppression pool, where most of the steam is condensed. Steam can also be released through the safety relief valves and associated piping directly into the suppression pool. In the event that the pressure in the wetwell exceeds the pressure in the drywell, vacuum breakers are provided that equalize the pressure.

The water in the suppression pool can be recycled through the core cooling systems, much the same as sump water is recycled in a PWR. Long term containment heat removal can be provided by sprays or suppression pool cooling systems either of which can be aligned with appropriate heat exchangers. In addition, Mark I containments are equipped with lines connected to both the drywell and the wetwell (provided initially for inerting, leak testing, and other purposes) that can be used to vent the containment if the pressure becomes too high. As will be discussed later, the particular venting strategy chosen can significantly impact the course of an accident.

Because of the small volume of the Mark I containment, hydrogen control measures are required. In this case, the drywell is inerted with nitrogen to preclude the possibility of combustion. More details on hydrogen concerns for Mark I BWRs are contained in Section 4.6.

4.1.1.5 BWR Mark II Containments

Mark II containments are similar in concept to Mark I containments. Figure 4.1-8 shows a Mark II containment. The suppression pool design is simplified and can remove steam more efficiently, and the entire containment structure is more unified. Instead of the complicated torus design included in the Mark I containment, the suppression pool simply sits in the wetwell region below the drywell. Containment heat removal systems (sprays and suppression pool cooling) and nitrogen inerting strategies are the same as for the Mark I containments. Containment venting can also be performed in a similar fashion to the Mark I containments.

4.1.1.6 BWR Mark III Containments

While the Mark II design represented an evolution of the Mark I design, the Mark III design introduced major changes. A typical Mark III containment is shown in Figure 4.1-9. Mark III containments can be free-standing steel or steel-lined concrete. These containments have a drywell that functions much as the older designs, but have a larger surrounding containment that includes the wetwell. In the Mark III design, the suppression pool is located in an annular region outside the drywell.

The suppression pool function is essentially the same as in the older designs. In this case, if there is a loss-of-coolant accident in the drywell, then steam will flow through horizontal vents to the suppression pool where the steam will be condensed. It is possible for the blowdown to cause the suppression pool to slosh over the weir wall and partially fill the drywell. In order to assure that adequate water is available in the suppression pool, allowing for recirculation, evaporation, and sloshing, water can be added to the suppression pool from the upper pool above the drywell.

If the pressure in the outer containment exceeds the pressure in the drywell, then vacuum breakers open to equalize the pressure. Long-term containment heat removal can be accomplished with suppression pool cooling or by containment sprays (with appropriate circulation of the water through heat exchangers) in the outer containment.

An important asset of the Mark III design is construction of the outer containment around the drywell, effectively providing a double layer of protection. If containment failure were to occur, in many cases the outer containment would fail first, leaving the drywell and suppression pool intact. Any subsequent fission product releases would still be scrubbed as they passed through the suppression pool, greatly reducing the source term. Thus, the only accidents (other than bypass sequences) likely to produce large source terms must involve failure of the outer containment plus either loss of the suppression pool or failure of the drywell.

The Mark III design is an intermediate-sized containment, much like the ice condenser containment. It is large enough that inerting is not required for hydrogen control, but still small enough that some hydrogen control measures are needed. Those measures are discussed in later sections.

4.1.2 Containment Design Criteria

Section 2.1 provided a discussion of design-basis accidents, as included in Chapter 15 of the Safety Analysis Report (SAR). For containments, the design must preclude exceedance of the 10 CFR 100 dose guidelines, given the most limiting accident evaluated in Chapter 15. Specifically, the requirements of 10 CFR 50, Appendix A, General Design Criterion 50 state:

> *The reactor containment structure, including access openings, penetrations, and the containment heat removal system shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any loss-of-coolant accident.*[5]

It is interesting to note that, while the criterion indicates *any loss-of-coolant accident*, only those loss-of-coolant accidents considered in Chapter 15 of the Safety Analysis Report are actually considered. For example, the containments are not specifically designed for Reactor Vessel Rupture or Steam Generator Rupture. Generally, one of the most limiting Chapter 15 accidents is the large break Loss-Of-Coolant Accident (LOCA). The large break LOCA tends to produce both higher pressures and more fission products in containment than the other Chapter 15 accidents. Main Steam Line Breaks tend to produce the highest temperatures in containment and determine the temperature design limits.

Section 2.1 discusses the calculations involved in analyzing a Chapter 15 accident, including the significant conservatisms. Figures 4.1-10, 4.1-11, and 4.1-12 depict containment pressure, temperature and energy balance results for PWR design-basis LOCAs in a large dry containment. Figure 4.1-10 shows the calculated containment pressures resulting from a spectrum of postulated reactor coolant system pipe breaks. For this set of calculations the maximum containment pressure of 50.21 psig (346 Kpa) occurs for an 8 ft^2 (.74 m^2) reactor coolant pump discharge line break. Figures 4.1-11 and 4.1-12 provide more detail for this particular accident. In this accident, the blowdown takes approximately 25 seconds. Despite the fact that the blowdown occurs with no containment cooling systems operating, the peak pressure does not occur during this period. The reflooding of the core, which includes core flood tank injection at 15.3 seconds and emergency core cooling at 26 seconds, generates additional steam which continues to pressurize containment until about 918 seconds, when the peak pressure is reached. In this calculation, which can vary for other plants, a containment cooler is started at 43 seconds and the sprays are started at 67 seconds, providing some positive reduction in the peak pressure. After 918 seconds, the pressure declines, and recirculation cooling from the sump is established at 3500 seconds.

While the large break LOCA presents the most significant design-basis accident pressure challenge for containment designers, there are other types of loads that must be considered in the design.[6] These loads include:

1. Temperature transients and gradients
2. Safe shutdown earthquake loads
3. Internal and external missiles
4. Mechanical loads from pipe rupture
5. External pressures
6. Winds and tornadoes

Section 2.1.4 described the design basis for seismic and other external events. Thermal transients and gradients could conceivably lead to stresses and cracks or tears in the containment. Missiles can come from many sources, including control rod ejection, shrapnel from a failed pipe, or aircraft impact. When a pipe ruptures, the resulting forces on the piping could cause failure at the point where the piping penetrates the containment. External pressures (and buoyant forces) can result due to external increases in barometric pressure or internal drops in pressure resulting from internal cooling or inadvertent spray operation.

In practice, it is impossible to design and construct a perfect containment, that is, one that has zero leakage over the range of postulated accident conditions. Therefore, nonzero design leakage rates are established that are intended to be as low as can be reasonably achieved and that will keep the offsite exposures below the dose guidelines established in 10 CFR 100.[7] These design leakage rates can be site and plant specific, because the offsite doses are affected by the site geometry and the local meteorology, as well as the reactor type. However, some plants simply use standard technical specifications that are more stringent than a site-specific analysis would allow.

Leakage from a containment structure can occur due to failure of the containment structure, failure of penetrations through the structure, and failure of isolation valves. Penetrations through the containment structures include piping penetrations, electrical penetrations, hatches and airlocks. Isolation valves are provided on all pipes and ducts that penetrate the containment. Normally, two isolation valves are provided for each line, with the isolation valves consisting of locked closed or automatic isolation valves. Requirements for these isolation valves are contained in 10 CFR 50, Appendix A, General Design Criteria 54 through 57.[8]

Containment leakage rates are determined in the Safety Analysis Report and Technical Specifications. Table 4.1-2 provides some examples of design leakage rates. The higher allowed leakage rates for the pressure suppression containments is a result of their smaller volumes. Assuring that the design leakage rates are met is a complex process involving a variety of tests. Criteria for testing containment leakage are set forth in 10 CFR 50, Appendix J.[9] Generally, three types of tests are performed to assure that leakage remains within design limits:

1. Type A tests - tests of the overall integrated leakage rate,
2. Type B tests - tests to detect local leaks around containment penetrations, and
3. Type C tests - tests to measure containment isolation valve leakage rates.

The leakage is difficult to measure to the required precision, and changes to these requirements have been considered.

The amount of leakage from a containment is a function of the length of time that the containment remains pressurized. Further, there are some postulated accidents in which energy may be added to containment for many hours or even days. Therefore, the NRC has established requirements for containment heat removal. These requirements are contained in 10 CFR 50, Appendix A, Criterion 38.[10] Containment heat removal systems may involve sprays, fan coolers, suppression pool cooling, or emergency core cooling recirculation cooling and must meet the single failure criterion.

4.1.3 Containment Failure Modes

In the event that a containment does fail, the manner in which it fails can have a significant impact on offsite releases. If a containment leaks slowly, then large fractions of the radionuclides may still be retained inside the containment or surrounding buildings, depending on where the leak occurs. Retention can result from gravitational settling of radioactive aerosols inside the containment or surrounding buildings or from sprays or other systems removing the radionuclides from the containment atmosphere. The effectiveness of these processes depends upon the residence time of the radionuclides in containment. Conversely, a large rupture of the containment can lead to rapid transport of radionuclides to the environment with minimal retention.

The containment failure mode that occurs depends upon the containment design and the particular phenomena that cause the failure. Particular severe accident phenomena (including those beyond the design-basis) will be discussed in later sections; however, the challenges that they produce include:

1. Overpressure
2. Dynamic pressures (shock waves)
3. Internal missiles
4. External missiles
5. Meltthrough
6. Bypass

Overpressure can theoretically lead to either leakage or large rupture in any type of containment. Overpressure can result from several different causes, as discussed in later sections. As a containment is pressurized, it begins to deform. These deformities can lead to leakage around penetrations in the containment or to tearing of the steel liner (in concrete containments). Based on recent studies, leakage is considered the more likely outcome for concrete containments.[11] The concrete structure is unlikely to rupture as a result of pressure challenges (even if the steel liner tears), but rather is more likely to crack. Steel containments are susceptible to rupture in the event that the penetrations do not leak and the containment continues to pressurize. Given sufficient pressure, a crack in a steel containment can propagate catastrophically. Generally, assuming that early penetration leakage does not occur, steel containments have a larger margin between the design and ultimate failure pressures than concrete containments.

Shock waves and missiles can potentially cause large holes in the containment. However, the containments are designed for the most credible external missiles, such as tornado-driven missiles, and some types of internal missiles, such as control rod ejections. Missiles or shock waves resulting from hydrogen detonations or steam explosions are a possible threat that will be discussed in more detail later.

There are two basic types of meltthrough to consider. First is the possibility of basemat meltthrough (the China Syndrome). In this case, following vessel failure, the molten material melts through the basemat over a period of hours or days and vents the containment through the surrounding soil. This failure mode is not generally catastrophic, because of the long time available for emergency response actions and the possibility of some retention in the soil. The second type of meltthrough is most applicable to Mark I BWR and some Mark II BWR containments. In this case, molten material can exit the area beneath the reactor and flow across the floor, directly contacting the steel liner and causing it to fail. This type of failure can happen much more quickly than basemat meltthrough and can lead to more serious consequences. A similar scenario may be possible for PWR ice condenser containments, if debris is blown out of the reactor cavity near the seal table.

There are two other types of containment failure that can lead to severe consequences: (1) containment bypass and (2) isolation failure. Containment bypass involves failure of the reactor coolant system boundary in such a manner that a path is created to the outside without going through containment.

Bypass involves failures in the reactor coolant pressure boundary separating high pressure and low pressure systems. Normally, this involves the failure of at least two valves. For example, the valves separating the primary system from the Residual Heat Removal (RHR) system may fail, thus putting high pressure into the RHR system. Because the RHR system is normally constructed with low pressure piping and components, it may fail outside containment, providing a direct path from the core to the outside. In PWRs, steam generator tube ruptures provide an additional source of containment bypass. Primary system pressure will lift the relief valves on the secondary side, with the potential for stuck-open valves to provide the path to the atmosphere.

Containment isolation failure involves failure of the containment isolation function as a result of containment isolation valve failures or other openings in the containment boundary external to the reactor coolant system. These failures may be the result of preexisting leaks or the failure of isolation valves to close upon demand. The failures are more related to system and procedural malfunctions, rather than severe accident phenomena. In this case, the containment has no chance to function and fission products have a direct path outside to the atmosphere. Isolation failures are extremely unlikely in Mark I and II BWRs because of their inerted containments that make large leaks easily detected. Similarly, isolation failures are unlikely in PWR subatmospheric containments.

Table 4.1-1. Number of U.S. Containments of Each Type*

CONTAINMENT TYPE	NUMBER
PWR Large Dry	61
PWR Subatmospheric	7
PWR Ice Condenser	8
BWR Mark I	24
BWR Mark II	9
BWR Mark III	4

*data taken from the following reports:
Integrated Leak Rate Test Report for Peach Bottom Unit 3, March 18, 1992.
Integrated Leak Rate Test Report for LaSalle Unit 1, March 12, 1992.
Integrated Leak Rate Test Report for Grand Gulf Unit 1, August 4, 1989.
Integrated Leak Rate Test Report for Sequoyah Unit 2, February 19, 1985.
Integrated Leak Rate Test Report for Surry Unit 2, September 3, 1991.
Integrated Leak Rate Test Report for Zion Unit 1, July 5, 1988.

Table 4.1-2. Examples of Design Leakage Rates (Integrated Leakage)

PLANT	CONTAINMENT TYPE	PEAK DESIGN-BASIS ACCIDENT PRESSURE psig (Kpa)	MAXIMUM ALLOWABLE LEAKAGE (weight %/day)
Peach Bottom	BWR Mark I	49.1 (339)	0.5
LaSalle	BWR Mark II	39.6 (273)	0.635
Grand Gulf	BWR Mark III	11.5 (79)	0.437
Sequoyah	PWR Ice Condenser	12 (83)	0.25
Surry	Subatmospheric	45 (310)	0.1
Zion	Large Dry	47 (324)	0.1

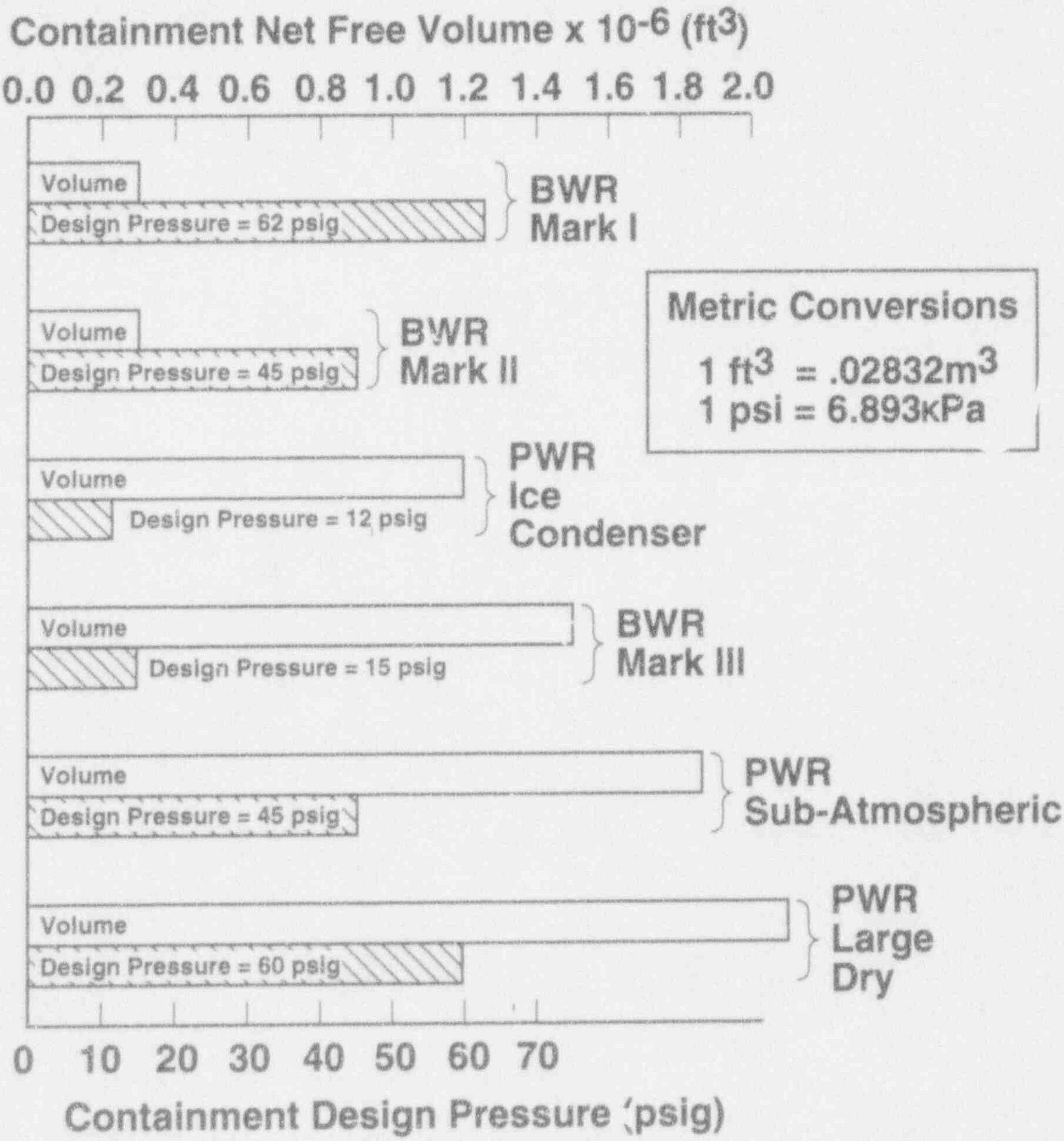


Figure 4.1-1 Typical containment volumes and design pressures

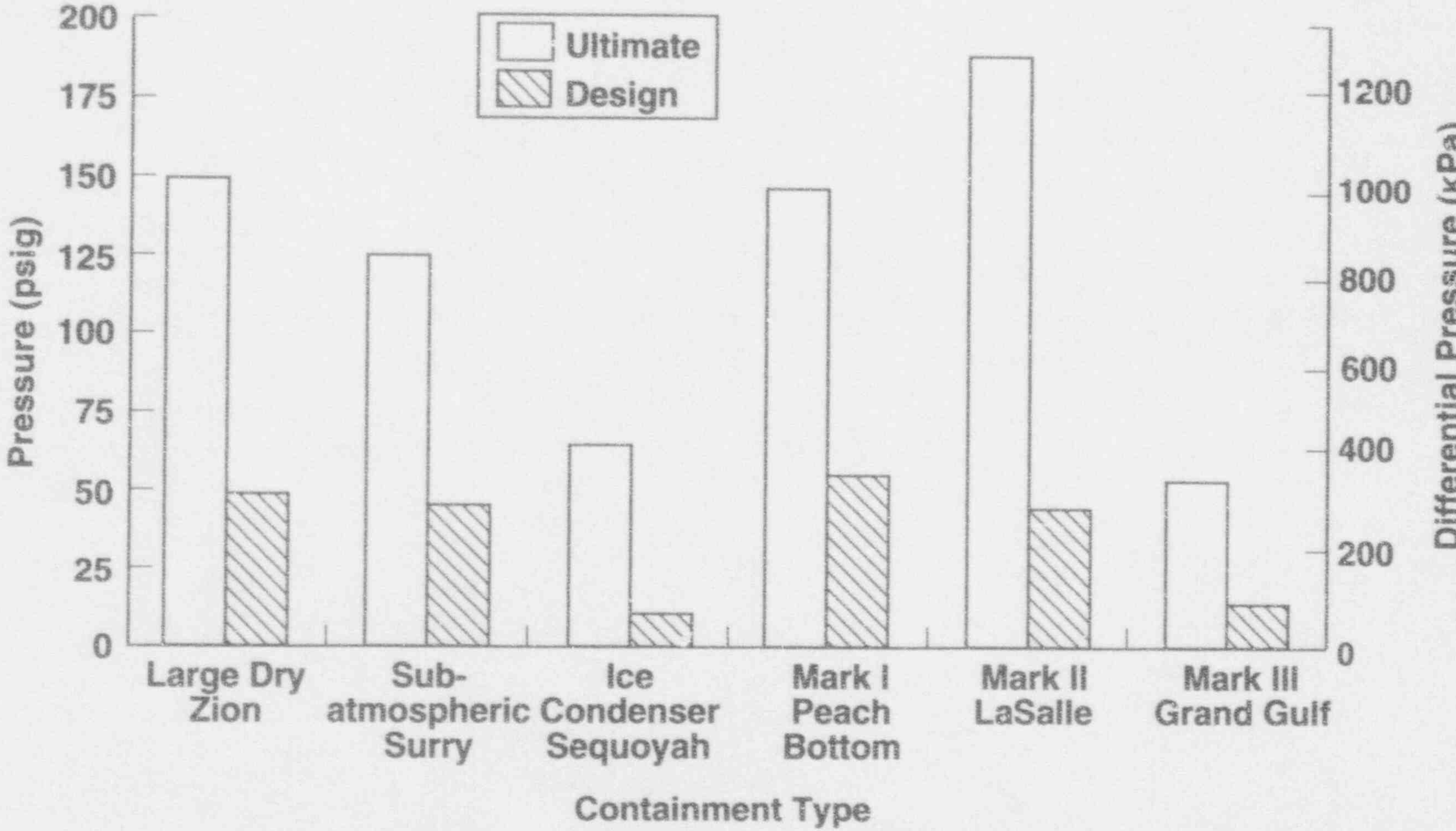


Figure 4.1-2 Comparison of design pressures to ultimate failure pressures

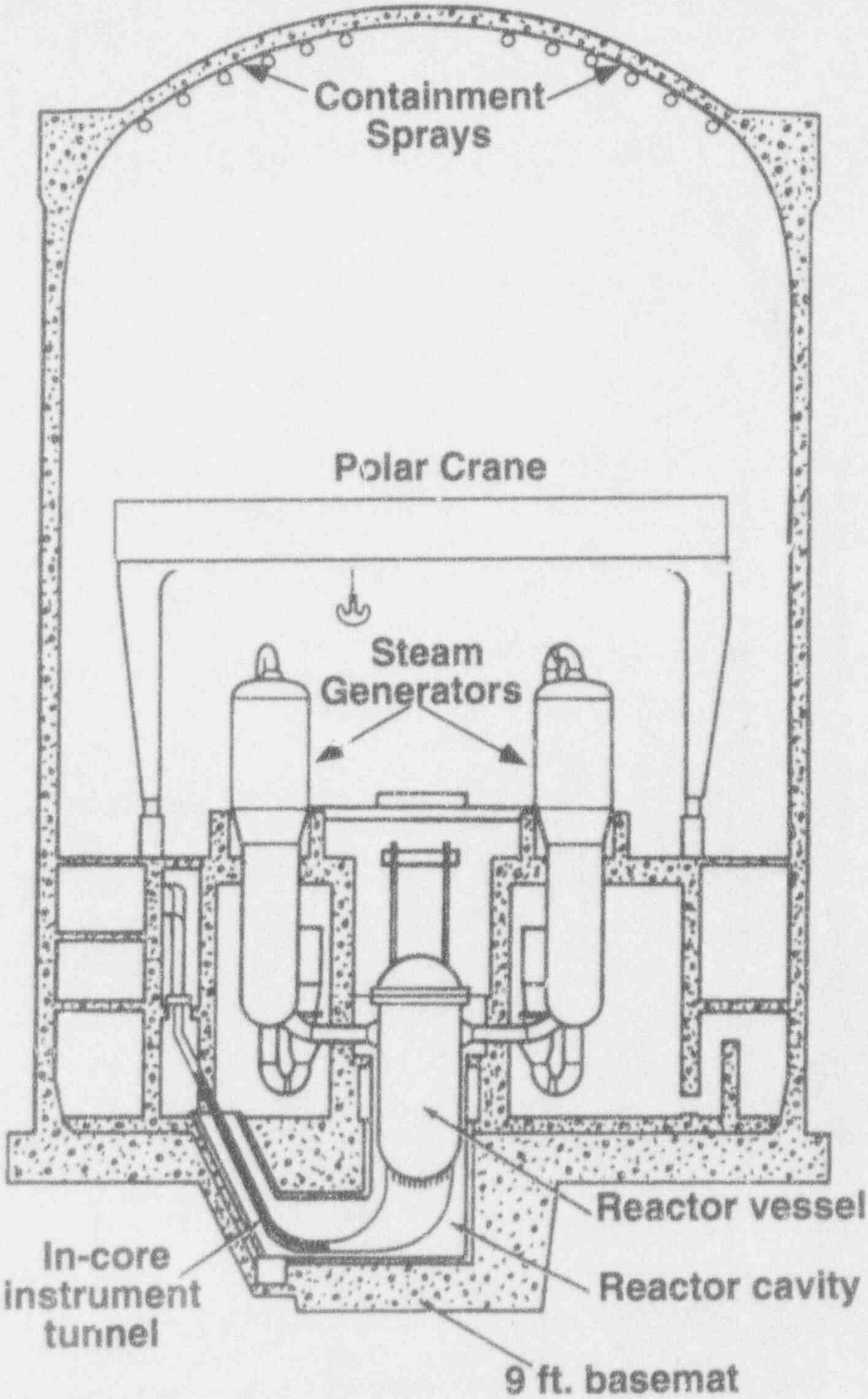


Figure 4.1-3 Typical large dry containment

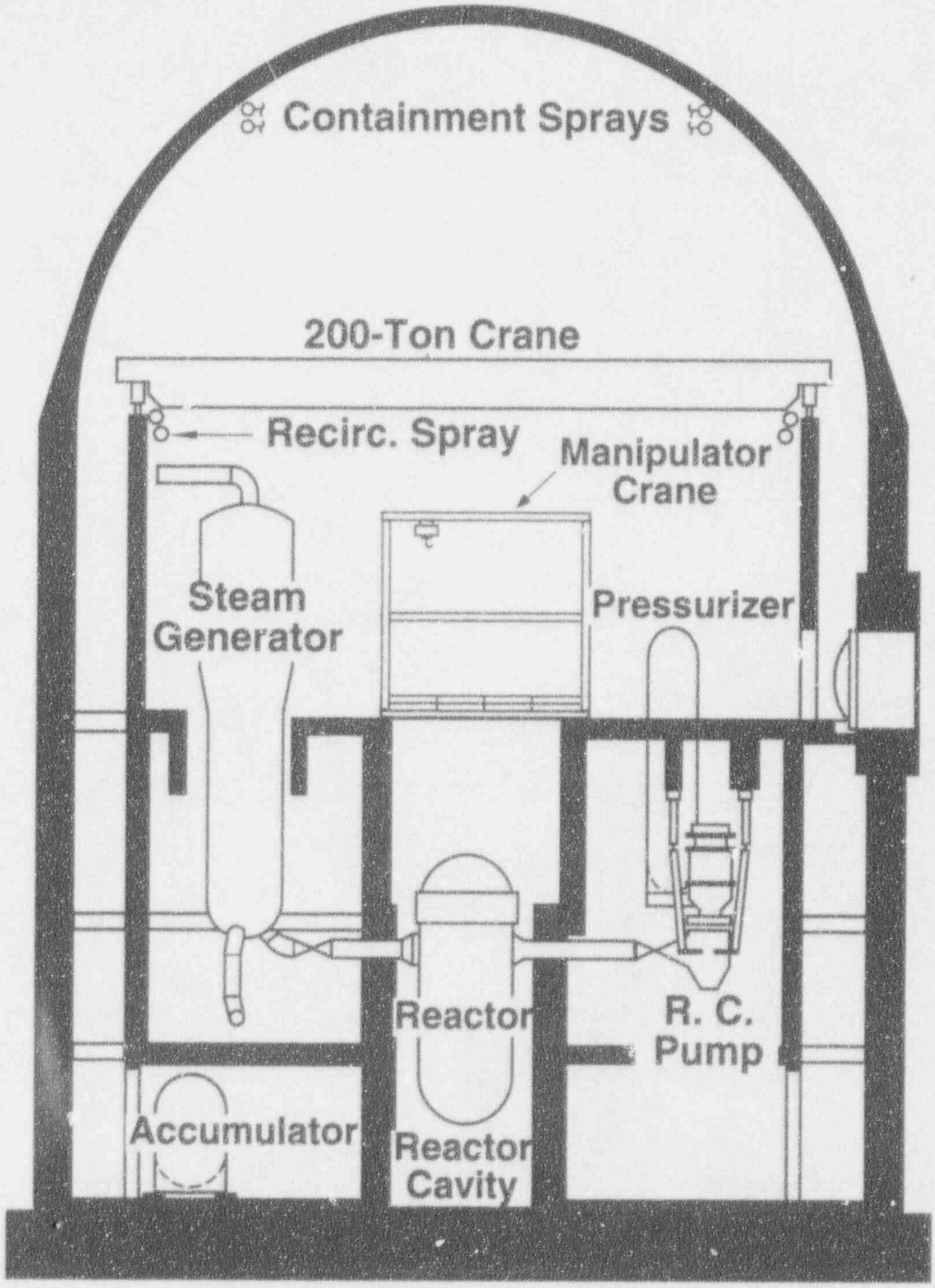


Figure 4.1-4 Typical subatmospheric containment

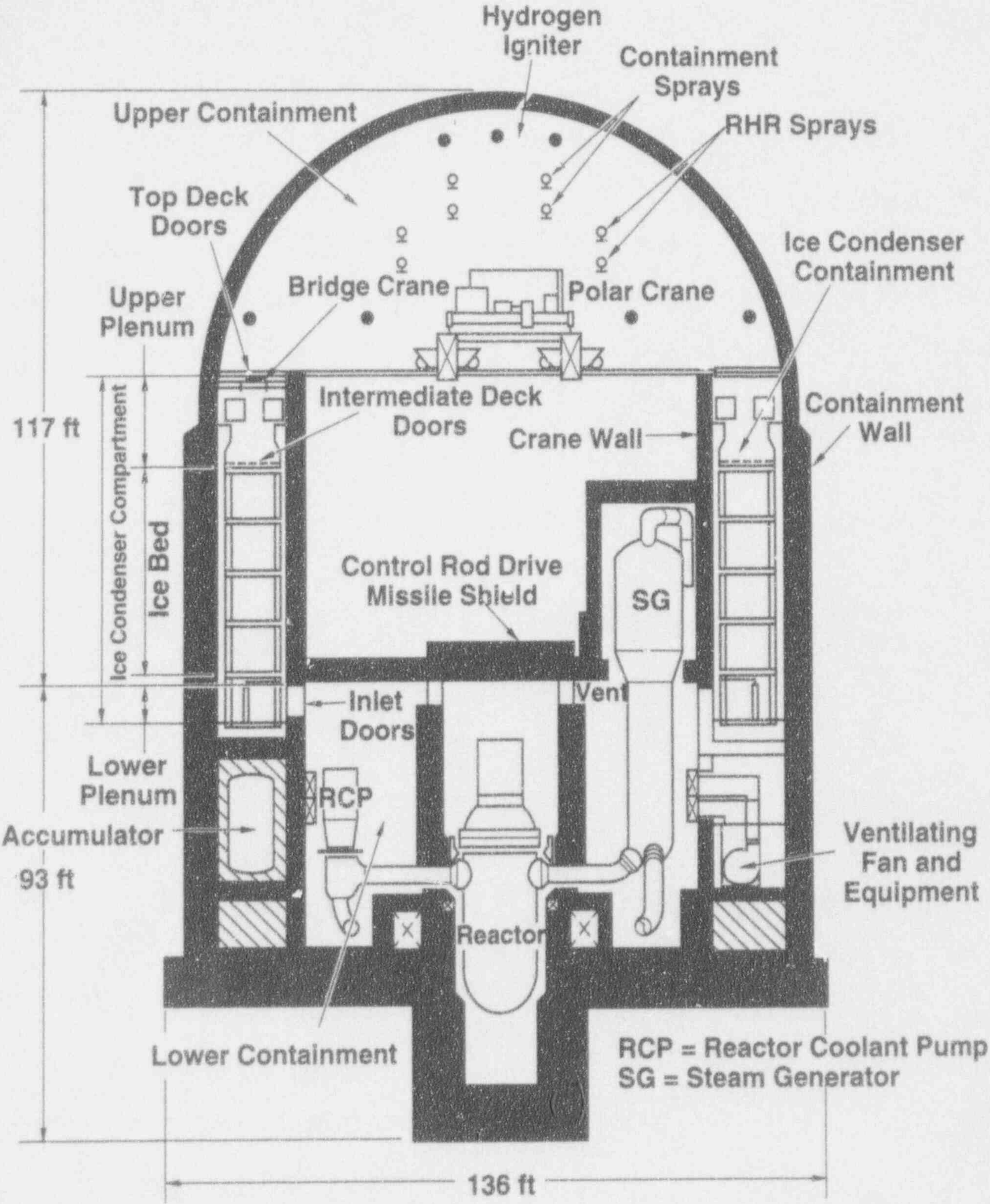


Figure 4.1-5 Typical ice condenser containment

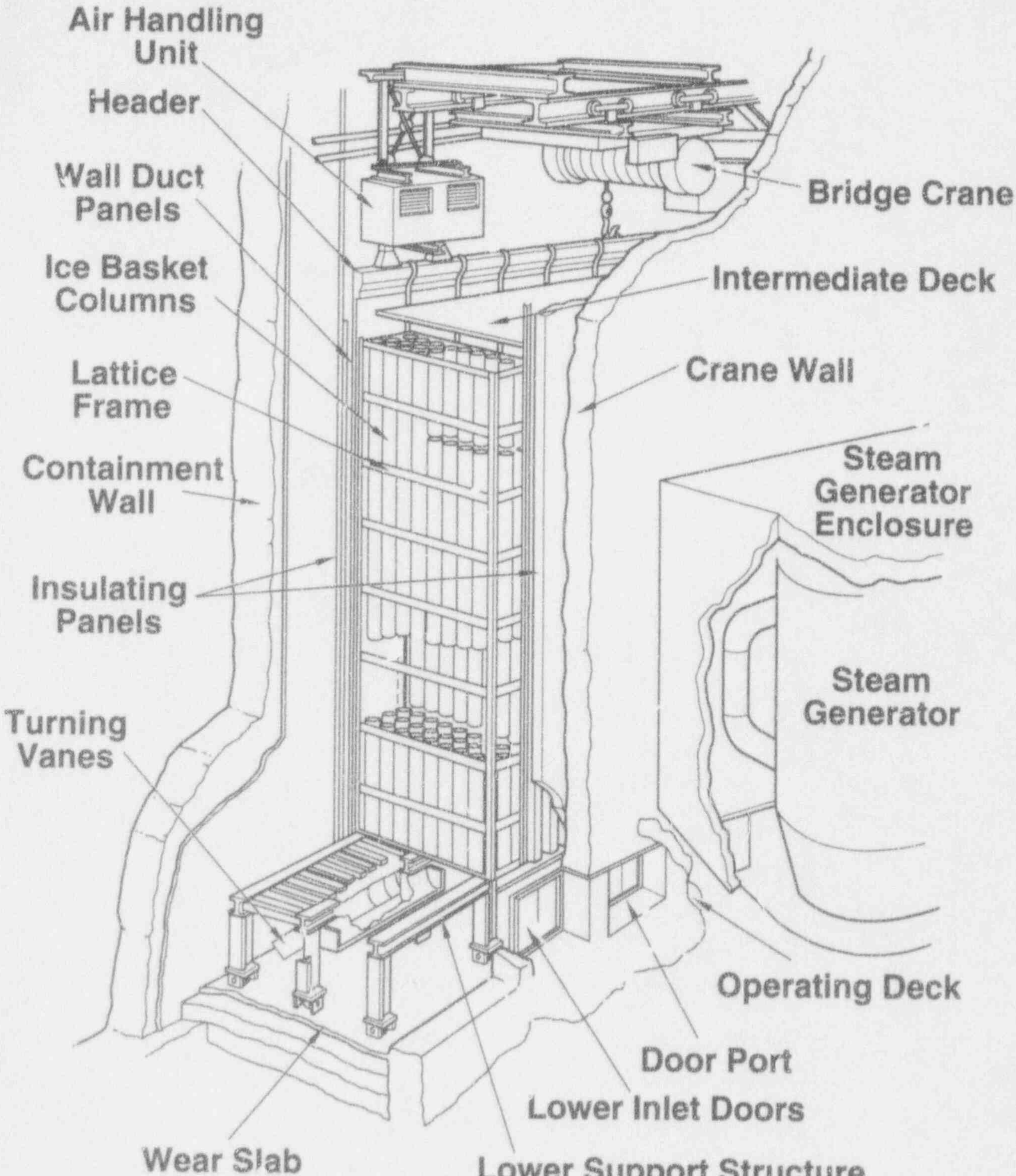


Figure 4.1-6 Ice condenser cutaway

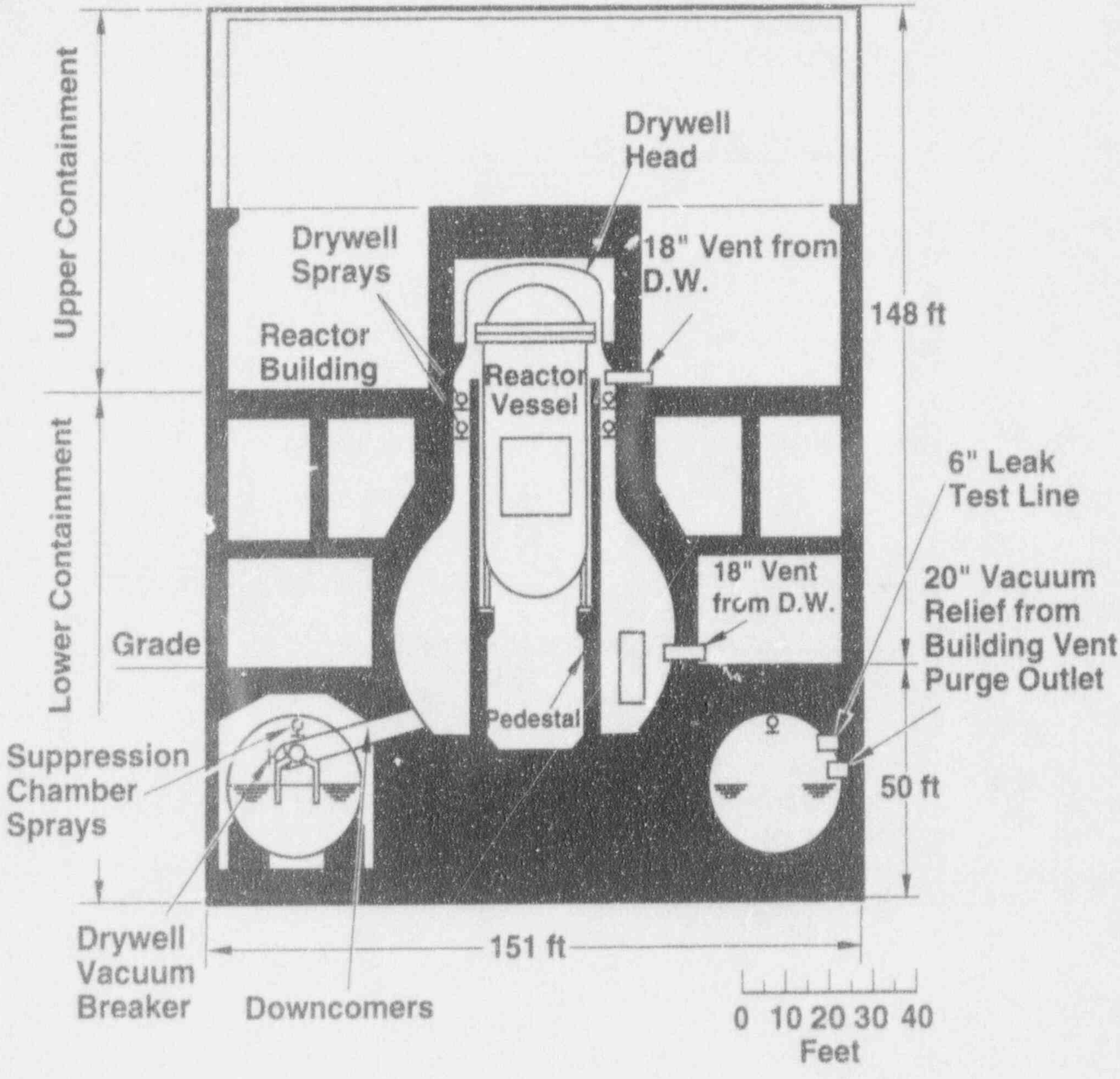


Figure 4.1-7 Typical BWR Mark I containment

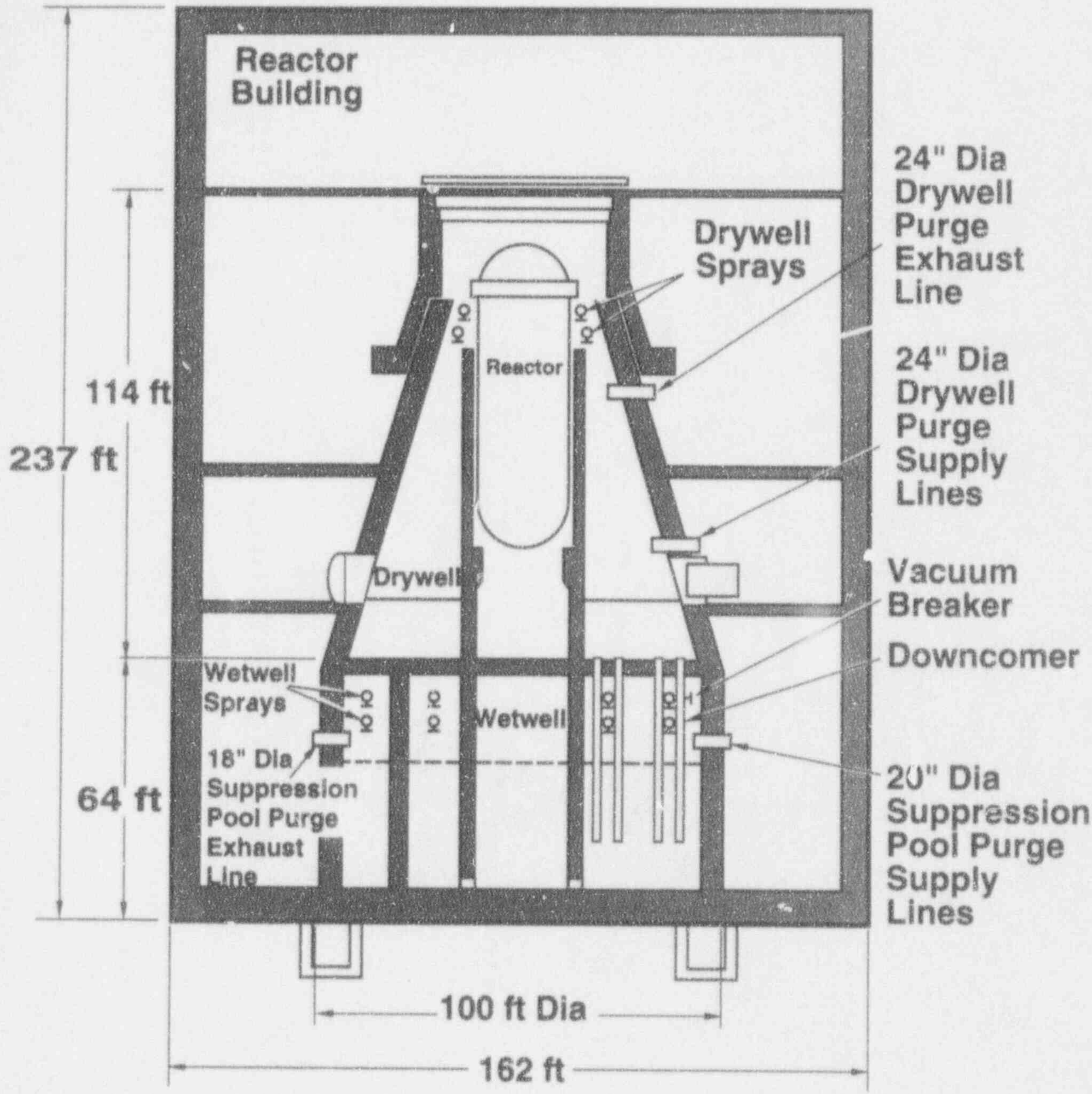


Figure 4.1-8 Typical BWR Mark II containment

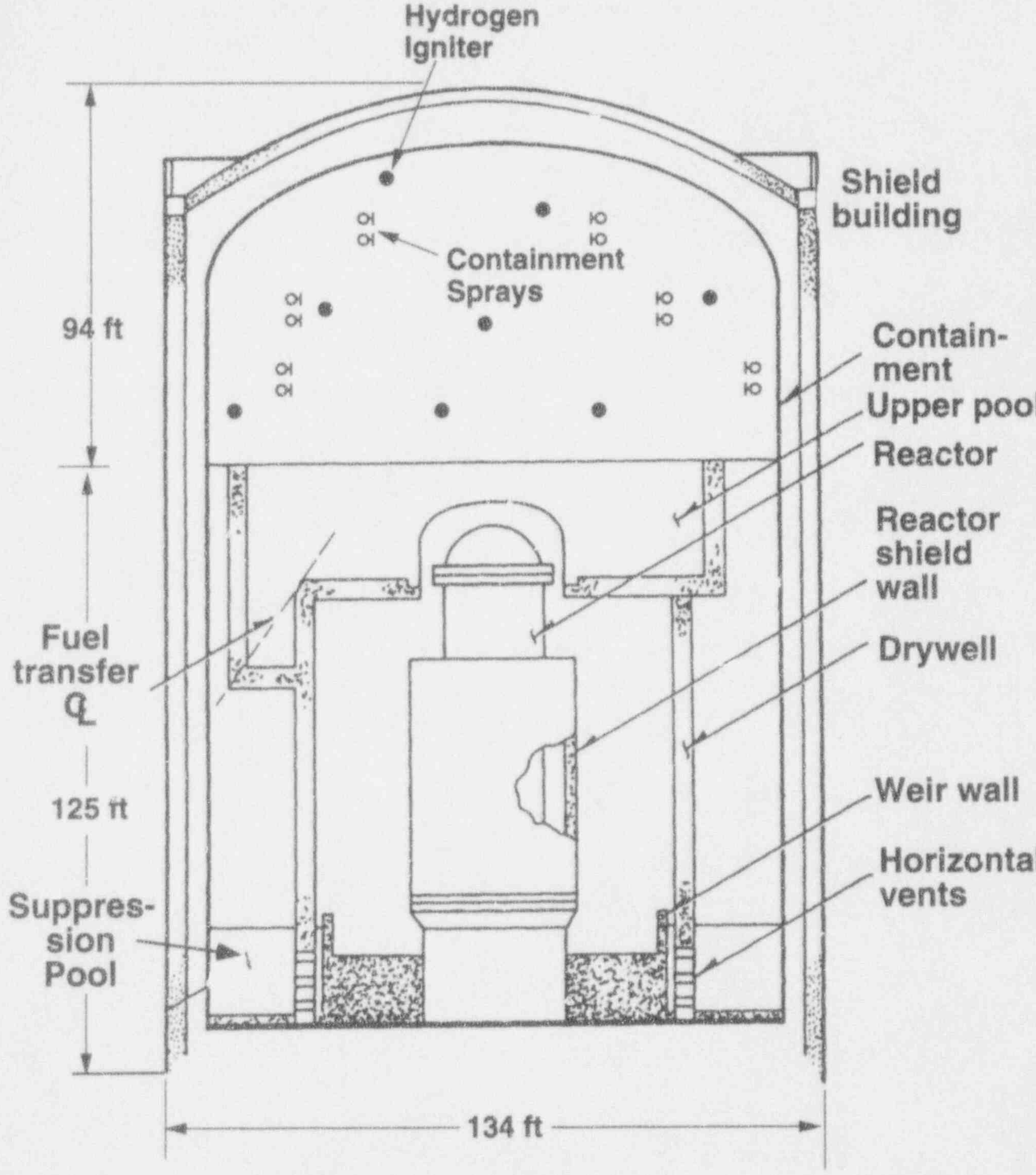


Figure 4.1-9 Typical BWR Mark III Containment

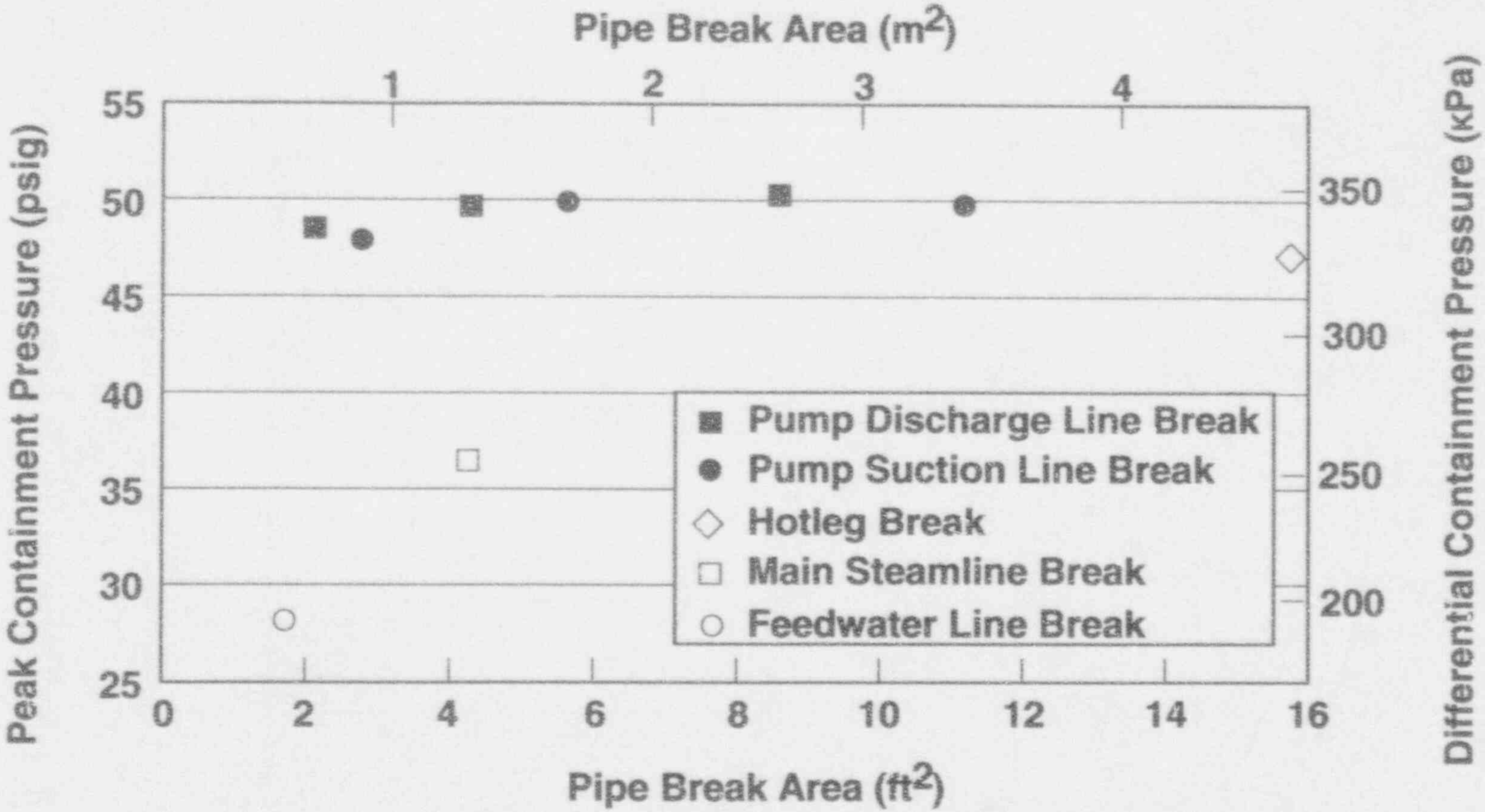


Figure 4.1-10 Peak containment pressure for one PWR

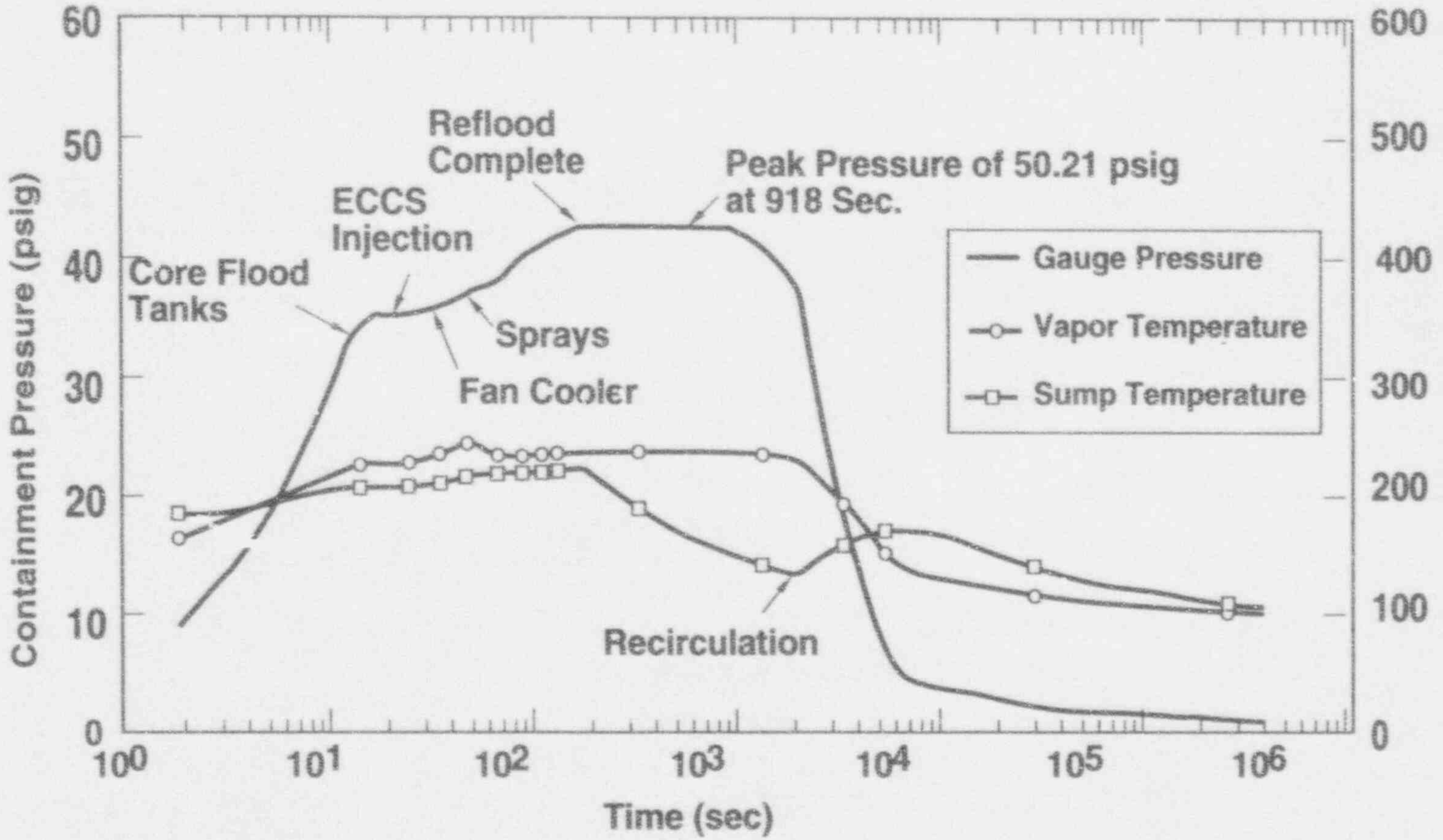


Figure 4.1-11 Containment pressure-temperature response for 8.55 ft^2 pump discharge break

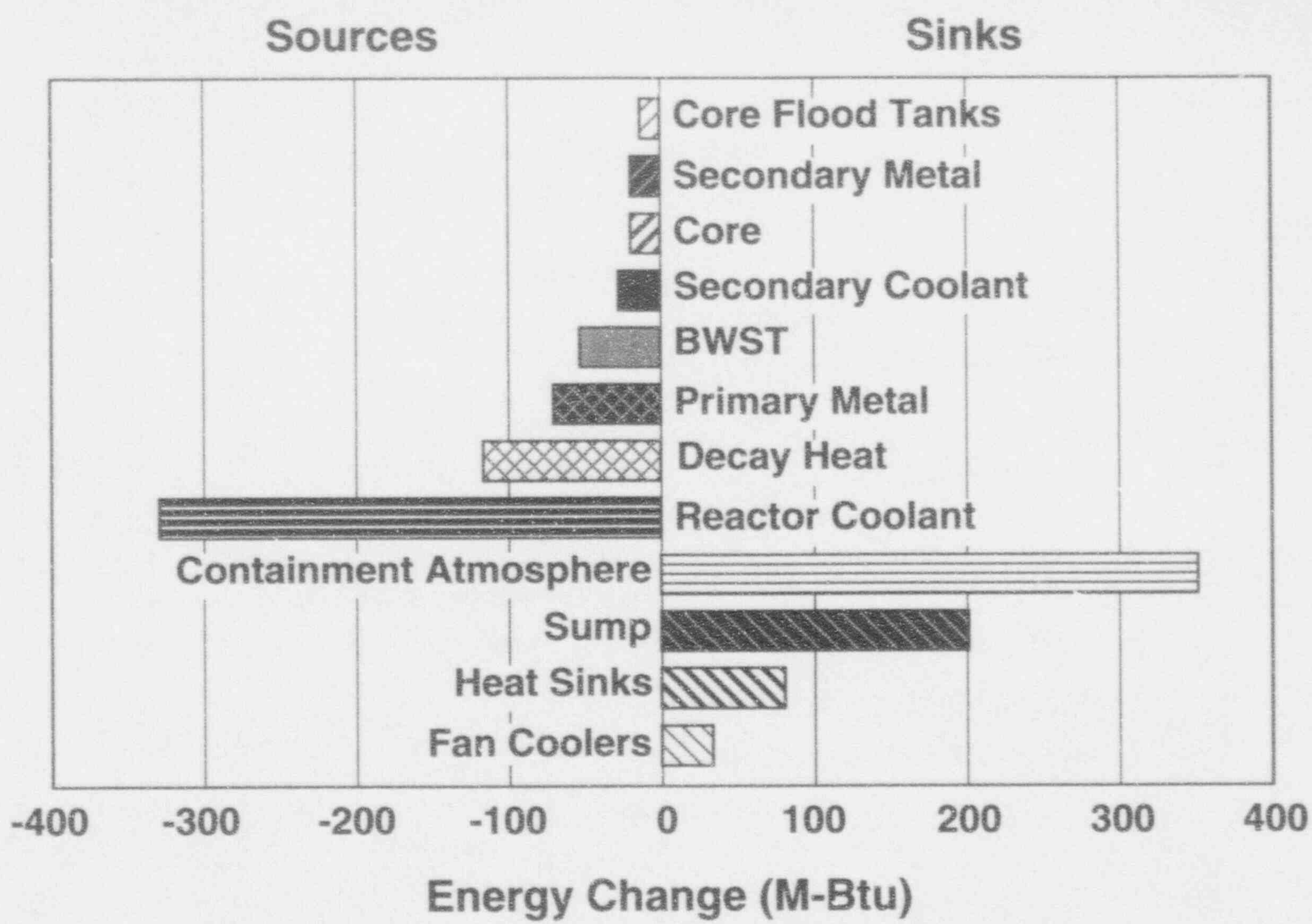


Figure 4.1-12 Energy changes up to time of peak containment pressure for one PWR

References for Section 4.1

1. NRC Information Digest, 1991 Edition, NUREG-1350, Vol. 3.

2. A. L. Camp, et al., *Light Water Reactor Hydrogen Manual*, NUREG/CR-2726, SAND82-1137, Sandia National Laboratories, August 1983.

3. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

4. T. D. Brown, et al., *Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant: Phenomenology and Risk Uncertainty Evaluation Program (PRUEP)*, NUREG/CR-5305, SAND90-2765, Sandia National Laboratories, 1992.

5. *Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 50*, U.S. Government Printing Office, January 1, 1991.

6. Kenneth C. Lish, *Nuclear Power Plant Systems and Equipment*, Industrial Press Inc., 200 Madison Avenue, New York, NY, 1972.

7. *Title 10, Code of Federal Regulations, Part 100*, U.S. Government Printing Office, January 1, 1991.

8. *Title 10, Code of Federal Regulations, Part 50, Appendix A*, U.S. Government Printing Office, January 1, 1991.

9. *Title 10, Code of Federal Regulations, Part 50, Appendix J*, U.S. Government Printing Office, January 1, 1991.

10. *Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 38*, U.S. Government Printing Office, January 1, 1991.

11. R. J. Breeding, et al., *Evaluation of Severe Accident Risks: Quantification of Major Input Parameters*, NUREG/CR-4551, Vol.2, Rev. 1, Part 3, March 1992.

4.2 Containment Response to Beyond-Design-Basis Accidents

As discussed in Section 4.1, containments are not likely to fail from the loads resulting from design-basis accidents. In fact, there are very large margins between the pressures resulting from design-basis accidents and predicted ultimate failure pressures. However, the China Syndrome and the Reactor Safety Study made it clear that more severe challenges to containment were possible.[1,2] In fact, it appeared that public risk was probably dominated by accidents in which substantial core damage occurred and the containment failed or was bypassed. The TMI-2 accident further emphasized the importance of phenomena, such as hydrogen combustion, that could accompany severe accidents. This section provides some general perspectives on the vulnerabilities of containments to severe accident phenomena. Isolation failures and bypass were addressed in Section 4.1. Later sections will describe key severe accident phenomena in more detail.

4.2.1 Containment Challenges and Timing of Events

Severe accident challenges to containments can occur during three time regimes:

1. Prior to reactor vessel failure,
2. At or soon after reactor vessel failure, or
3. Long after reactor vessel failure.

Table 4.2-1 summarizes the time regimes and their associated containment challenges. Prior to vessel failure, there are three types of containment pressure loads that can occur. The first type of load is simply the pressure loads that result from the initial reactor coolant system blowdown and subsequent steam and hydrogen releases due to reflooding. For design-basis accidents, these loads are not a threat; however, containments are not designed to withstand the loads that may occur during some severe accidents resulting from the rupture of a reactor vessel or steam generator. As of early 1992, there have been no definitive studies concerning the likelihood of containment failure from such events; fortunately, the frequency of such events is estimated to be very small.

A second type of load that can occur prior to vessel breach involves the failure of containment heat removal systems to cope with the ongoing mass and energy additions to the containment even though core cooling is successful. This problem can occur in many ATWS sequences or in loss-of-coolant accidents or transients in which containment heat removal systems fail. In the latter cases, the design pressure may be exceeded early, but the ultimate failure pressure would not be reached for many hours or even days. In fact, some containments may not fail at all, if the heat losses through the structure can eventually match the decreasing decay heat load. If the containment does fail, then there is the potential for the loss of core cooling as a result of several phenomena, including:

1. Loss of net positive suction head (NPSH) to pumps that are recirculating water from a sump or suppression pool,
2. Failure of piping as a result of the containment failure, or
3. Failure of components in the reactor building of a Mark I or Mark II BWR when steam enters the surrounding reactor building following containment failure.

If core damage results from one of these phenomena, then the accident will proceed in a containment that is already failed.

The third phenomena that can cause failure prior to vessel breach is hydrogen combustion. Hydrogen will be generated during the core heatup and meltdown phase due to zirconium-steam reactions. If a significant amount of this hydrogen is released through relief valves (as at TMI-2) or through a pipe break, then combustion prior to vessel breach can threaten the containment. Hydrogen combustion is discussed in more detail later in this module.

The second time phase of interest, and the one that is often most threatening to containment, is the phase that occurs at or soon after vessel breach. When vessel breach occurs, there are several phenomena that can ensue, sometimes acting simultaneously. Those phenomena include:

1. Steam spike
2. Steam explosion
3. Direct containment heating
4. Hydrogen combustion
5. Liner meltthrough (Mark I BWR)
6. Downcomer failure (Mark II BWR)

Steam spikes or explosions can occur if there is water in the reactor cavity or pedestal region below the reactor vessel. In-vessel steam explosions and α-mode failures were addressed in module 3. This water may be present as a result of leakage from the reactor coolant system, the operation of containment sprays, or melted ice in an ice condenser containment. By themselves, steam spikes are unlikely to threaten containment, unless the containment is already substantially pressurized. The amount of mass and energy added to the containment atmosphere is determined by the amount of water converted to steam as the melt is quenched in the water. If a steam explosion occurs, then shock waves may cause damage to the containment structure or the vessel supports. If the vessel supports fail and the vessel moves significantly, then containment failure may result around the piping penetrations. In some BWRs, steam explosions could lead to suppression pool bypass, possibly resulting in eventual overpressurization of the containment. Steam explosions are discussed more in a later section.

Direct Containment Heating (DCH) involves the ejection of the melt from the vessel at high pressure, thus spraying the molten material into containment. With the melt broken up into small particles, rapid heat transfer to the containment atmosphere can occur, most likely accompanied by the chemical energy associated with oxidation of metals in the melt. This "direct heating" has the potential to transfer more energy to the containment atmosphere than a steam spike and provides a more significant threat to containment.

When the reactor vessel fails, any hydrogen contained in the reactor coolant system will be released to containment, and additional hydrogen may be generated as a result of chemical reactions accompanying steam spikes, steam explosions, or direct containment heating. This hydrogen may burn immediately if oxygen is present, particularly if the molten material provides an ignition source or the hydrogen is already at very high temperatures. Hydrogen combustion at vessel breach may directly threaten containment or may threaten containment in combination with one or more of the other phenomena that can occur.

A phenomenon of importance for Mark I BWRs is shell (liner) meltthrough. At vessel breach, the molten material may flow out of the pedestal region, across the drywell floor and then directly contact the steel liner, causing failure. The likelihood of this event may be reduced if there is a substantial amount of water on the drywell floor.

A phenomenon of importance for Mark II BWRs is downcomer failure. While Mark II designs vary significantly, there is often the potential for molten material to flow across the floor and into the downcomers. This molten material may directly fail the downcomer or, possibly, lead to a steam explosion that fails the downcomer. Downcomer failure does not lead to immediate containment failure; however, the suppression pool is bypassed, thus negating its heat removal and fission product scrubbing capabilities.

The third time phase of interest is the late phase, hours or more after vessel failure. The late phase threats consist primarily of high temperature, overpressure, basemat meltthrough, and hydrogen burns. High temperature and long term overpressure can result if containment heat removal systems are inoperative. In a BWR, high drywell temperatures can result even if the suppression pool cooling systems are working. With most of the core materials now present in the containment, the decay heat must be removed somehow to prevent temperature and pressure buildup. High temperatures can result in weakened structures that may leak more than expected or fail at pressures lower than the expected ultimate failure pressure. The problem is exacerbated by noncondensible gases that can be generated by core-concrete interactions. These noncondensible gases contribute to the overall pressure.

Basemat meltthrough is a long term result of core-concrete interactions. These interactions can generate hydrogen and other noncondensible gases, generate copious amounts of radioactive and nonradioactive aerosols, and eventually fail the basemat. Core-concrete interactions will be discussed in more detail in a later section.

Hydrogen burns can also occur during the late phase. In some cases this may involve hydrogen that was present previously, but did not burn due to the lack of an ignition source or an excess of steam in the atmosphere. If steam is removed late in an accident, for example due to recovery of sprays, a gaseous mixture that was inert may become flammable. Another factor affecting hydrogen burns is the amount of flammable gases (hydrogen and carbon monoxide) being generated from core-concrete interactions. These additional gases can lead to burning late in an accident.

Section 4.2.1 has summarized the time phases of an accident and the phenomena that occur during those phases. Section 4.2.2 will now discuss estimates of containment failure probabilities as a result of those particular phenomena.

4.2.2 Implications of Containment Failure

The significance of containment failure depends upon the particular accident sequence, the mode of containment failure and the timing of radioactive releases. Module 5 will address the importance of the timing of releases relative to warning times and evacuation speeds. The importance of accident sequence type and containment failure mechanisms are discussed briefly below.

Containment failure can only represent a significant concern if radionuclides are released from the fuel and the reactor coolant system. If fuel melting does not occur and only the activity in the reactor coolant and the radioactive gases in the fuel pins (gap release) are released, then the consequences will be minimal even if containment failure occurs.

If fuel melting does occur and a significant amount of radionuclides is released to containment, then the timing and mode of containment failure are critical factors in determining the offsite consequences. Generally, the most severe failure modes are ones that occur early in time (before or during reactor vessel failure) and involve little retention of radionuclides in the containment. Radionuclides can be retained in containment in a number of ways:

1. Scrubbing in suppression pools,
2. Scrubbing by containment sprays,
3. Retention in an ice condenser,
4. Gravitational settling and other atural processes,
5. Trapping along tortuous release paths.

Most of these retention mechanisms are affected by the time available for the mechanism to work. Small containment leaks allow more time for settling and scrubbing by sprays. Therefore, ruptures are more likely to lead to severe consequences than leaks. If the radionuclides can be mostly retained until after evacuation occurs, then many of the health effects can be substantially reduced. Also, failures that lead into surrounding buildings allow further opportunities for retention.

Module 5 will discuss the offsite consequences of particular accident types in more detail. However, the importance of containment failure can be summarized by stating that the worst failures are failures (or bypasses) that occur early and allow rapid, unscrubbed transit of radionuclides out of the containment.

4.2.3 Likelihood of Containment Failure During Severe Accidents

The most comprehensive study of containment failure probabilities is contained in the NUREG-1150 documents.[3] Despite the fact that severe accidents provide challenges beyond the design-basis, NUREG-1150 (and other related studies) show that containments have the capacity to withstand many of these accidents. This capability is a result of the very conservative design process that provides substantial margin with respect to less severe design-basis accidents.

The actual containment failure probability depends upon several factors, including the particular containment design and accident sequence. The containment failure frequency is determined from:

$$CFF = \sum_{i=1}^{n} S_i C_i$$

where CFF is the containment failure frequency,

S_i is the frequency of accident sequence i,

C_i is the conditional probability of containment failure given accident sequence i,

and

n is the total number of accident sequences.

Because S_i and C_i depend on the particular accident sequences, the containment failure frequency can be significantly different for two plants with identical containments.

Figure 4.2-1 shows the relative probability of different containment failure modes, given a core damage accident, for the five plants evaluated in NUREG-1150. In this figure, early failures include failures that occur before, at, or soon after vessel breach. Note that many of the containment failures at Grand Gulf, which has a Mark III containment, involve failure of the outer containment with the drywell and suppression pool remaining intact. Therefore, the containment failures for Grand Gulf do not all lead to significant radiological releases.

With the caveat noted above for Grand Gulf, the failures that most impact public risk are the early failures and the bypass events. Figure 4.2-2 shows the frequency of such events for the five NUREG-1150 plants. This figure, which considers only internally initiated accidents, accounts for the variation in accident frequency and type in estimating the containment failure frequency. As noted in Module 2, Grand Gulf has a substantially lower core damage frequency than Sequoyah, and this is reflected in a lower containment failure frequency, even though Grand Gulf has a higher probability of early failure **given** an accident.

Section 2.7.4 discussed the large release safety goal and the possible use of early containment failure frequency as a surrogate for the large release frequency in making backfitting decisions. Figure 4.2-2 shows that the NUREG-1150 plants would not meet the 10^{-6} frequency goal, based on early containment failure frequency. However, the actual releases will vary widely for each accident, and not all containment failures will result in substantial offsite releases.

4.2.4 Containment Venting Strategies

Containments are somewhat unusual in that they are pressure vessels without safety relief valves. Thus, if containment heat removal is lost, there is no designed-in feature to prevent structural failure. Most containments have penetrations that could conceivably be used to vent the containment and relieve pressure. These penetrations include the lines used for leak rate testing, among others. However, most plants do not have procedures for venting during an accident. There are several reasons for this, including the belief that it is unnecessary, the requirements for AC power for valves, the guaranteed release of radioactive materials, and the potential hazards to personnel involved in the venting process.

Recently, utilities with BWR Mark I and II containments have included venting in their emergency procedures. Venting can be particularly valuable for accident sequences involving the long-term loss of containment heat removal in Mark I and II BWRs. In these sequences, often referred to as TW sequences, core cooling is initially successful. However, the loss of containment heat removal leads ultimately to containment failure. After containment failure, the core cooling systems may fail as a result of the loss of net positive suction head or from the harsh environments due to steam in the reactor building. In some cases, core cooling may fail even before the containment fails. For some plants, high containment pressure can cause the Automatic Depressurization System (ADS) valves to close, leading to the loss of low pressure injection systems. In others, the reactor core isolation cooling system will fail due to high turbine exhaust backpressure. Venting can prevent these problems.

The particular venting procedures vary widely from plant to plant, but include use of leak rate testing lines and lines to the standby gas treatment systems. These plants generally have several possible lines that can be used, ranging in size from two inches to two feet in diameter. Generally, the venting is effective only for long-term loss of containment heat removal sequences. Venting can not occur fast enough to relieve pressure rises frc... energetic events, such as steam explosions or hydrogen burns. Venting is generally not possible during station blackout, due to the requirements for AC power to open the vents and is not adequate to handle the steaming rate from an Anticipated Transients Without Scram (ATWS) event.

As discussed in Section 4.1, vent lines are available from both the wetwell and the drywell in Mark I and II BWRs. Venting from the wetwell is advantageous, because any radionuclide releases can still be scrubbed through the suppression pool. Thus, such venting is more attractive for BWRs than for other designs. A possible negative effect is that venting may lead to a saturated suppression pool, causing loss of net positive suction head to some pumps.

At some plants venting occurs through strong piping. However, in others the venting may involve ductwork and relatively weak gas flow paths. If venting occurs at high containment pressure, this ductwork will fail, releasing steam and possibly hydrogen and noble gases into the reactor building. These gases may lead to failure of safety equipment ..1 the reactor building and exacerbate the accident. Recently, the NRC has reached agreement with owners of

Mark I containments to develop procedures for venting only through hardened piping to alleviate this concern.[4]

A final note concerns venting as it relates to emergency response. Current procedures for venting do not attempt to coordinate venting strategies with orders to evacuate. Venting at the wrong time, particularly from the drywell, could conceivably lead to significant releases at the time when the public is moving out onto the roads and is most vulnerable.

The remaining sections in Module 4 discuss some of the specific phenomena that can challenge containments during a severe accident.

Table 4.2-1. Containment Threats According to Time Regime

TIME REGIME	CHALLENGE
Start of the Accident	Pre-existing Leak Containment Isolation Failure Containment Bypass
Prior to Vessel Breach	Reactor Coolant System Blowdown Insufficient Containment Heat Removal Hydrogen Combustion Late Bypass
At or Soon After Vessel Breach	Steam Spike Steam Explosion Combustion Direct Containment Heating Debris Contact with Containment
Late (> 2 Hours After Vessel Breach)	Failure of Containment Heat Removal Combustion Non-condensible gas generation Basemat Meltthrough

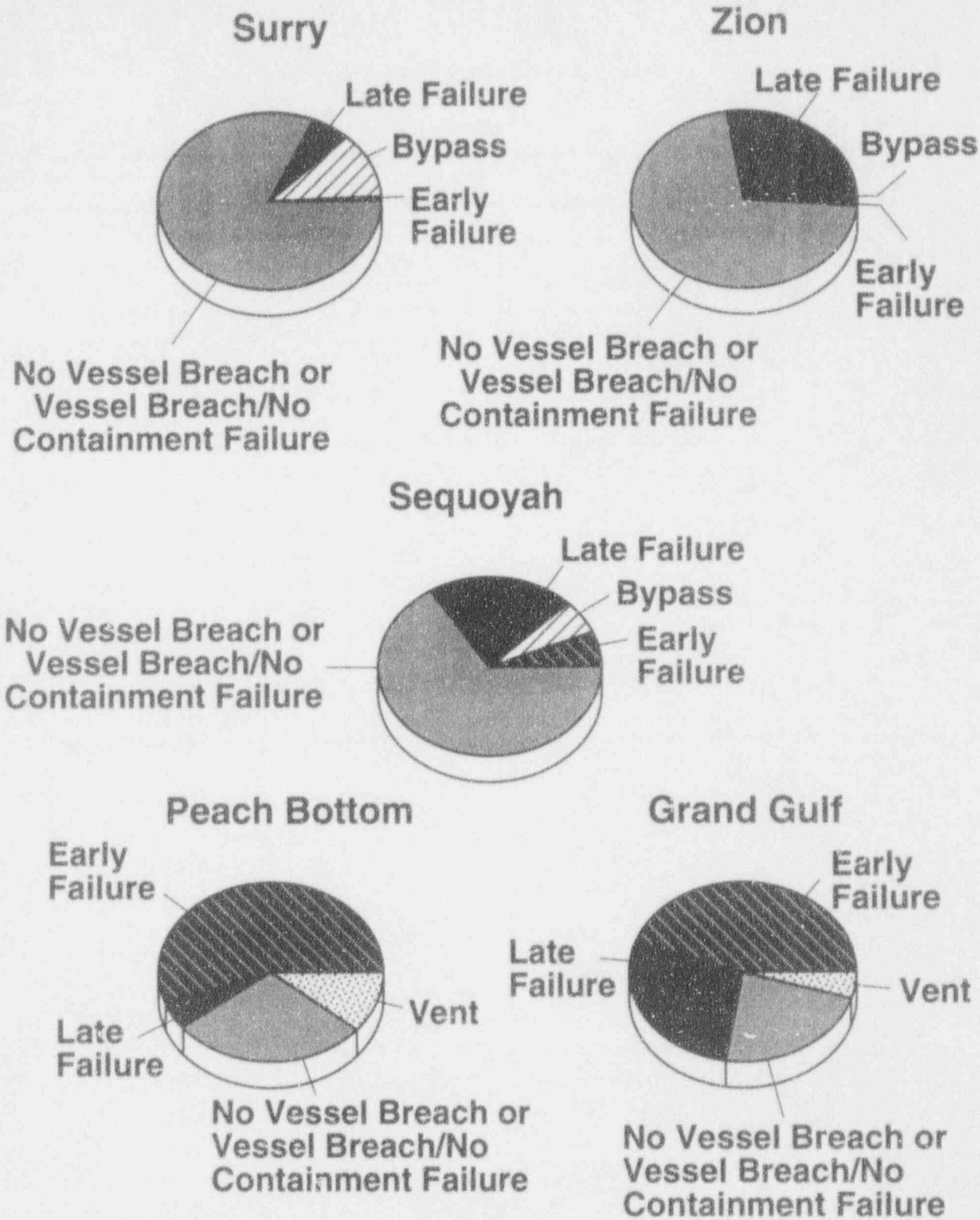


Figure 4.2-1 Relative probability of containment failure modes (internal events from NUREG-1150) given core damage

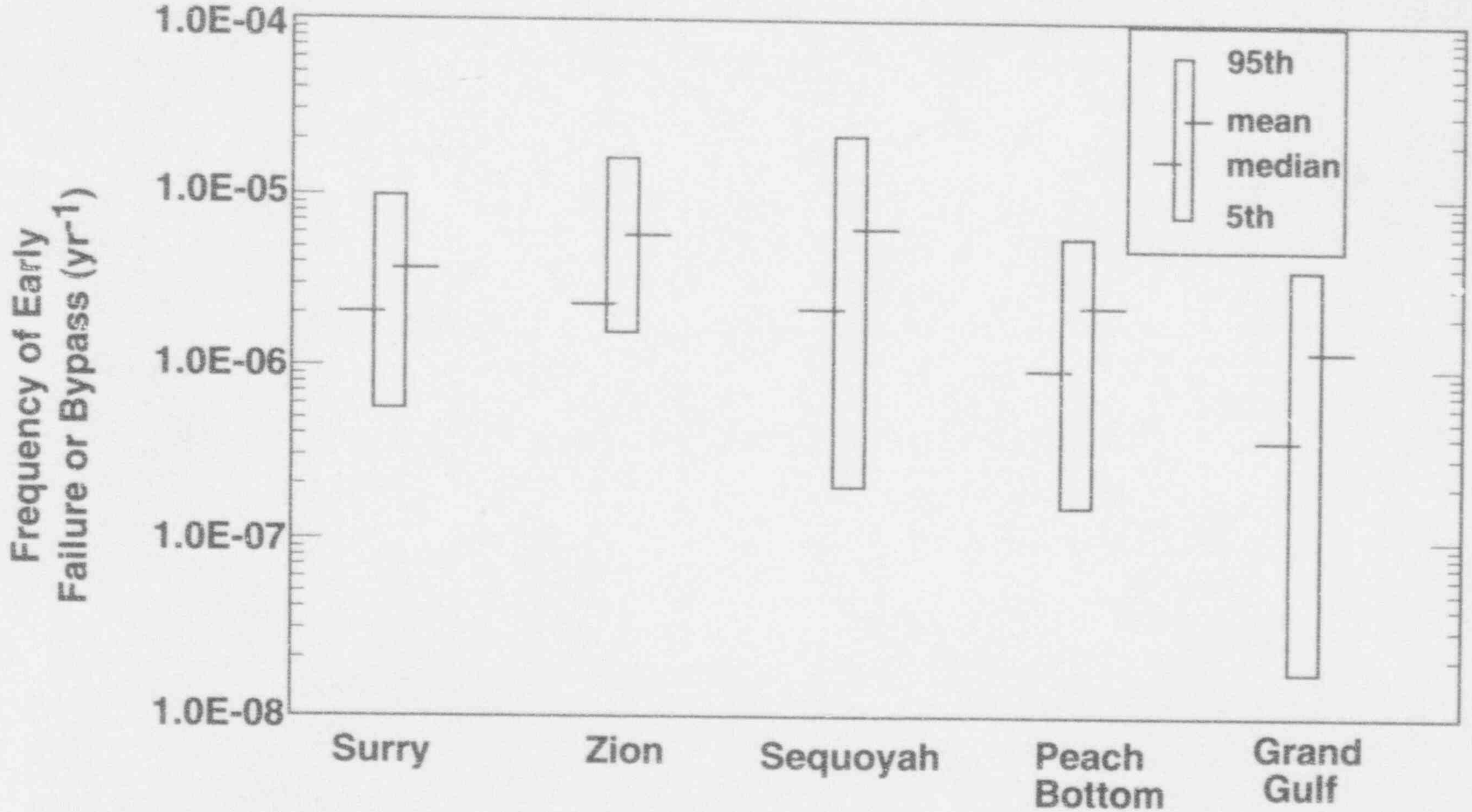


Figure 4.2-2 Frequency of early containment failure or bypass (internal events from NUREG-1150)

References for Section 4.2

1. David Okrent, Nuclear Reactor Safety: *On the History of the Regulatory Process*, The University of Wisconsin Press, Madison, WI (1981), (June 3, 1966), pp99-101.

2. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, WASH-1400, October 1975.

3. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

4. Generic letter 89-16, *Installation of a Hardened Wetwell Vent*, September 1, 1989

4.3 Ex-Vessel Fuel-Coolant Interactions

In many accidents, water will be present underneath the reactor vessel when the molten material exits the vessel at the time of failure. In other cases, water may be added on top of the molten material subsequent to vessel failure. It is generally considered axiomatic that water addition is always a good thing in a reactor accident. While current guidance to operators is always to add water, it is important to note that there are several different possible outcomes when molten core debris contacts water, and only some of these outcomes are desirable:

1. The water may act to cool and quench (refreeze) the molten core debris,
2. The debris may form a molten pool under the water, probably with an overlying crust layer, and remain molten, or
3. An energetic fuel-coolant interaction may occur.

Each of these possibilities is discussed in more detail below.

4.3.1 Quenching of Core Debris

Quenching and continued cooling of the core debris is generally the most desirable outcome. When the debris is solidified, the release of radioactive materials from the debris is effectively terminated. The most significant detrimental effect of quenching is the generation of large quantities of steam, which causes a pressure spike in the containment atmosphere. For the most part, a steam spike will not directly be a threat to the containment unless other phenomena occur simultaneously or the containment is already pressurized significantly prior to the steam spike.

Figure 4.3-1 depicts the quenching process. The process involves energy transfer from the molten core debris to liquid water. The molten debris gives up latent heat of fusion plus sensible heat in cooling down to a near-equilibrium temperature. Some oxidation energy will be involved if there are unoxidized metals present in the melt. The energy transferred to the water will heat the water to saturation and produce boiling sufficient to account for the available energy. The steam generated will then enter the containment atmosphere, causing a pressure increase. The speed of the quenching process depends upon how well the molten core mixes with water, the debris particle sizes, and the geometry of the mixture. The quenching process may be very rapid or take many minutes, depending upon these factors.

A calculation was performed for a station blackout sequence in the Zion large dry containment, considering the complete quenching of an entire molten core, along with 30% oxidation of the available metals.[1] This quenching process would yield approximately 268 Million BTU (283,000 MJ) of energy, and would produce a pressure spike of about 35 psig (240 kPa). Figure 4.3-2 shows the pressure in the Zion containment that could result from this accident sequence, assuming that the entire core is dropped into a reactor cavity full of water at about 14,000 seconds. The total containment pressure approaches 90 psig (620 kPa) as a result of the combined effects of prepressurization prior to vessel breach, vessel blowdown at vessel breach, and the 35 psi (241 kPa) pressure rise resulting from the quenching in the reactor cavity. Two different quenching times are shown in Figure 4.3-2, corresponding to one minute and one hour. Without operating containment heat removal systems, the two different times produce similar containment pressure rises. The longer time available for heat transfer to structures is somewhat offset by the continued addition of decay heat.

In reality, quenching the debris will usually result in pressures much less than those indicated in Figure 4.3-2. First, it is extremely unlikely that all of the core debris will be involved in one large steam spike. Most models of accident progression indicate that a significant fraction of the core will remain in the vessel and be released slowly over a long time period. Second, there must be sufficient water available to participate in the quenching process. In the example shown, there was a completely full reactor cavity. Even if sufficient water is initially present, some of the water may be blown out of the reactor cavity before it can contact the core debris, possibly resulting in debris that is not quenched.

Subatmospheric containments will respond to steam spikes in much the same manner as large dry containments. There is general agreement that other containment types are even less susceptible to steam spikes due to their pressure suppression design.[1] While not designed precisely for steam spikes at vessel breach, suppression pools and ice condensers can readily handle such loads, provided that the water or ice has not been depleted prior to the event. Note that, after the debris quenches, a continuing water supply and long-term heat removal are still necessary in most cases to remove the decay heat that can gradually pressurize the containment.

4.3.2 Non-Coolable Debris

There are some cases in which core debris may not quench, or if quenched, may subsequently form a rubble bed that is non-coolable. Cooling of core debris requires that the debris remain in contact with water, to allow boiling heat transfer to carry away the decay heat. Two mechanisms that can prevent this contact are debris bed dryout and crust formation. The vapor that flows up out of the debris bed can provide resistance to overlying and surrounding water that is needed to permeate the debris bed. If the resistance to water is sufficient, parts of the bed may dry out, leading to continued melting and possible core-concrete attack. Figure 4.3-3 depicts the mechanisms contributing to debris bed dryout.

As discussed in Module 3, the key factors affecting debris bed dryout are the particle sizes and the geometry of the debris bed. Mixed particle sizes, particularly with smaller particles and deeper debris beds, tend to be less coolable than shallow debris beds composed of large particles. With smaller particles, the porosity of the bed decreases, the surface area for heat transfer is larger, and therefore, the vapor generation rates are increased relative to water ingress rates. Many particle sizes are possible during a severe accident, ranging from .01 inches (.025 cm) or less up to inch size and larger. There is no one exact particle size that provides a threshold for coolability. However, particle sizes of a tenth of an inch (.25 cm) and smaller are the ones most likely to be non-coolable. Such small particles can form during energetic melt ejection from the vessel or as a result of energetic fuel-coolant interactions (discussed in the next subsection).

In addition to debris bed dryout, there is a second possibility for non-coolable core debris. If a molten pool is contacted by an overlying water pool, a crust may form, preventing the further contact of water with the melt. In this case, core-concrete attack may continue unabated, as discussed in Section 4.4.

With non-coolable core debris, any boiling that does occur will not rapidly affect the containment pressure, and can generally be neglected, unless a sequence involves loss of all containment heat removal for many hours or even days. Because some of the decay heat goes into the core-concrete attack as opposed to the containment atmosphere, this case actually produces less of a long-term overpressure threat from steaming than the case where the debris is quenched. The threats from core-concrete attack and combustible (and other non-condensible) gas generation may more than offset the benefits of reduced steaming and are discussed in more detail in later sections.

4.3.3 Ex-Vessel Steam Explosions

The largest threat to containment resulting from the ex-vessel interaction of molten core debris and water is an energetic ex-vessel fuel-coolant interaction (steam explosion). An ex-vessel steam explosion is simply an extreme case of a steam spike, where the quenching occurs explosively, and produces dynamic as well as static pressures. An ex-vessel steam explosion can threaten the containment is several different ways, including:

1. Generation of dynamic pressure loads (shock waves) that can fail the containment structure,
2. Generation of pressures and shock waves that can fail vessel support structures, leading to movement of the vessel and failure of containment piping penetrations,
3. Generation of energetic missiles that can be thrown into the containment, or
4. Generation of pressures and shock waves that can fail the drywell floor of a BWR Mark II containment or the drywell wall of a Mark III containment.

Generally, the second and fourth threats above are the ones of most concern, and generally more so for BWRs (and a few PWRs), because of the confined pedestal region and the impact of pedestal failure on the containment. Section 4.3.4 discusses the design-specific aspects of ex-vessel steam explosions in more detail. As with in-vessel steam explosions, there are many factors that contribute to the magnitude of any ex-vessel steam explosion. These include:

1. The amount of water available to participate,
2. The composition of the melt, including the amount of unoxidized metals that may react during the explosion,
3. Cavity or pedestal region geometry, insofar as it may lead to confinement of the explosion or focusing of shock waves,
4. Transmission of shock waves through a water pool,
5. Pouring rate and contact mode, i.e., water on corium, corium on water, or jet ejection into water, and
6. Fraction of the core participating.

The physical processes involved in steam explosions were described in Module 3. Those processes are similar for ex-vessel steam explosions, except that some of the initial conditions are different. The ex-vessel case will always be at low pressure, no higher than the containment failure pressure. Steam explosions tend to be more likely at low pressure. Second, the geometry is different, involving varying degrees of confinement. Third, there are three contact modes to consider. The corium may pour from the vessel into a water pool or water may be added on top of corium, not unlike some in-vessel scenarios, or the corium may be ejected from the vessel as a high pressure jet into a water pool.

The latter case is unique to ex-vessel conditions and results when the vessel fails at high pressure. Experiments indicate that some steam explosions are almost certain under these conditions, but the magnitude is largely unknown. If the initial mass exiting the vessel reacts, it may blow the water out of the cavity or pedestal region, resulting in less reaction of the later material. Because the jet is not all released instantaneously, it is likely that a fairly small fraction of the core will participate. However, significant challenges to containment and vessel supports are still possible, particularly if oxidation accompanies the explosion.

One potential benefit of an ex-vessel steam explosion is that the core debris may be dispersed in the containment, reducing the concerns of core-concrete attack, and possibly making the debris more coolable. On the other hand, the benefit of such an event depends on exactly where the debris ends up and the continuing availability of long-term containment heat removal.

As noted in Module 3, rapid quenching of core debris, explosively or otherwise, can result in significant oxidation of any metals contained in the core debris. Hydrogen generated as a result of this oxidation can present a significant threat that will be discussed in later sections.

4.3.4 Containment Design Considerations

As noted above, there are many features that can impact the importance of ex-vessel fuel-coolant interactions. First and foremost, the presence of water is necessary for a fuel-coolant interaction to occur. In some scenarios, particularly for large dry PWR containments, the reactor cavity will be dry or nearly so. Generally, for large quantities of water to be present in the reactor cavity, the containment sprays must have operated or large quantities of water have been pumped out a break in the primary system. Then, if the sump and floor design allows, some of this water will overflow into the reactor cavity. Ice condenser containments are more likely to contain water in the reactor cavity due to the melting of ice combined with other sources. In fact, ice condenser containments can be deeply flooded in the lower compartment, mitigating fission product releases, but also providing a transmission medium for shock waves.

In BWR containments, water is likely to be present under the vessel for most loss-of-coolant accidents. Transient sequences may have a relatively dry pedestal region if the drywell sprays have not been used, and there has not been significant prior leakage. Mark III containments are the most likely to have large amounts of water under the vessel as a result of water spilling over the weir wall from the suppression pool. However, all three BWR containment types are susceptible to failure of the vessel supports, with relatively small amounts of water present. Figures 4.3-4, 4.3-5, and 4.3-6 depict typical pedestal regions for BWRs and point out some of the important vulnerabilities. As noted earlier, the Mark II containments are also susceptible to failure of the floor separating the drywell from the wetwell. Another factor for Mark II containments, resulting from the considerable design variation among the Mark II containments, is the possibility of corium flowing down the downcomers into the suppression pool, failing the downcomers with a steam explosion or as a result of meltthrough. Some Mark II containments have downcomers located directly below the vessel, guaranteeing some flow into the downcomers.

For both BWRs and PWRs, if water is not present prior to vessel failure, then water may be pumped into the reactor coolant system at a later time and flow through the failed vessel onto the melt.

Finally, the relative containment failure probabilities from ex-vessel fuel-coolant interactions were assessed for the six containment types in the NUREG-1150 and LaSalle studies.[2,3] These studies indicate that containment failure is very unlikely for the three PWRs examined. For the three BWRs, drywell failures from steam explosions contribute noticeably to the overall containment failure probabilities, particularly for the Mark I and Mark II designs.

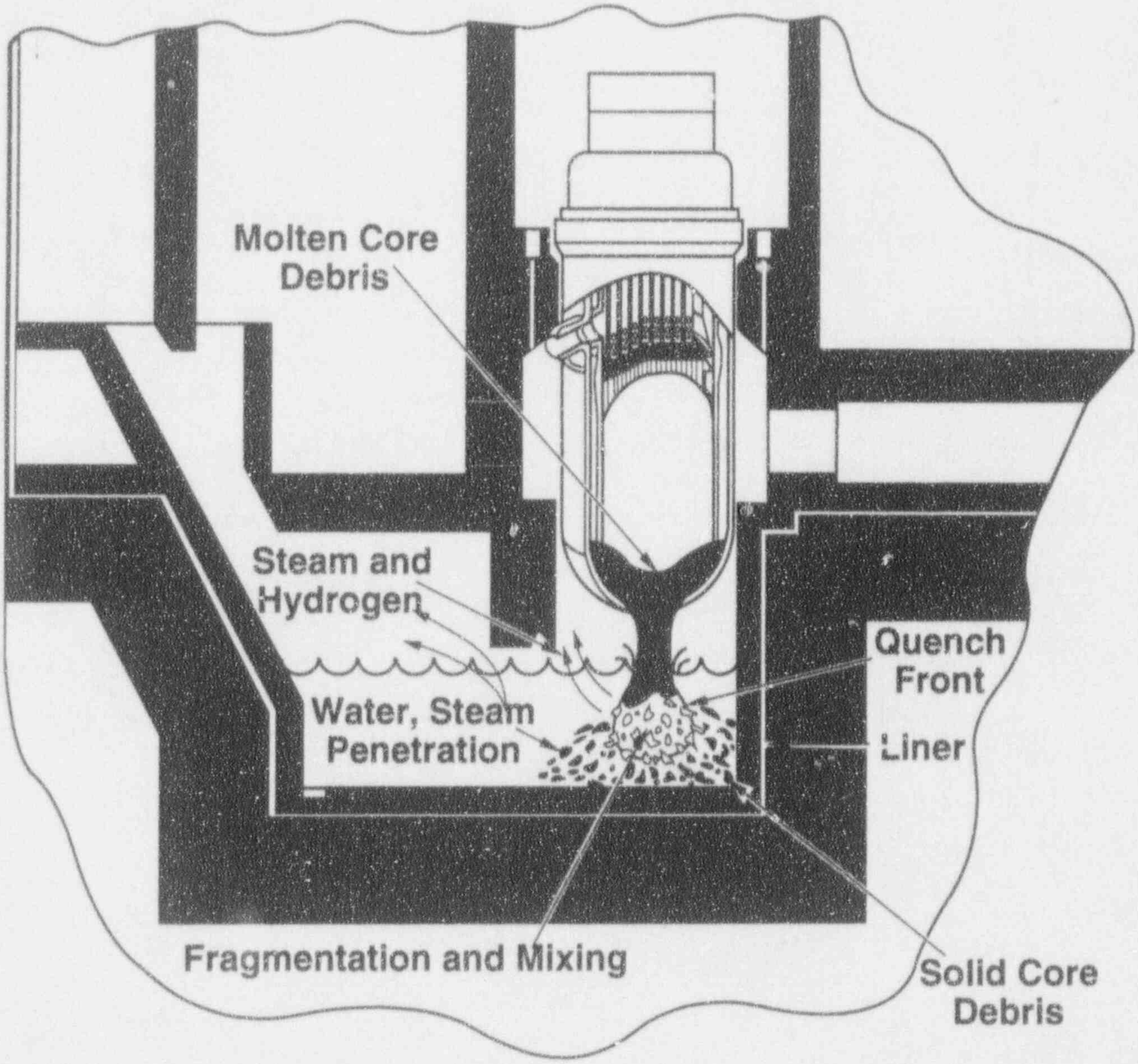


Figure 4.3-1 Molten Core Quenching Process

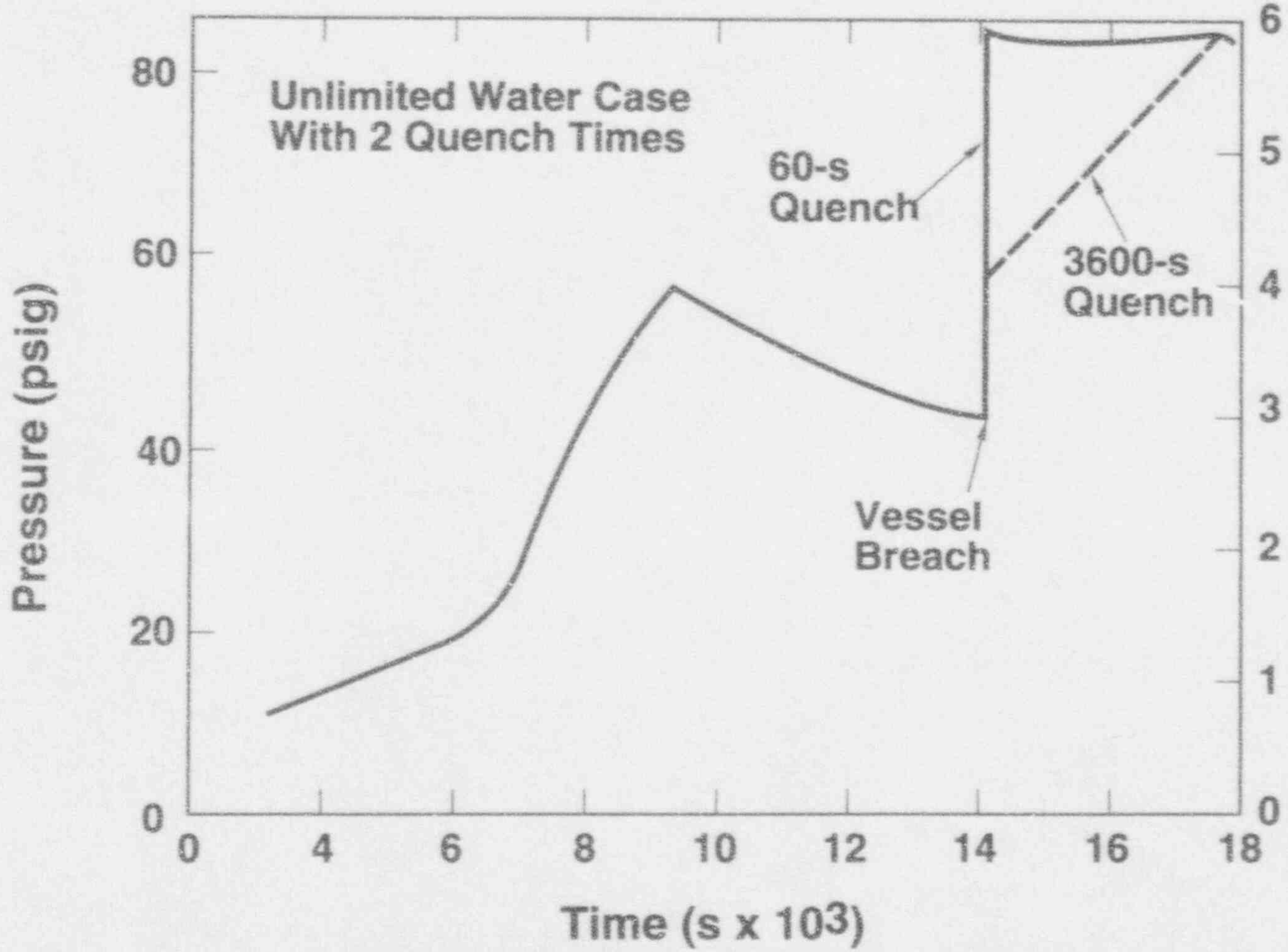


Figure 4.3-2 Containment pressure versus time for Zion Station blackout sequence

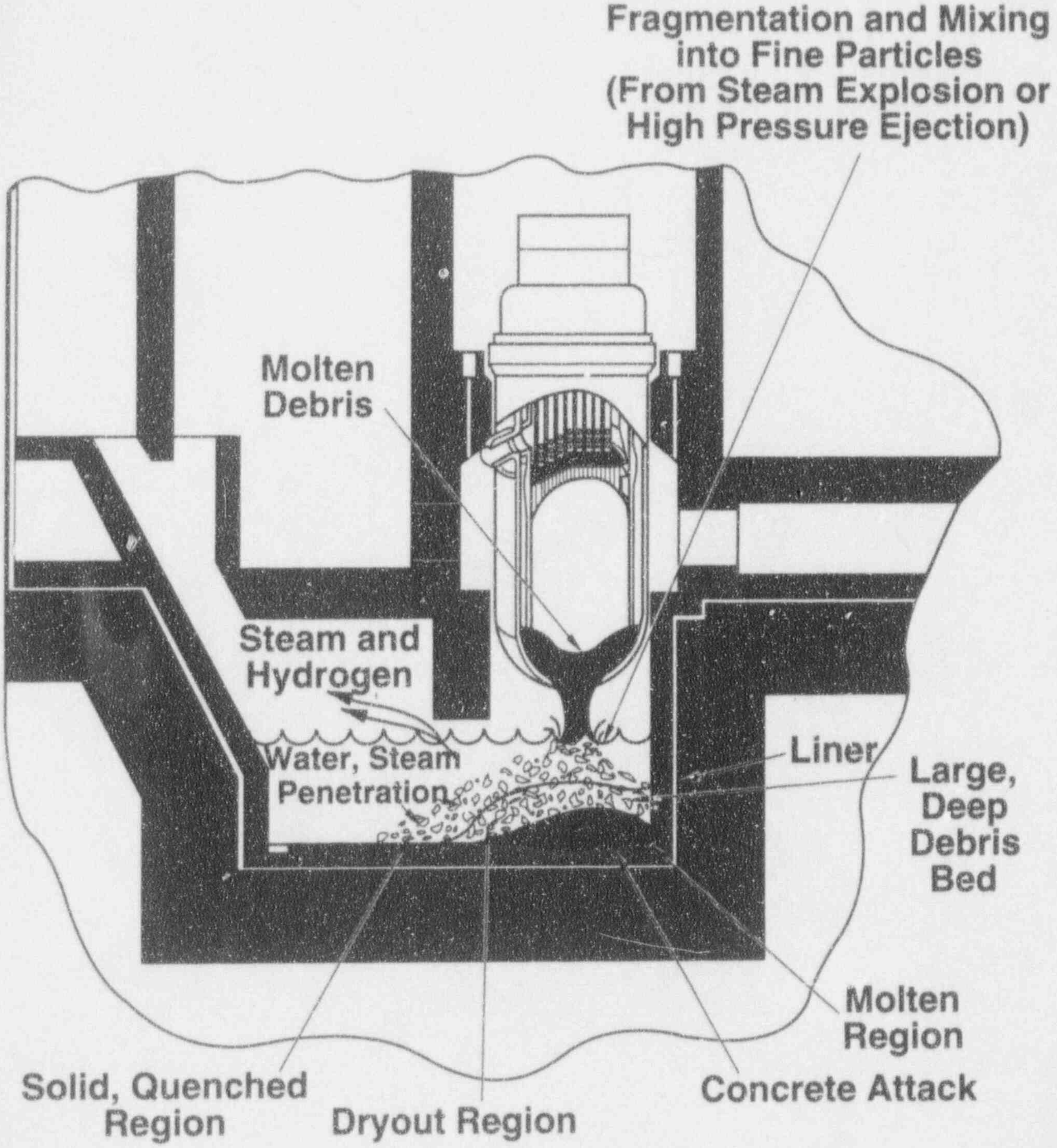


Figure 4.3-3 Noncoolable debris bed

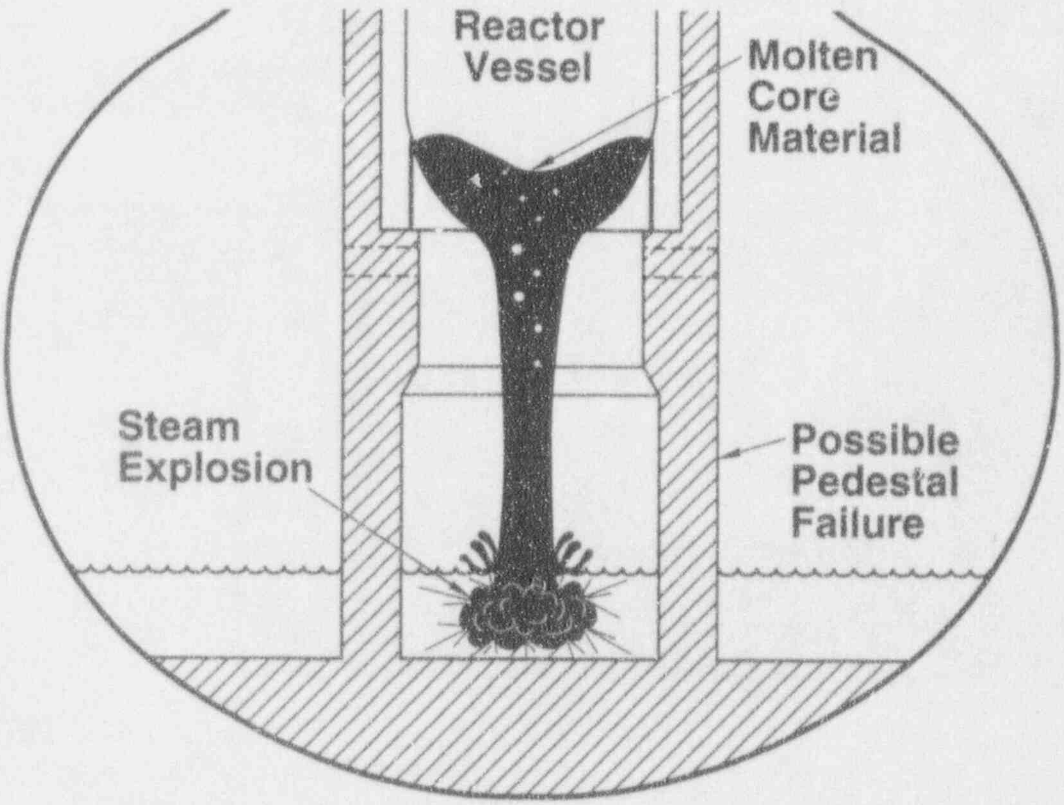


Figure 4.3-4 BWR Mark I containment pedestal region

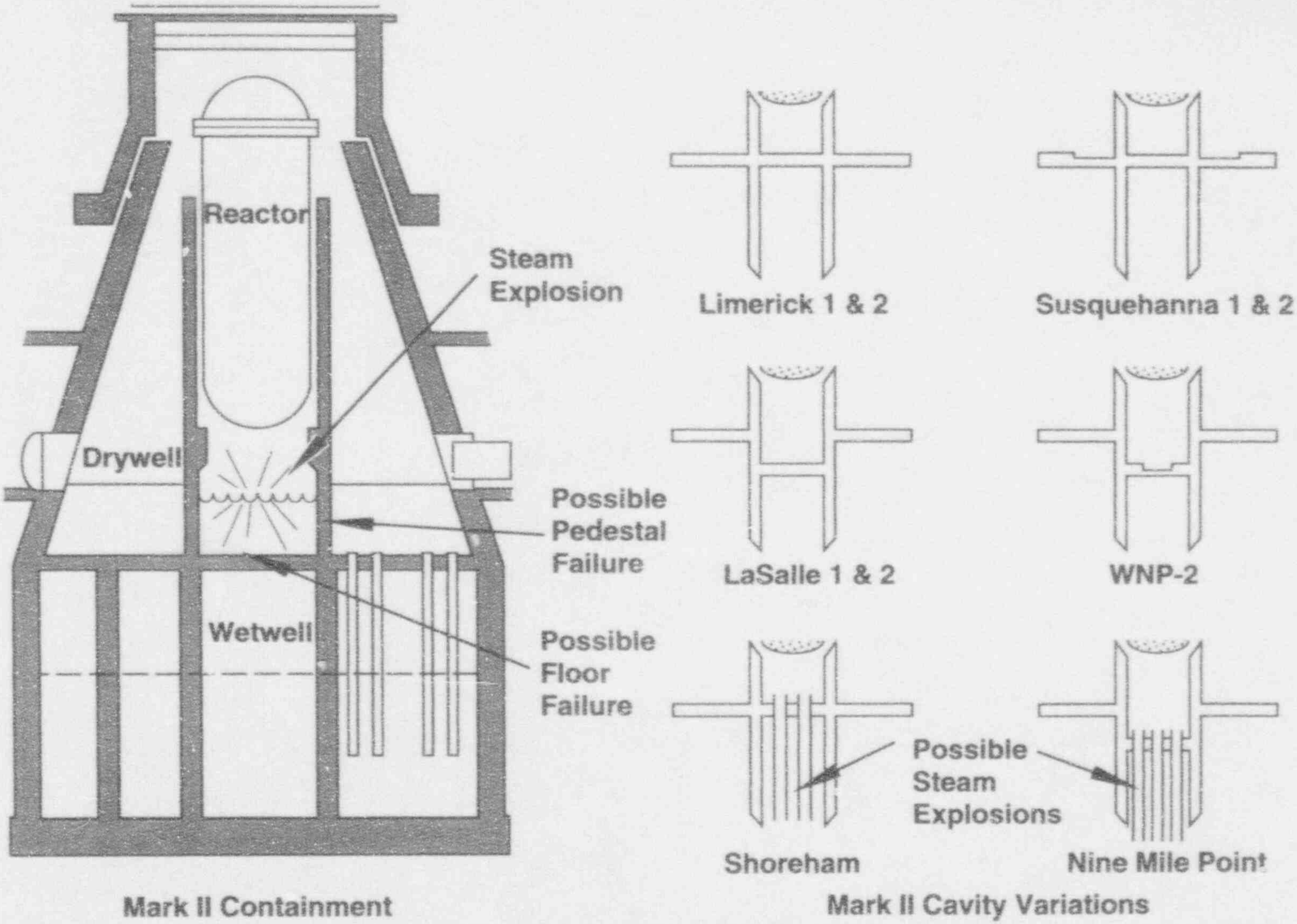


Figure 4.3-5 BWR Mark II containment pedestal region

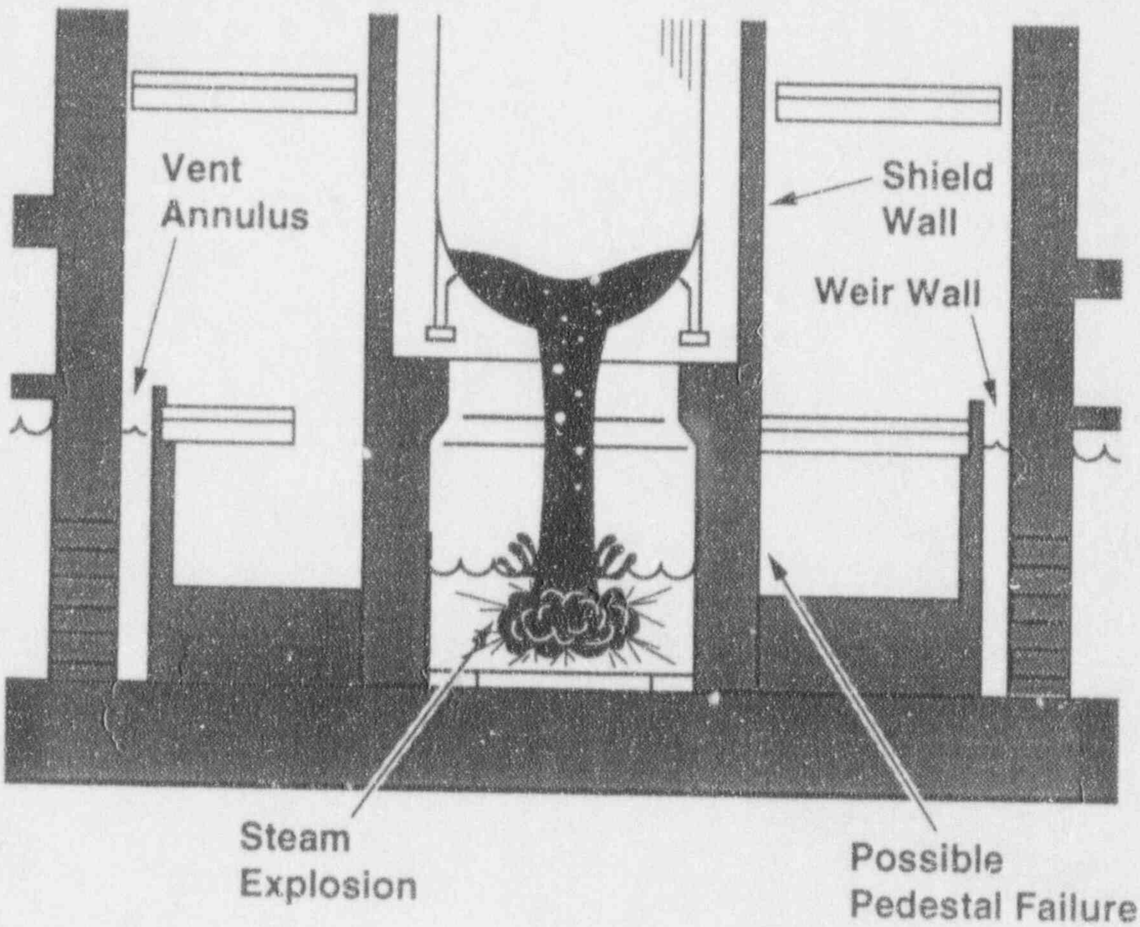


Figure 4.3-6 BWR Mark III pedestal region

References for Section 4.3

1. *Estimates of Early Containment Loads from Core Melt Accidents*, NUREG-1079, Draft Report for Comment, December 1985.

2. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

3. T. D. Brown, et al., *Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant: Phenomenology and Risk Uncertainty Evaluation Program (PRUEP)*, NUREG/CR-5305, SAND90-2765, Sandia National Laboratories, 1992.

4.4 Core-Concrete Interactions

If molten core material falls into the reactor cavity or pedestal region and is not blown out due to high pressure melt ejection or ex-vessel steam explosions, then Core-Concrete Interactions (CCIs) are possible. The possibility of CCIs leading to basemat meltthrough and containment failure was highlighted by Brookhaven National Laboratory in reference to the China Syndrome.[1] Numerous studies and experimental programs have since verified that basemat meltthrough is possible, although there are still significant uncertainties. Research has indicated that CCIs can also have other important effects in accidents, even when the basemat remains intact. In particular, combustible gas generation can occur and large quantities of aerosols can be generated, thus affecting the source term if the containment fails. In the subsections below, these topics are discussed in more detail.[2]

4.4.1 Concrete Attack

The most obvious concern about CCIs is the compromising of the containment structure. In addition to basemat meltthrough, CCIs can lead to failure of vessel supports and other local structures that can indirectly lead to containment failure. The ensuing discussions of concrete attack are intended to include all of these possibilities.

Most concrete used in reactor applications is either Type I or Type II Portland cement combined with various types of aggregate materials. As shown in Figure 4.4-1, the attack of concrete by corium is largely a thermal process. Decay heat and some heat from chemical reactions (which may dominate for short periods of time) are generated in the molten pool and may be transferred to the top surface of the pool or to the surrounding concrete. Under most circumstances, the heat flux to the concrete is sufficient to decompose it, releasing gases and melting the residual materials which are primarily oxides and metal reinforcing bars. The melted materials are added to the molten pool, thus diluting it, increasing its surface area, and reducing the volumetric heat generation rate. In time, heat transfer out the top of the molten pool and through the surrounding concrete may be sufficient to remove the generated heat and the temperature will decline to the point at which the CCI is terminated. Typical CCIs can penetrate concrete at the rate of a few inches (several cm) per hour. Whether or not the CCI is terminated prior to basemat meltthrough is determined by many factors, including:

1. Type of concrete and aggregate used in the structure,
2. Basemat thickness,
3. Cavity size and geometry,
4. Melt mass in the cavity,
5. Melt composition, and
6. Presence of overlying water.

As noted in Section 4.3, the presence of an overlying water pool does not guarantee that the debris will be coolable. A crust may form over the melt or the boiling rate may simply not be sufficient to remove the decay heat. However, it is possible that water will have some beneficial effect and at least slow down the concrete attack.

As concrete attack progresses, concrete begins to fail (lose its structural integrity) even before gross melting of its constituents occurs. The loss of structural integrity accompanies the release of water and carbon dioxide from the concrete in three phases:[3]

1. Release of molecular and physically entrapped water between 86 and 446°F (30 and 230°C),

2. Release of water chemically constituted as hydroxides between 662 and 932°F (350 and 500°C), and

3. Release of carbon dioxide from the aggregate and the cementitious phases between 1112 and 1832°F (600 and 1000°C).

The point at which concrete loses its integrity varies with the type of concrete, but generally occurs well before the carbon dioxide is released. Typical concrete contains about 4 to 9 weight percent water and 0 to 45 weight percent carbon dioxide. Loss of structural integrity is particularly important when considering the possible impact of CCIs upon vessel supports in BWRs.

Figures 4.4-2 and 4.4-3 show examples of calculations of concrete attack.[4,5] The contours in Figure 4.4-3 represent the movement of the ablation front downward and radially outward with time (one hour per contour). An important aspect of basemat meltthrough is that, even if it occurs, one would expect that many hours would be available to initiate emergency response plans, including evacuation and sheltering, so that offsite health effects can be minimized.

4.4.2 Combustible Gas Generation

A significant byproduct of CCIs is the generation of combustible gases. Combustible gases are generated indirectly in a CCI. As shown in Figure 4.4-4, water and carbon dioxide are released from the concrete. These gases then react with unoxidized metals in the molten pool to produce metal oxides and the combustible gases hydrogen and carbon monoxide. As a result of complex reactions within the melt, the actual concentrations of hydrogen and carbon monoxide in the gases exiting the melt can vary significantly. It is likely that the flow of gases up through the melt will be nonuniform and that the melt itself will consist of layers of varying metallic content.

The total amount of combustible gas that can be formed is limited primarily by the amount of metallic constituents present in the melt, although some other reactions are possible that can slightly increase this quantity. It is noteworthy that this total amount of combustible gas can be larger than that produced by 100% oxidation of all available zirconium, which is normally the limit for in-vessel hydrogen production. The molten pool in the cavity may contain large amounts of steel from the vessel and other structures; this steel is also available for oxidation. It is not inconceivable that a few thousand pounds (or kilograms) of combustible gases could be generated from CCIs.[3]

As the combustible gas exits the top of the melt, there are several possibilities. First, if there is an overlying water pool, the gases will cool before they pass into the containment atmosphere. Second, if there is no overlying water pool, the gases may spontaneously ignite above the molten corium. This spontaneous ignition requires high temperatures (supplied by the molten pool) and the presence of oxygen. Oxygen in the cavity will be rapidly depleted unless flow paths exist to circulate oxygen from the rest of containment. Spontaneous ignition can not occur in Mark I and II BWRs which have inert containments. Combustion effects will be discussed in more detail in Section 4.6.

For Mark I and II containments, despite their inerted condition, gases from CCIs can still represent a concern. Because these gases are noncondensible, they can lead to significant pressure buildup that can not be removed using sprays or suppression pool cooling. Venting may ultimately be required to prevent long-term overpressure from these gases.

4.4.3 Aerosol Generation

CCIs can have a significant impact upon the source terms in accidents in which the containment fails above ground. In general, generation of radioactive aerosols will increase the resulting source term if the containment fails. However, if large quantities of non-radioactive aerosols are generated they can lead to agglomeration and retention of many of the radioactive aerosol particles. Large quantities of aerosols, radioactive or otherwise, have the potential to plug filters that are not designed for such loadings.

Generation of aerosols and fission product transport involve complex processes. Volatile and semi-volatile fission products can be present in gases that are passing up through the melt. As these materials exit the melt and cool, they condense into thick aerosol clouds that carry fission products throughout the containment. Chemical reactions are possible during the vaporization processes. As the chemical reactions progress, the volatility of the fission products changes, based on the changing chemical forms. Additional aerosols, including less volatile radionuclides, form when gas bubbles burst at the surface of the melt, producing particles that are entrained in the flowing gases. An overlying water pool can substantially mitigate this fission product release; however, CCIs account for a major fraction of the source term in many accident sequences.

Figure 4.4-5 shows example VANESA calculations of aerosol generation rates as a result of CCIs at three plants and for three different accident scenarios.[6] The wide variations result from differences in melt composition and concrete type. These calculations do not account for any overlying water pools. This figure indicates the tremendous mass of material that can be suspended in the containment in the form of aerosols. Tables 4.4-1 and 4.4-2 indicate the types of materials that can be contained in the aerosols. Most of the mass is made up of concrete materials, such as CaO and SiO_2. However, the tables also show that significant fractions of fission products are also released during CCIs.

Table 4.4-1. Core-Concrete Release for Sequoyah Station Blackout Sequence

Species	Released Mass (kg) (1 kg = 2.2lb.)	Release Fraction(1)
Fission Products		
I+Br	.47	1.0
Cs+Rb	5.9	1.0
Te+Sb	2.3	0.46
Sr	10	0.17
Mo	1.9×10^{-3}	1.0×10^{-5}
Ru(2)	2.3×10^{-5}	9.0×10^{-8}
La(3)	2.5	4.0×10^{-3}
Nb	3.5	1.0(4)
Ce+Np+Pu	5.3	6.6×10^{-3}
Ba	7.7	0.10
Steel		
Fe(5)	1052	1.4×10^{-2}(6)
Cr	1.1	1.0×10^{-4}
Ni	18	3.5×10^{-3}
Zircaloy		
Zr(7)	2.4×10^{-2}	1.0×10^{-6}
Sn	8.8	2.8×10^{-2}
Control Rods		
Ag+In	251	9.2×10^{-2}
Cd	143	1.0
Fuel		
U	6.0	7.0×10^{-5}
Concrete (6)		
CaO	1915	4.3×10^{-2}
Al_2O^3	67	4.2×10^{-2}
Na_2O	14	0.18
K_2O	131	0.20
SiO_2	221	6.2×10^{-2}

(1) Based on melt inventory at start of core-concrete interaction.
(2) Includes Tc, Rh, and Pd.
(3) Includes Y, Zr(fp), Pr, Nd, Pm, Eu, and Sm.
(4) Quantitative release is calculated because of the assumed oxide chemical form, which is under review.
(5) Includes Fe from concrete and reinforcing bars.
(6) Release fraction based on the amount of concrete and reinforcing bars incorporated into the molten pool.
(7) Structural Zr only.

Table 4.4-2. Core-Concrete Release for Peach Bottom Station Blackout Sequence

Species	Released Mass (kg) (1 kg = 2.2lb.)	Release Fraction(1)
Fission Products		
I+Br	1.8	1.0
Cs+Rb	27	1.0
Te+Sb	14	0.64
Sr	53	0.84
Mo	5.0×10^{-4}	2.0×10^{-6}
Ru(2)	3.0×10^{-4}	9.0×10^{-7}
La(3)	33	3.9×10^{-2}
Nb	4.3	1.0(4)
Ce+Np+Pu	90	9.0×10^{-2}
Ba	64	0.62
Steel		
Fe(5)	1234	1.3×10^{-2}(6)
Cr	6.6×10^{-2}	8.10^{-6}
Ni	29	6.2×10^{-3}
Mn	89	0.50
Zircaloy		
Zr(7)	0.55	8.0×10^{-6}
Sn	46	5.0×10^{-2}
Control Material		
Gd	17	5.8×10^{-2}
Fuel		
U	23	2.0×10^{-4}
Concrete (6)		
Ca0	1988	2.9×10^{-2}
$A1_20^3$	339	0.14
Na_20	82	0.74
K_20	656	0.64
$Si0_2$	1124	6.21

(1) Based on melt inventory at start of core-concrete interaction.
(2) Includes Tc, Rh, and Pd.
(3) Includes Y, Zr(fp), Pr, Nd, Pm, Eu, and Sm.
(4) Quantitative release is calculated because of the assumed oxide chemical form, which is under review.
(5) Includes Fe from concrete and reinforcing bars.
(6) Release fraction based on the amount of concrete and reinforcing bars incorporated into the molten pool.
(7) Structural Zr only.

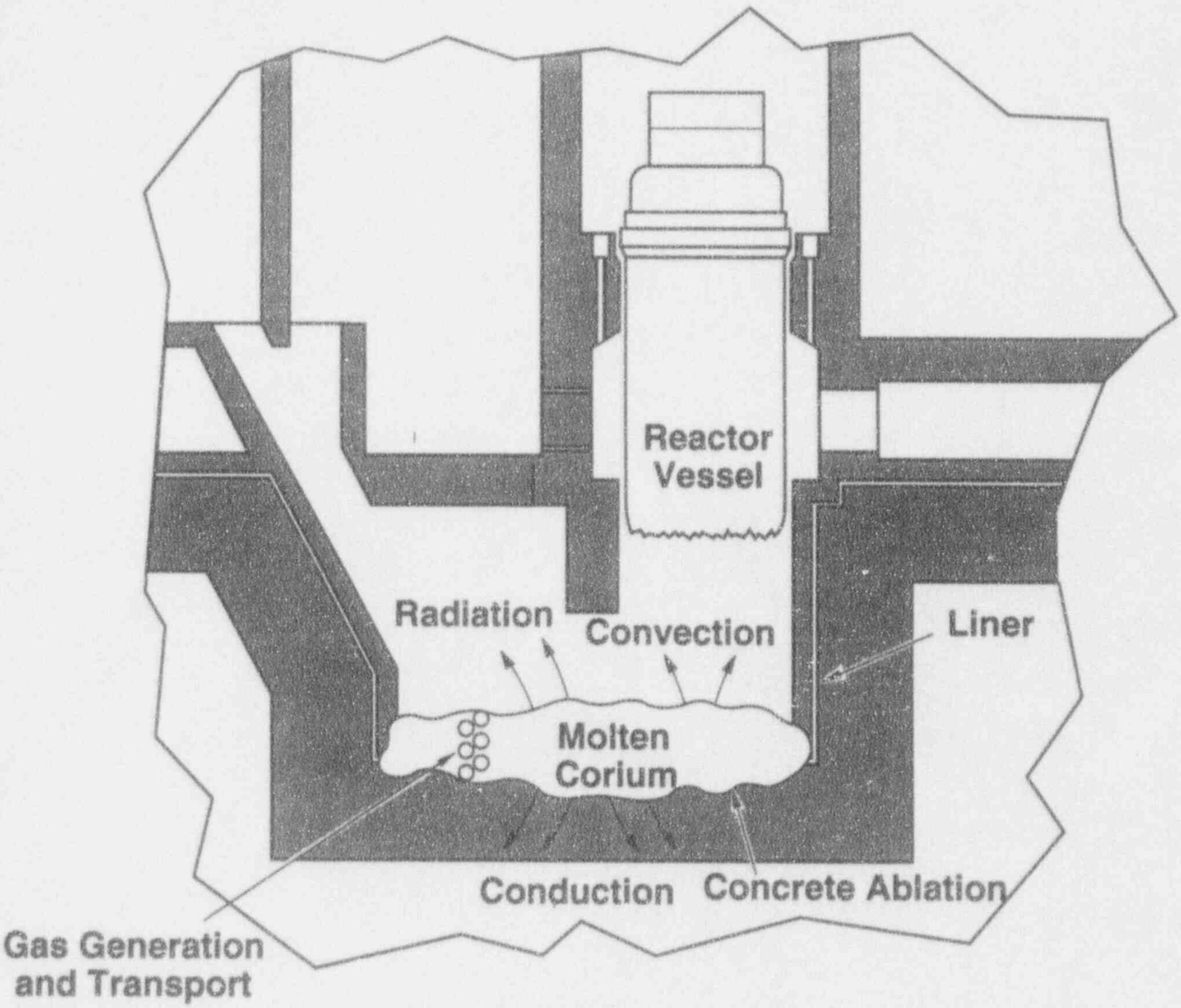


Figure 4.4-1 Thermal aspect of core-concrete interactions

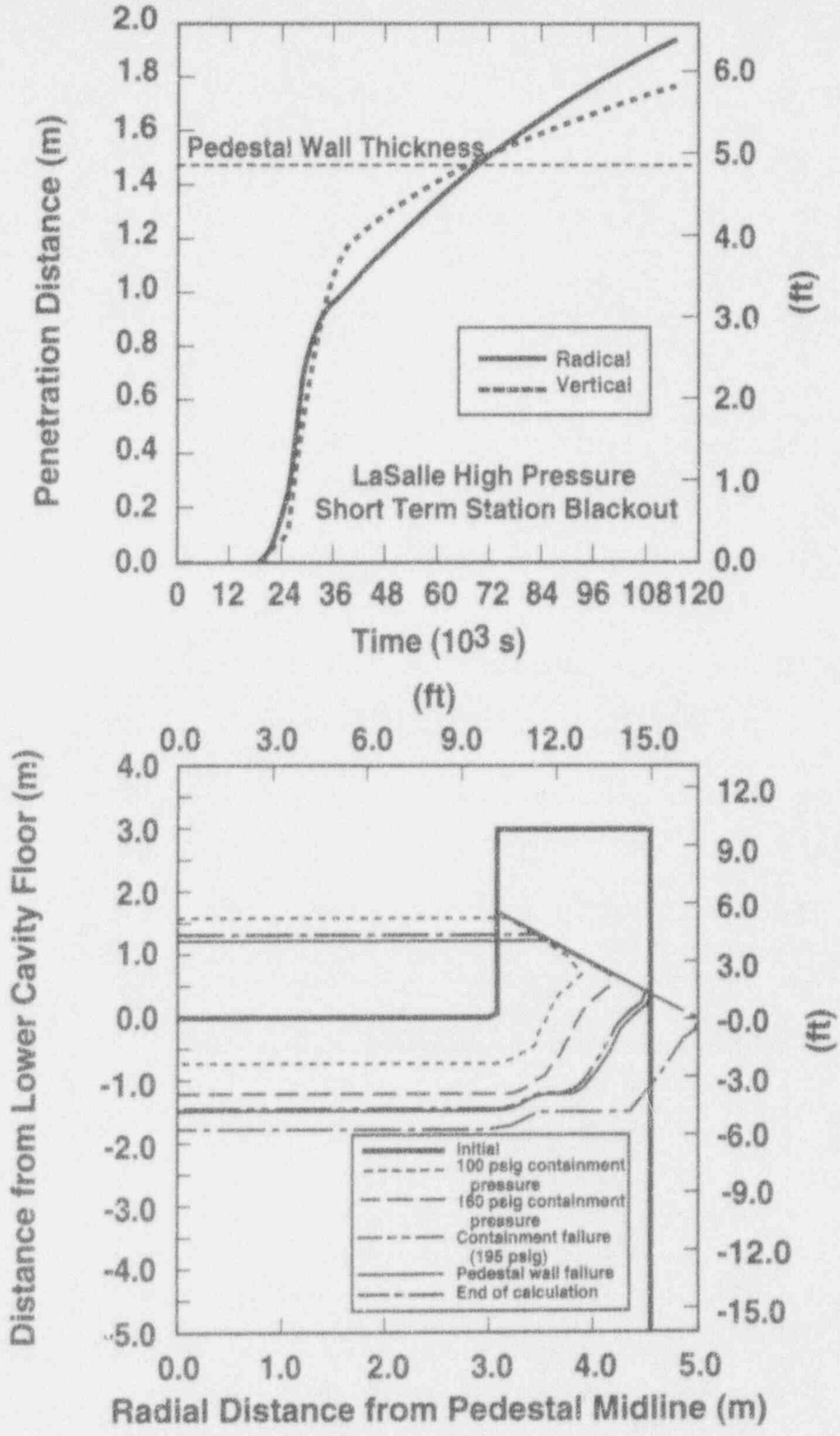


Figure 4.4-2 Calculation of concrete attack in a BWR Mark II containment during a station blackout sequence

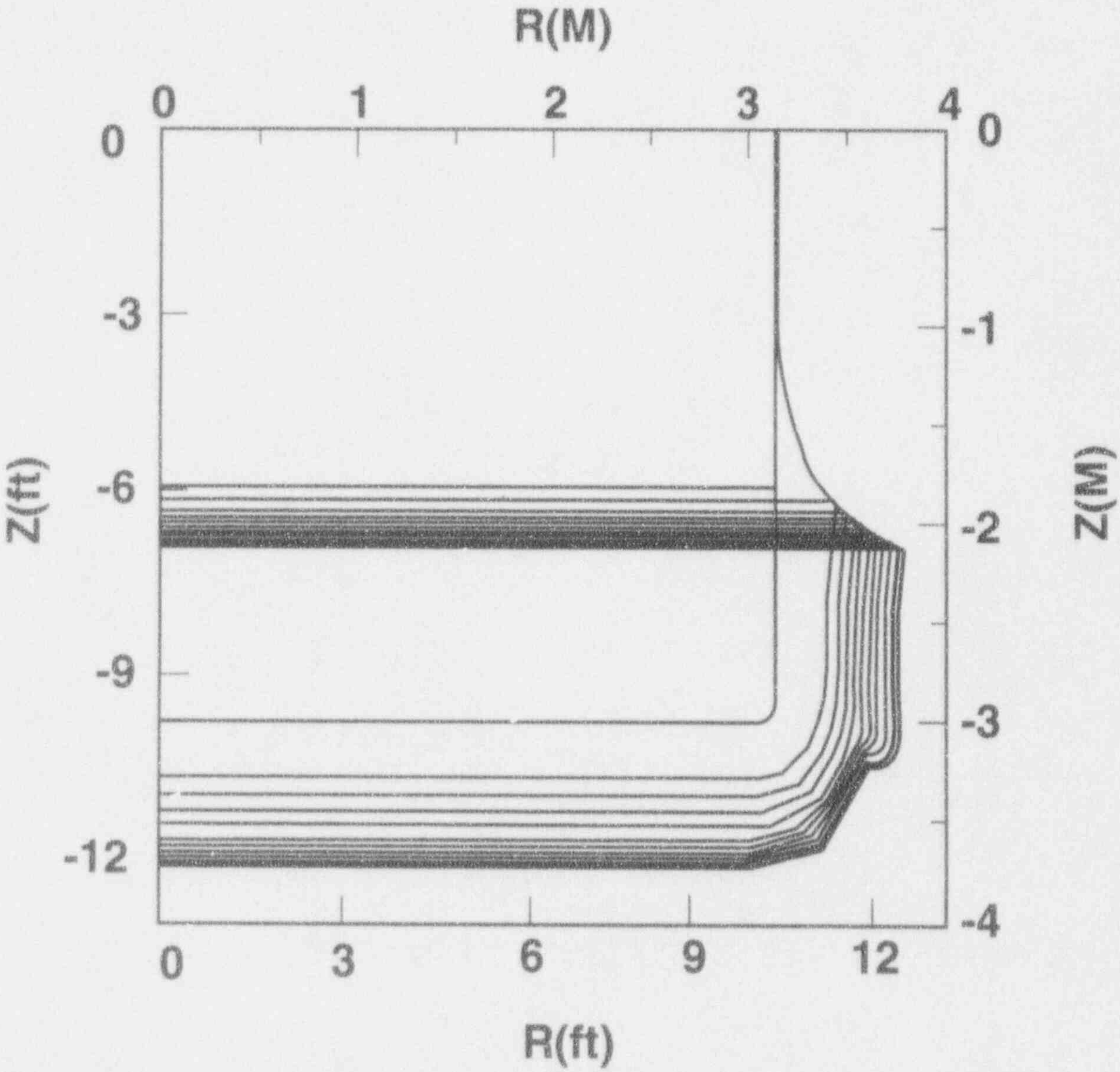


Figure 4.4-3 Example calculation of concrete attack for a PWR

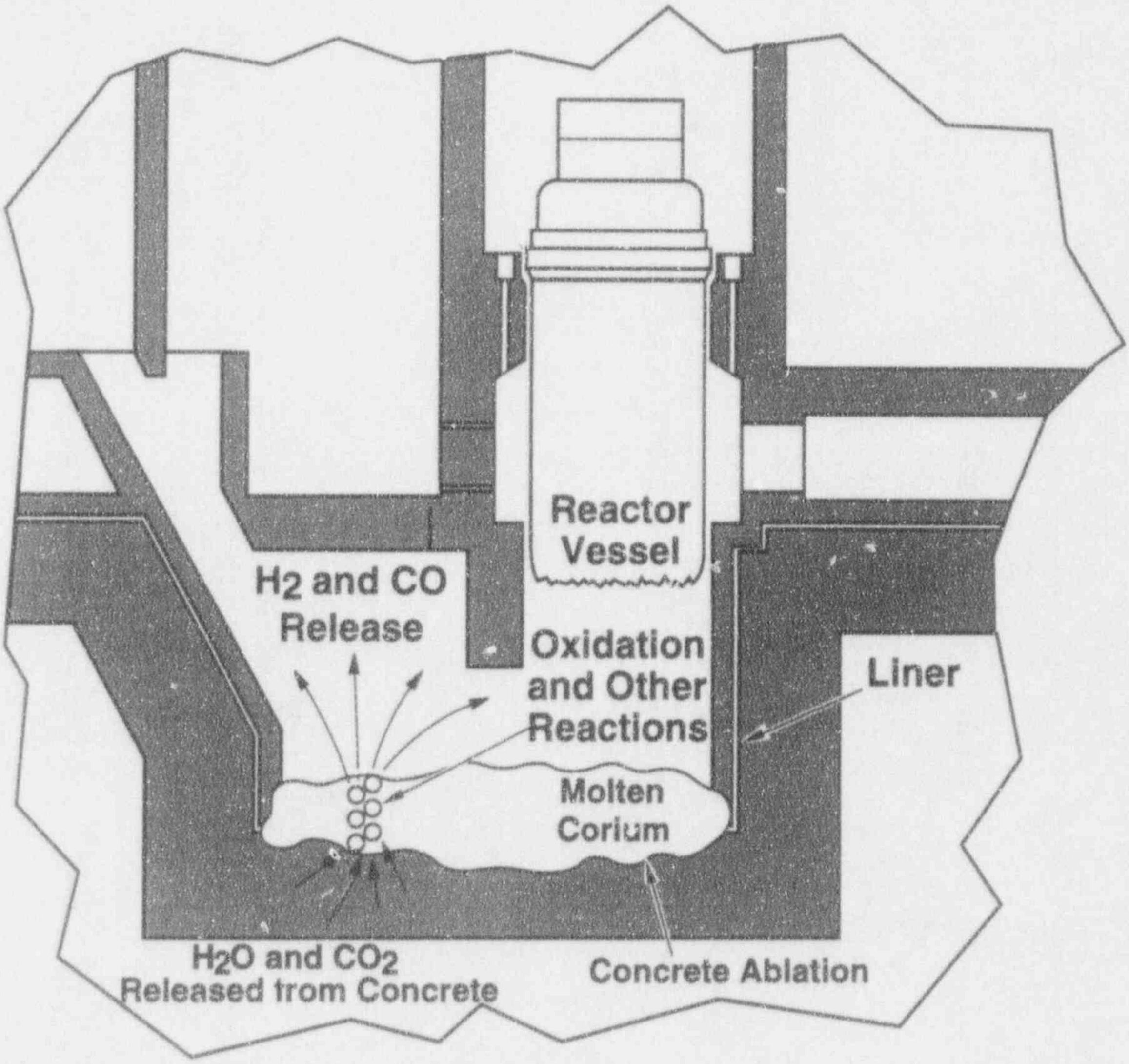


Figure 4.4-4 Combustible gas generation during CCIs

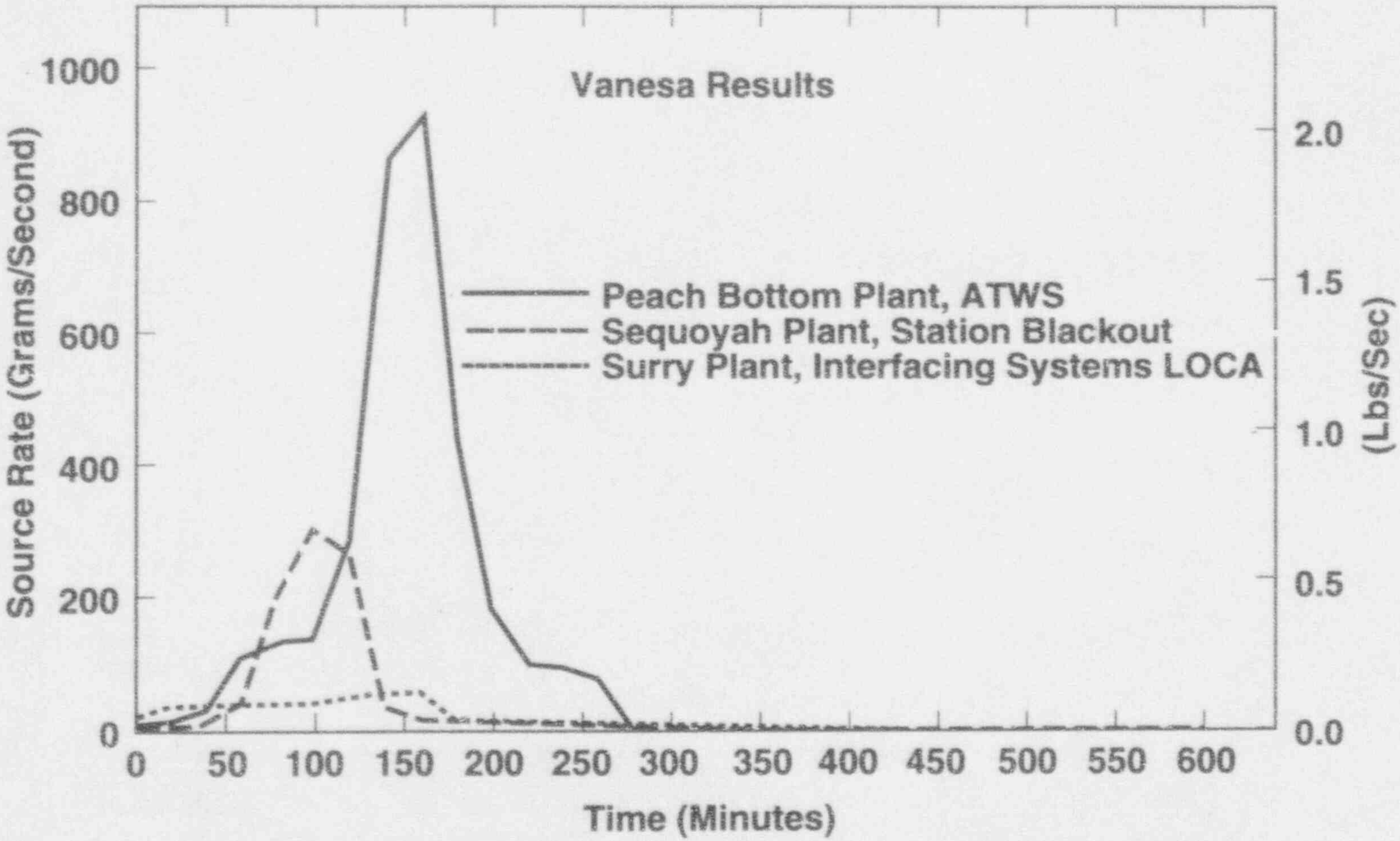


Figure 4.4-5 VANESA calculations of aerosol source rates

References for Section 4.4

1. ACRS Subcommittee Meeting Minutes (June 3, 1966), reproduced in Okrent, pp. 99-101.

2. R. K. Cole, Jr., D. P. Kelly, M. A. Ellis, *CORCON-Mod2: A Computer Program for Analysis of Molten-Core Concrete Interactions*, NUREG/CR-3920, SAND84-1246, Sandia National Laboratories, Albuquerque, NM, August 1984.

3. A. L. Camp, et al., *Light Water Reactor Hydrogen Manual*, NUREG/CR-2726, SAND82-1137, Sandia National Laboratories, Albuquerque, NM, August 1983.

4. C. J. Shaffer, L. A. Miller, A. C. Payne Jr., *Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant: Phenomenology and Risk Uncertainty Evaluation Program (PRUEP), Volume 3: MELCOR Code Calculations*, NUREG/CR-5305/3 of 3, SAND90-2765, Sandia National Laboratories, Albuquerque, NM, July 1992.

5. Proceedings, International Meeting on Light Water Reactor Severe Accident Evaluation, August 28-September 1, 1983, Cambridge, Massachusetts

6. M. Silberberg, et al., *Reassessment of the Technical Bases for Estimating Source Terms*, NUREG-0956, July 1986.

4.5 Direct Containment Heating (DCH)

A severe accident may progress with either high or low pressure in the reactor coolant system up to the point of vessel breach. Modules 2 and 3 discussed some of the accident scenarios that could involve high pressure at the time of vessel breach. When vessel failure occurs at a pressure of a few hundred psi (several hundred kPa) or more, the melt will be ejected as a jet into the reactor cavity. What happens next depends upon the reactor vessel pressure, the cavity and containment design, the presence of water in the cavity, the amount of melt ejected and other factors. One possibility, discussed earlier, is that a steam explosion will result in the reactor cavity, if sufficient water is available. Another possibility is that some of the melt will be fragmented by jet breakup and swept out of the cavity into the containment where it will heat the atmosphere (direct containment heating). This latter process can lead to very rapid and efficient heat transfer to the atmosphere, possibly accompanied by oxidation reactions and hydrogen burning that further enhance the energy transfer. The important phenomena are discussed in more detail below.

4.5.1 Ejection of Melt from the Vessel

The melt ejection process is depicted in Figure 4.5-1. Vessel failure may occur at a small opening, such as an instrument tube, or as a result of a larger rupture. The size of the opening is important in two ways, both related to the time required to eject the molten material. First, the amount of material participating in an ex-vessel steam explosion and the nature of the explosion will be affected by the ejection rate. Small amounts of molten material may result in small explosions that sweep water out of the cavity and preclude larger explosions. Second, if the hole is small, it may take many seconds or even several minutes to eject all of the molten material, thus allowing some time for containment heat transfer and reducing the peak pressure from direct heating. However, it appears that even small openings are likely to enlarge during the melt ejection process, as the melt erodes the metal surrounding the hole. Rapid enlargement of small holes to 1.5 feet (.5 m) or more are expected, resulting in ejection times on the order of several seconds.*

Along with the hole size, the amount and composition of molten material in the lower plenum of the vessel is also an important factor. In some scenarios, vessel failure may occur early, when only part of the core is molten. Core material that has not relocated to the lower plenum will not contribute significantly to the direct heating process. Figure 4.5-2 shows an example estimate of the amount of material that may be ejected for given core melt scenarios in PWRs.[1]

When the vessel first fails, molten material will be ejected as a liquid stream. As the liquid corium level in the vessel drops, gas blowthrough will begin to occur, resulting in a two-phase mixture blowing down from the vessel. The high velocity expanding gas flow provides the motive force for entraining corium and ejecting it from the reactor cavity.

* R. W. Ostensen, et al., *Models and Correlations for Direct Containment Heating*, Letter Report to the NRC, Sandia National Laboratories, March 15, 1991.

4.5.2 Interactions in the Reactor Cavity

When molten material is ejected into the reactor cavity at high pressure, there are a number of phenomena that are important to consider. The possibility of an ex-vessel steam explosion was already identified. Additional phenomena include molten jet breakup, gas evolution and chemical reactions, erosion of concrete in the cavity, and trapping of a portion of the jet before it can escape the cavity. These processes are depicted in Figure 4.5-3.

The presence of water in the reactor cavity could result in some quenched debris, thus partially mitigating the DCH threat. However, experimental evidence indicates that the presence of water in the reactor cavity can be very detrimental and will probably result in a steam explosion.* With small levels of water, the experiments show that the initial contact with molten debris produces a steam explosion that blows the remaining water out of the cavity, ending immediate debris-water interactions. Experiments with water-locked cavities have produced drastic steam explosions of sufficient magnitude to destroy the cavity itself. In addition to potential steam explosions, water also provides an additional source of hydrogen by interacting with the molten debris.

Jet breakup is important for several reasons. The resulting particle sizes influence the trajectories followed by the particles as they pass through the cavity, thus affecting the likelihood that they are trapped. Second, the particle sizes will affect the heat transfer and chemical reaction rates (by determining the available surface area), as well as particle transport within containment. Jet breakup is a very complex process in severe accidents. In addition to the expected hydraulic forces affecting the breakup, gas evolution within the jet and splashing off of the cavity walls can play important roles. The jet breakup does not occur instantaneously, but rather over a considerable distance that can allow for particle reagglomeration as well as breakup. Figure 4.5-4 shows some estimated particle sizes that can result for given conditions.

Gas evolution from the melt can result in changes in the jet breakup, and can also significantly affect fission product releases. The melt breakup process is likely to release most of the volatile materials and also allow formation of numerous radioactive aerosols, although these processes are not well understood. As the jet encounters water or steam (either from the blowthrough or as a result of water in the cavity), oxidation of any metals can occur, leading to rapid hydrogen production. Some experiments indicate that the gases exiting the reactor cavity can contain as much as 50% hydrogen during some phases of the blowdown.*

As the high-temperature jet passes through the cavity, melt is entrained and swept out into the containment. Gases exiting the reactor cavity may have velocities of several hundred feet per second (hundreds of m/s) according to some estimates.[2] As the melt is swept along, some of it impinges upon the cavity floor or walls. Significant erosion of concrete is not expected to occur because the melt will mostly splash off.

As the jet passes through the cavity, corium will bounce off of the walls, perhaps multiple times, as it is carried along by the gases. Ultimately, depending on the driving pressure, some fraction of the melt will be retained in the cavity and not enter the main containment. Particles may be trapped under a seal table or any other obstruction in the path of the jet, as long as the jet does not cut through the obstruction. Locations where the flow sharply changes direction may also collect debris. Note that the trapped material may result in subsequent core-concrete interactions within the reactor cavity.

* Memo from Richard Griffith to R. G. Gido, Sandia National Laboratories, May 11, 1992.

4.5.3 Energy Deposition and Pressure Rise in Containment

As core debris is swept out of the reactor cavity, it is transported throughout the containment. The degree to which the debris can be transported to the top of the containment affects the resulting pressure rise. In the lower regions of PWR containments, the containment is highly subcompartmentalized. It is expected that significant quantities of the core debris will be trapped in these subcompartments before it can reach the upper regions of containment. This trapping may significantly reduce the predicted containment pressure rise.

Suspended debris particles can rapidly transfer their energy to the containment atmosphere. Because of the small particle sizes, the total surface area for heat transfer is enormous. The amount of thermal energy available in a molten core was discussed previously in Module 3. This thermal energy can be transferred to the containment atmosphere through radiative and convective heat transfer. This heat transfer will be very rapid, with much of it occurring in a matter of seconds.

In addition to heat transfer, energy may be imparted to the containment atmosphere as a result of exothermic oxidation reactions involving metallic constituents in the core debris and either air or steam. The metal-steam reactions will result in the production of additional hydrogen. Hydrogen from these reactions plus hydrogen previously injected into containment may then burn, resulting in additional pressurization. The hot debris particles and the high temperatures of the exiting gases may lead to some hydrogen combustion even for mixtures outside the normal flammability limits (see Section 4.6).

Figure 4.5-5 shows examples from the NUREG-1150 study of the range of pressures considered possible for a DCH event in the Surry subatmospheric containment.[3] In that study, the important factors were considered to be the vessel pressure, the presence of water in the cavity, the vessel hole size, the core fraction ejected, the amount of zirconium oxidation, and the operation of containment sprays.

In Figure 4.5-5, the dry cavity case (Case 1) results in higher pressures than the equivalent wet cavity case (Case 2). In these estimates, steam explosions resulting in dynamic pressures damaging the cavity or other parts of the containment were not considered. Without steam explosion damage, water was predicted to be beneficial, with the heat absorption outweighing any detrimental effects of hydrogen production.

4.5.4 Containment Failure Probabilities for DCH

While DCH is possible, it is averted in many core melt accidents because they do not proceed to vessel breach at high pressure. First, many accidents are arrested in-vessel, prior to melt ejection. Second, many accidents involve vessel failure at low pressure, without the necessary driving force for DCH. BWRs may be depressurized as a result of a loss-of-coolant accident or relief valve operation. PWRs may be depressurized as a result of a loss-of-coolant accident or because of previous temperature-induced failure of the reactor coolant system (other than the bottom of the vessel), as discussed in Module 3.

As noted in Section 4.1, the estimated ultimate failure pressure for Surry is about 126 psig (870 kPa), although there are important uncertainties in that estimate. Based on the estimates in Figure 4.5-5 and the fact that many accidents are arrested in-vessel or proceed at low pressure, the Surry containment is not expected to fail in most accidents as a result of DCH. We have taken the information available from the files of the NUREG-1150 studies and estimated the conditional probability of containment failure at vessel breach for a variety of accident types at Surry. Those results are shown in Figure 4.5-6.

Current studies for selected large dry and subatmospheric PWR containments indicate that they would survive many expected DCH events. However, ongoing research indicates that the uncertainties are large and some types of PWR containment geometrics, such as those with direct venting from teh cavity to the upper containment, have not been studied. Therefore, the NRC has undertaken research in an Accident Management Program that has examined the efficacy of providing intentional depressurization capability for some types of PWRs. Thus far, no specific regulatory actions have resulted from this work. When evaluated from a risk perspective, intentional depressurization to preclude DCH has the possible detrimental effects of reducing the time for in-vessel recovery (for early depressurization) and increasing the possibility of in-vessel steam explosions.* The tradeoffs between the positive and negative aspects of intentional depressurization are not precisely quantifiable, and there is a possibility that temperature induced failures of the reactor coolant system may render the question moot.

There has been little research directed toward DCH in ice condenser and BWR containments. Ex-vessel steam explosions may be very important in deeply flooded ice condenser containment reactor cavities. In BWRs, the vessel will be depressurized for many accidents. However, if high pressure melt ejection occurs, the pedestal region is sufficiently confined that high local pressures are possible, that is, the gases can not be vented fast enough. Further, drywell pressurization leading to drywell failure can be very important. While code calculations have been performed for some of these cases, there is virtually no experimental data available to support evaluations of these containment types.

* Susan Dingman, Risk Sensitivity Evaluations for the Intentional Depressurization Strategy, Letter Report to the NRC, Sandia National Laboratories, Albuquerque, NM, March 1991.

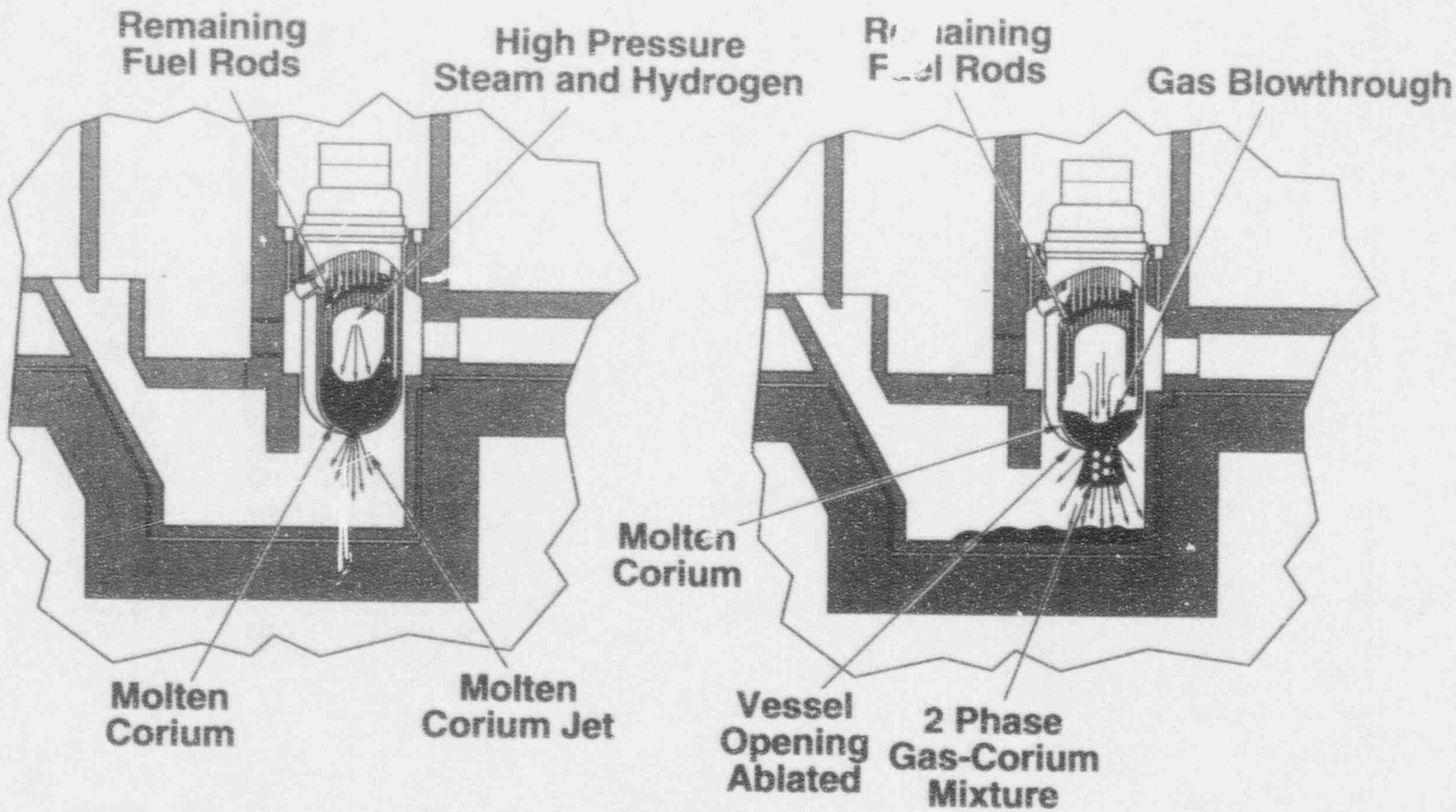


Figure 4.5-1 Melt ejection process

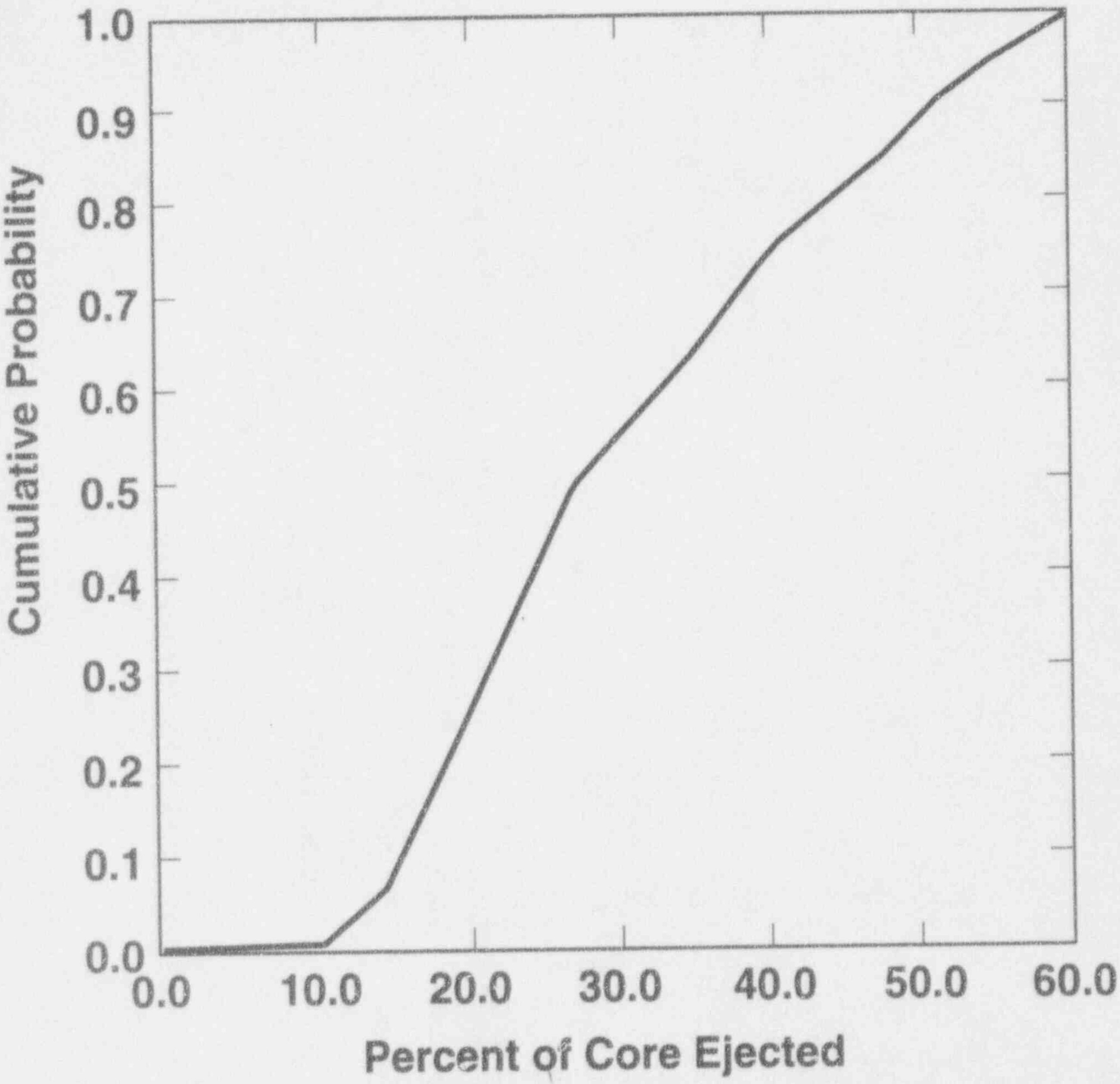


Figure 4.5-2 Distribution for fraction of core material ejected, PWR

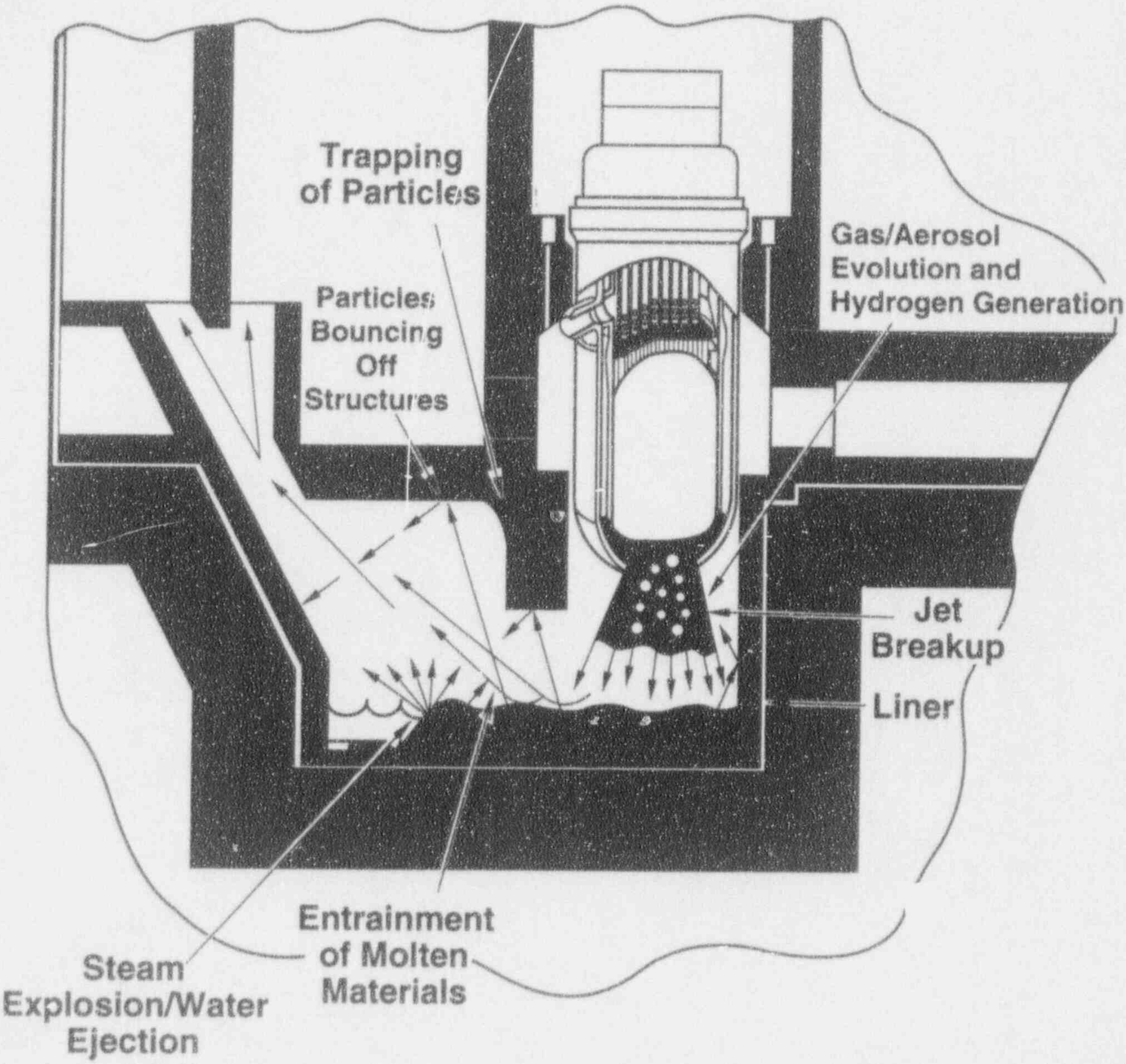


Figure 4.5-3 Reactor cavity interactions

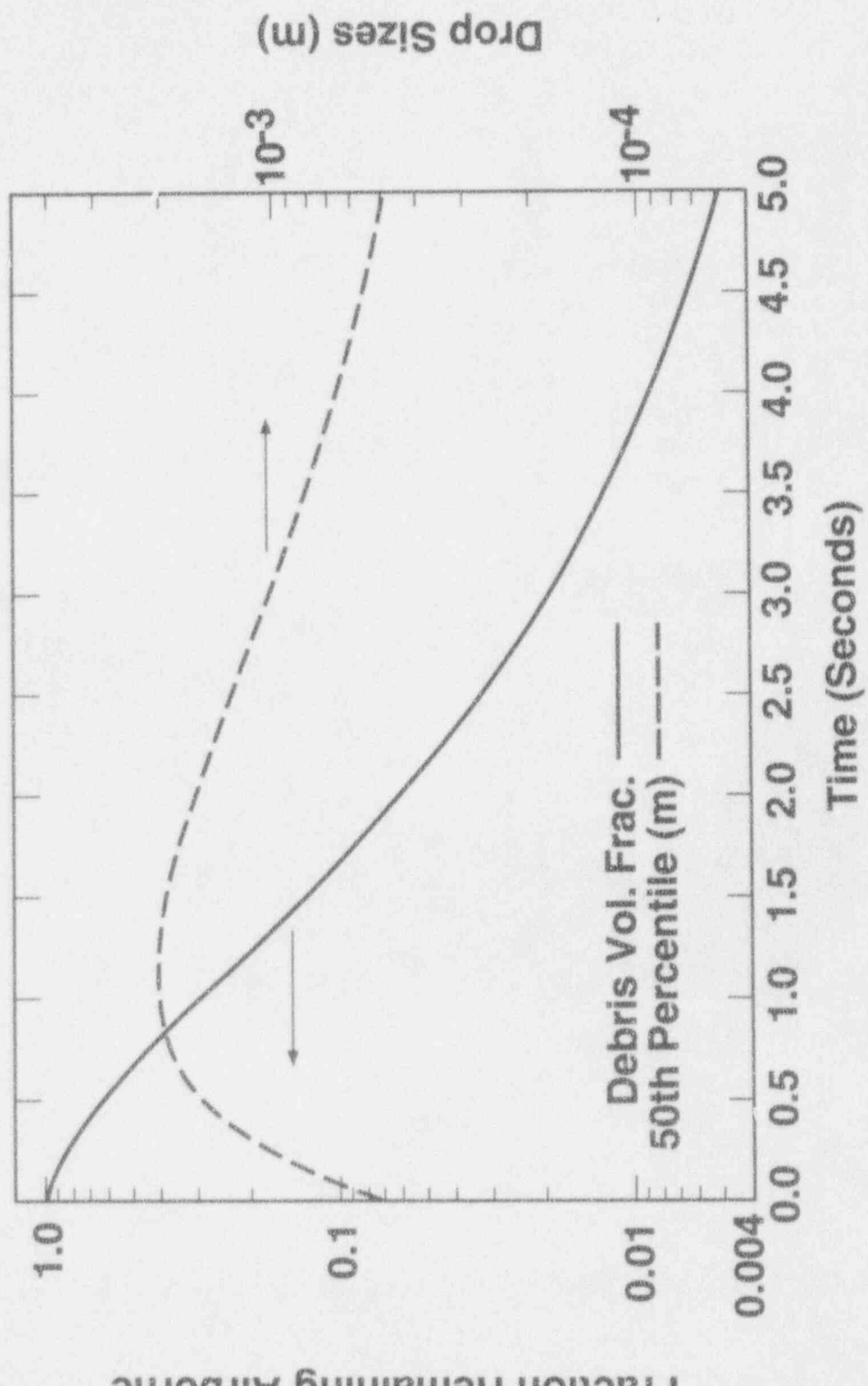
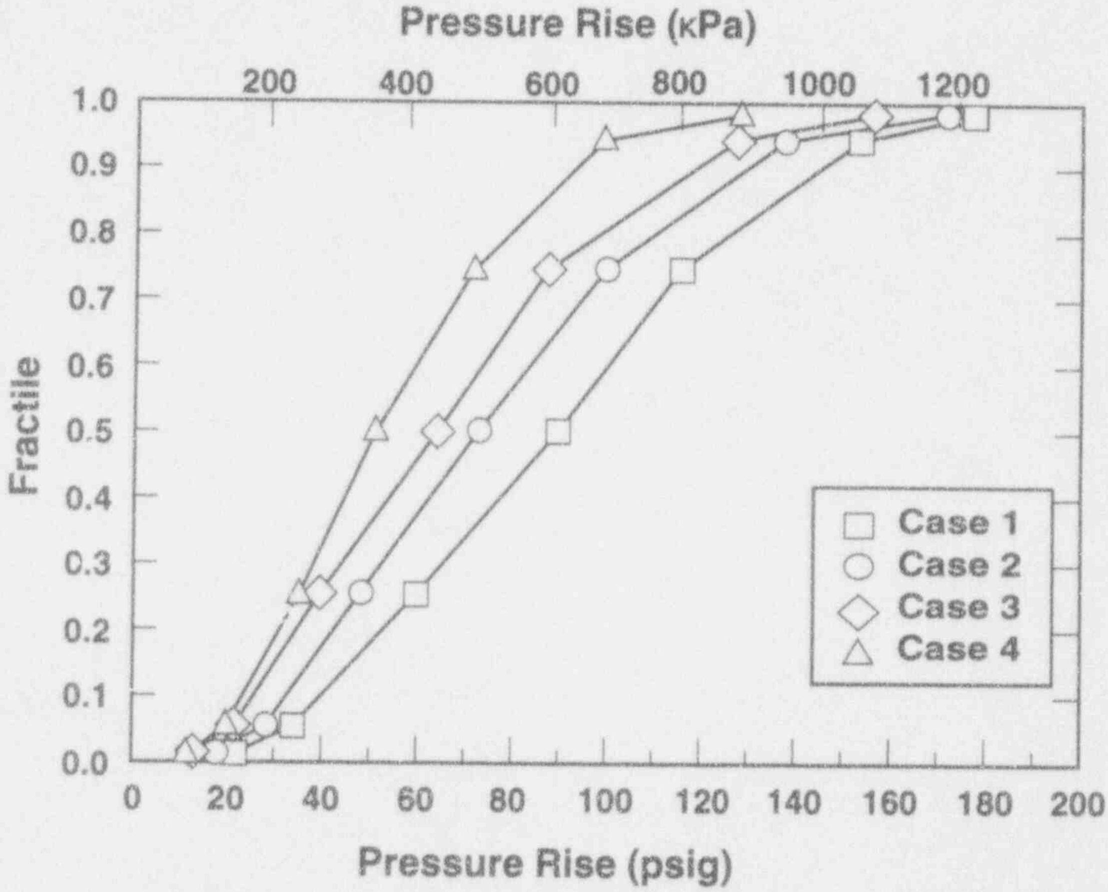


Figure 4.5-4 Estimated median partical size versus time



	RCS Pressure psi (MPa)	Vessel Hole Size $ft^2(m^2)$	Cavity	Core Fraction Ejected
Case 1	2000-2500 (13.8-17.2)	21.5 (2)	Dry	40-60%
Case 2	2000-2500 (13.8-17.2)	21.5 (2)	Wet	40-60%
Case 3	500-1000 (3.4-6.9)	21.5 (2)	Wet	40-60%
Case 4	500-1000 (3.4-6.9)	1.1 (0.1)	Dry	20-40%

Figure 4.5-5 Example distributions for pressure rise at vessel breach, Surry

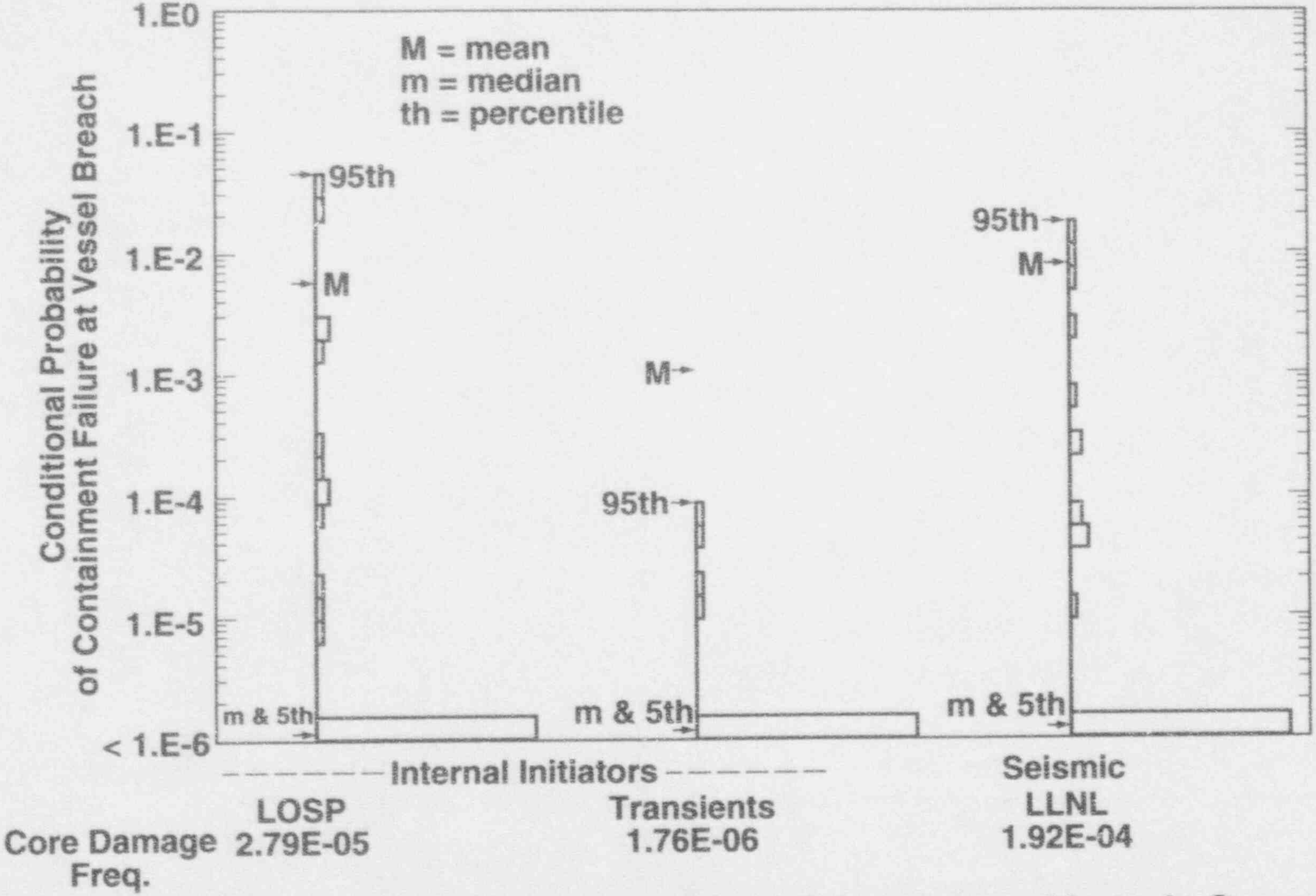


Figure 4.5-6 Containment failure probabilities at vessel breach, Surry

References for Section 4.5

1. F. T. Harper, et al., *Evaluation of Severe Accident Risks: Quantification of Major Input Parameters*, NUREG/CR-4551, SAND86-1309, Vol. 2, Rev. 1, Part 1, Sandia National Laboratories, Albuquerque, NM, December 1990.

2. F. T. Harper, et al., *Evaluation of Severe Accident Risks: Quantification of Major Input Parameters*, NUREG\CR-4551, SAND86-1309, Vol. 2, Rev. 1, Part 2, Sandia National Laboratories, Albuquerque, NM, April 1991.

4.6 Hydrogen Combustion

During the TMI-2 accident, hydrogen generated from in-vessel zirconium oxidation was released to the containment through the pressurizer relief valve. This hydrogen eventually ignited, resulting in a 28 psig (193 kPa) peak pressure in the containment. While this particular event did not threaten the TMI-2 containment, it raised awareness of the potential threats that might arise for other scenarios and for other containment types. The main concern over hydrogen combustion in nuclear reactor containments is that the high pressure generated might cause a breach of containment and a release of radioactivity. A second concern is that the resultant high temperature or pressure might damage important safety-related equipment. This section describes the physical mechanisms important to hydrogen combustion events, discusses the TMI-2 event in more detail, and describes the subsequent regulatory activities that have been taken to reduce the potential combustion threats. Much of the material in this section is excerpted from the *Light Water Reactor Hydrogen Manual.*[1]

4.6.1 Hydrogen Combustion Reaction

Combustion of hydrogen according to the reaction:

$$2H_2 + O_2 \rightarrow 2H_2O + \text{energy (heat)}$$

results in the release of about 5.2 x 10^4 Btu/lbm of hydrogen burned (57.8 kcal/gm-mole). Combustion waves are usually classified either as deflagrations or detonations. The term "explosion" usually refers to a detonation, but is somewhat ambiguous and should be avoided. Deflagrations are combustion waves in which unburned gases are heated by thermal conduction to temperatures high enough for chemical reaction to occur. Deflagrations normally travel subsonically and result in quasi-static (nearly steady state) loads on containment. Detonations are combustion waves in which heating of the unburned gases is due to compression from shock waves. Detonation waves travel supersonically and produce dynamic or impulsive loads on containment in addition to quasi-static loads. The pressure and temperature obtained from the complete combustion of hydrogen in air, adiabatically (without heat loss) and at constant volume, are shown in Figures 4.6-1 and 4.6-2. These figures show the ratio of initial to final pressures and final temperatures that could be expected for gas mixtures with low steam concentrations. Appendix 4A shows examples of pressure and temperature calculations for the types of air-steam-hydrogen mixtures that might occur in a reactor containment. In the following sections, the conditions necessary for combustion and the different combustion modes are discussed in detail.

4.6.2 Conditions Necessary for Combustion

Normally, for substantial combustion of hydrogen to take place, the gaseous mixture must be flammable, and an ignition source must be present. The special case of high temperature combustion is discussed later. For a flammable gas mixture, the flammability limits are defined as the limiting concentrations of fuel, at a given temperature and pressure, in which a flame can be propagated indefinitely. Limits for upward propagation of flames are wider than those for downward propagation. Limits for horizontal propagation are between those for upward and downward propagation.

The lower flammability limit is the minimum concentration of hydrogen required to propagate a flame, while the upper limit is the maximum concentration. At the lower limit, the hydrogen is in short supply and the oxygen is present in excess. At the upper limit of flammability for hydrogen in air, the oxygen is in short supply, about 5% oxygen by volume. The behavior of the upper limit of flammability of hydrogen with various mixtures such as air:steam is more easily understood if one considers it as the lower flammability limit of oxygen.

In large PWR containments we are usually interested in the lower limit of flammability, there being large amounts of oxygen present. In the much smaller BWR containments, particularly the inerted containments, we may be interested in the upper flammability limit.

For hydrogen:air mixtures, the flammability limits of Coward and Jones are still accepted.[2] Values for hydrogen flammability in air saturated with water vapor at room temperature and pressure are given in Table 4.6-1. These limits may vary slightly during accident conditions. There may be scale effects due to the large size of reactor containments as well as variations in flammability due to the ignition source strength.

In reactor accidents the conditions inside containment prior to hydrogen combustion may include elevated temperature, elevated pressure, and the presence of steam. The flammability limits widen with increasing temperature. For example, at 212°F (100°C) the lower limit for downward propagation is approximately 8.8% (see Figure 4.6-3).

If the containment atmosphere is altered by the addition of carbon dioxide, steam, nitrogen, or other diluent, the lower flammability limit will increase slowly with additional diluent, while the upper flammability limit will drop more rapidly. With continued increase in diluent concentration the two limits approach one another until they meet and the atmosphere is inerted. A flame cannot be propagated a significant distance for any fuel:air ratio in an inerted atmosphere. The addition of diluents has been proposed as a hydrogen mitigation strategy. Figure 4.6-4 shows the flammability limits with the addition of excess nitrogen or carbon dioxide. Note that for 75% additional nitrogen, the atmosphere is inert.[3,4] This corresponds to 5% oxygen at the limit of the flammable region, a value very close to that of the upper limit for hydrogen:air combustion. For carbon dioxide, the atmosphere is inerted when the carbon dioxide concentration is 60% or above, corresponding to 8% oxygen or less. The larger specific heat of carbon dioxide reduces the flame temperature and flame velocity; hence carbon dioxide suppresses flammability more than nitrogen. It requires about 60% steam to inert hydrogen:air:steam mixtures. The triangular diagram of Shapiro and Moffette indicates regions of flammability of hydrogen:air:steam mixtures.[4] It has been widely reproduced and appears as Figure 4.6-5.

Ignition of dry hydrogen:air mixtures, particularly when the mixtures are well within the flammability limits, can occur with a very small input of energy.[4] Common sources of ignition are sparks from electrical equipment and from the discharge of small static electric charges. The minimum energy required from a spark for ignition of a quiescent hydrogen:air mixture is of the order of 10^{-7} BTU (a very weak spark). The ignition energy required as a function of hydrogen concentration is shown in Figure 4.6-6.[5] For a flammable mixture, the required ignition energy increases as the hydrogen concentration approaches the flammability limits. The addition of a diluent, such as steam, will increase the required ignition energy substantially. As mentioned previously, high energy ignition sources can cause mixtures outside the flammability limits to burn for some distance.

4.6.3 Deflagrations

Deflagrations are flames that generally travel at subsonic speeds relative to the unburned gas. Deflagrations propagate mainly by thermal conduction from the hot burned gas into the unburned gas, raising its temperature high enough for a rapid exothermic chemical reaction to take place. The propagation of a deflagration can be understood by examining the flammability limits discussed in the previous section. Consider a quiescent mixture of hydrogen:air. For hydrogen concentrations below about 4.1% there will be no significant propagation away from an ignition source. For hydrogen concentrations between 4.1 and 6.0%, there will be upward propagation from the ignition source. Hydrogen concentrations between 6.0 and 9.0% will produce both upward and horizontal propagation, and hydrogen concentrations above 9.0% will produce propagation in all directions, although the upward propagation may be faster than the downward propagation. Exact values for propagation limits will, of course, vary with temperature, pressure, and the presence of diluents. The degree of turbulence is also very important with turbulence tending to enhance combustion as long as the turbulence is not violent enough to "blow out" the flame.

It has been found in laboratory experiments that when hydrogen:air mixtures with hydrogen concentrations in the range 4-8% were ignited with a spark, some of the hydrogen was not burned.[6,7,8,9,10] The resultant pressure rise was below that predicted for complete combustion, as shown in Figure 4.6-7. Experimental results with a spark ignition source indicate that the completeness of combustion in quiescent mixtures increases with increasing hydrogen concentration, and is nearly complete at about 8-10% hydrogen. The range of incomplete combustion corresponds to the range in which the mixture is above the flammability limit for upward propagation, but below the flammability limit for downward propagation. As shown in Figure 4.6-7 for the "fans on" cases, turbulence and mixing of the gases can significantly increase the completeness of combustion. The additional variations in Figure 4.6-7 for mixtures below 8% tend to result from variations in the geometry and scale of the experiments.

Another important parameter when studying deflagrations is the flame speed. The flame speed determines how much time is available for heat transfer during a burn. Heat transfer results in pressures and temperatures below those predicted in Figures 4.6-1 and 4.6-2. The dominant heat transfer mechanisms are evaporation of containment sprays, radiation, and convection. Some plants also contain fan coolers. Normally, if the sprays are on, they will dominate the heat transfer process. Radiation heat transfer can also be important due to the high gas temperatures expected during a hydrogen burn. Convection may be less significant over the short time of a burn. One note is that the presence of sprays may significantly increase the flame speed due to the increased turbulence induced by the sprays. Typically, pressure rises above 80% of the adiabatic pressure rises are predicted for reasonable values of the flame speed, assuming complete combustion.

As shown in Figure 4.6-8, laminar burning velocities are quite slow. The laminar burning velocity (in a Lagrangian sense) denotes the speed of gases at a steady burner. Propagating laminar flames have flame speeds (in an Eulerian sense) which are 5-7 times faster due to volumetric expansion of the burned gases. The maximum laminar burning velocity of hydrogen:air mixtures is about 9.8 fps (3 m/s) near a concentration of about 42% hydrogen. The burning velocity becomes much smaller as the flammability limits are approached.

In a reactor containment, it is likely that a laminar deflagration will become turbulent. Turbulent flames can have average burning velocities 2 to 5 times the laminar burning velocity. Therefore, a hydrogen combustion event can occur in a containment in a matter of seconds, as opposed to the long times predicted by the laminar burning velocities. If the turbulent flame speed (laboratory system) becomes greater than about one-tenth of the sound speed (the sound speed is approximately 1150 fps (350 m/s) in containment air), shock waves will be formed ahead of the flame front. In that case, dynamic loads, in addition to static loads, will be imposed on the containment structure. The mechanisms leading to flame acceleration and detonation will be discussed in the next section.

4.6.4 Detonation of Hydrogen

A detonation is a combustion wave that travels at supersonic speeds relative to the unburned gas in front of it. For hydrogen:air mixtures near stoichiometric this speed is about 6600 fps (2000 m/s)(see Figure 4.6-9). The compression of the unburned gas by shock waves in the detonation raises the gas temperature high enough to initiate rapid combustion.

We will attempt to answer as well as possible the following three questions:

1. Under what conditions is a hydrogen:air or hydrogen:air:steam detonation possible in containment?
2. If a detonation is possible, what is the likelihood that it will occur?
3. What pressure loads could a detonation cause?

We can answer the first question fairly well (at least with regard to hydrogen:air mixtures) and also the third question. The second question concerns the transition from deflagration to detonation and is still not completely understood after more than 50 years of investigation. We can say that, in most postulated reactor accident scenarios, deflagrations are much more likely than detonations.

4.6.4.1 Detonation Limits

Hydrogen:air mixtures near stoichiometric (about 29% hydrogen, two parts H_2 to one part O_2) are known to be detonable. Mixtures departing from stoichiometric, either in the hydrogen-lean or hydrogen-rich direction are increasingly more difficult to detonate. It has been observed that "detonation limits" are functions of geometry and scale, and not universal values at given mixture concentrations, temperatures and pressures.[11,12,13] Our understanding of the possibility of sustaining a detonation in hydrogen:air mixtures, as well as other gas mixtures, has greatly increased within the last few years. It has been found that a detonation wave is composed of unsteady oblique shock waves moving in an everchanging cellular structure (characterized by its transverse dimension), a "foamy" detonation front.

The cell size, λ, in a detonation is a fairly easy quantity to measure. The farther a mixture is from stoichiometric, and hence the less energetic the chemical reaction, the larger is the detonation cell size. It appears that the smallest diameter tube in which a detonation will propagate is one whose diameter is about a third of a cell width. The cell width for hydrogen:air has been accurately measured over an extensive range of hydrogen:air ratios (see Figure 4.6-10).[13] For example, at 16% hydrogen the cell size is about 9.6 in. (24.5 cm). This means that a 16% hydrogen mixture detonation should be able to propagate down a tube 3.2 in. (8.2 cm) in diameter. The larger the tube diameter, the wider is the range of detonable hydrogen concentrations.

The knowledge of hydrogen:air cell size is valuable for evaluating detonation concerns in particular geometries. It is known that if a detonation is to propagate from a tube into an open space, there is a minimum tube diameter for which the detonation will propagate, the critical tube diameter. For smaller tube diameters, the detonation will fail when leaving the tube. Experimental results show that the critical tube diameter is about 13 cell widths. For a 16% hydrogen mixture the critical tube diameter is therefore 10.5 ft. (3.19 m). For a rectangular duct, the critical duct height varies from about 11 cell widths (for a square duct) to about 3 (for a wide duct). For propagation into an open space confined on one side of the duct, there is some evidence that the critical duct height lies between 1.5 and 5.5 cell widths. Figure 4.6-11 shows the relationship between geometry and cell size for the geometries discussed above.

The detonability of a mixture is increased with increasing temperature. For example, in a 17 inch (43 cm) tube at 68°F (20°C), a detonation can be propagated in a mixture with 11.7% hydrogen. At 212°F (100°C), the detonability limit changes to 9.5% hydrogen.[14]

The information provided above helps to answer the first question, "Under what conditions is a hydrogen:air detonation possible in containment?" The detonation limits are not fixed but depend on the geometry and are wider for larger sizes and higher temperatures. The curve of cell size versus hydrogen fraction rises steeply on the hydrogen-lean side. For the large geometrical scales in containments, detonations may propagate in leaner mixtures than has been demonstrated in small and medium scale experiments.

4.6.4.2 Transition to Detonation

A detonable mixture may only deflagrate (burn) and not detonate. Detonations can start directly by the use of a vigorous shock wave coming from a high explosive, strong spark, or laser. Approximately 0.035 oz. (1 gm) of tetryl explosive will initiate a spherical detonation of a stoichiometric hydrogen:air mixture. The increase in explosive charge required as the mixture departs from stoichiometric is roughly proportional to the increase in detonation cell size. Detonations can also start from deflagrations that accelerate to high speeds pushing shock waves ahead of the burn front until at some point shock heating is sufficient to initiate the detonation. Sources of such highly accelerated flames are high speed jets coming from semiconfined regions and flames passing through fields of obstacles.

Many obstacles that might potentially cause flame acceleration, such as pipes and pressure vessels, are present in the lower sections of most containments. Very fast burns may also occur due to the presence of a very intense ignition source, such as a jet of hot combustion products formed subsequent to ignition in some adjoining semi-confined volume.

Deflagration-to-detonation transition is probably the least understood aspect of detonation theory at this time. Measurements have been made of the distance required to have transition to detonation in smooth tubes. Distances many times the tube diameter have been required. If obstacles are inserted into the tube, the required distance to detonation is greatly reduced. The motion of the expanding gases around the obstacles leads to greatly increased flame front area, rapid flame acceleration and rapid transition to detonation. Confinement greatly promotes transition, but one cannot rule out transition to detonation in a containment if a detonable mixture of sufficient size is present. The second question, "If a detonation is possible, what is the likelihood that it will occur?" therefore cannot be answered with certainty at present.

4.6.4.3 Detonation Pressures and Temperatures

For the purpose of studying the pressures and temperatures caused by a detonation, it is sufficient to ignore the detonation wave structure and consider it as a thin surface, a discontinuity. Chapman and Jouguet assumed that the detonation traveled at a speed such that the flow behind the detonation was sonic relative to the detonation. With this assumption one can compute a unique detonation speed for each hydrogen:air mixture, and find the corresponding temperature and pressure behind the detonation wave. The results are shown in Figures 4.6-12 and 4.6-13. It is an experimental fact that the measured speeds of detonations are approximately equal to the calculated Chapman-Jouguet values.

The burned gases behind a detonation are moving in the direction of the detonation. When a detonation hits a rigid wall, the gases must be brought to rest. This is accomplished by a reflected shock wave. We will consider only the case of a detonation wave striking a wall at normal incidence. The reflected shock wave further compresses the burned gas, increasing the detonation pressure by a factor of about 2.3. The pressures and temperatures predicted behind the normally reflected shock wave are also shown in Figures 4.6-12 and 4.6-13. In a containment one expects wave reflections from walls and obstacles to give rise to complex shock wave patterns. Wave interactions may lead to dissipation or, possibly, to wave focusing which can give rise to very high local peak pressures.

4.6.4.4 Local Detonations

In all the previous sections on detonations it has been assumed that the detonation is taking place in a homogeneous combustible mixture. Such detonations are global, traveling throughout the containment. With the exception of the strongest containments, containments will probably not be able to withstand the quasi-static pressure (adiabatic isochoric pressures) generated after the detonation, even without the additional dynamic loads due to detonation. It is therefore more appropriate to consider the effect of detonations when only a local portion of the containment atmosphere is detonable.

Consider a detonable cloud of hydrogen:air surrounded by air. As the detonation wave leaves the cloud, it will change into an expanding decaying shock wave. The shock wave intensity drops fairly rapidly if the shock wave expands spherically. Within a distance equal to 3 cloud radii, the shock wave pressure will drop to a value low enough to no longer threaten the containment structure. However, it has been found in detailed computer calculations that, because of the containment geometry, the shock waves may be focused in local regions, such as the top center of the containment dome, giving rise to large local peak pressures and impulses.[15,16] Local detonations may be dangerous in and near the detonable cloud, and may be dangerous at locations farther away if shock focusing effects are significant.

There are several locations to consider where high hydrogen concentrations are possible. These include:

1. Near the hydrogen release point,
2. Under ceilings or in the dome due to the rise and stratification of a low density plume, or
3. Near steam removal locations such as ice condensers, suppression pools, and fan coolers.

A detonable mixture requires adequate hydrogen and oxygen, but not too much steam. Regions of stratification tend to be difficult to establish and maintain in a turbulent containment environment. Steam removal locations are generally a more significant concern for local detonations.

4.6.4.5 Missile Generation

Missiles may be generated when combustion (deflagration or detonation) occurs in a confined region or when a propagating combustion front produces dynamic pressure loads on equipment. Such missiles may pose a threat to the containment structure itself, as well as representing a potential threat to safety and control equipment. For instance, electrical cables may not be expected to withstand the impact of a door or metal box. The actual risk to plant safety posed by missiles generated from hydrogen combustion depends upon a number of independent factors and is very difficult to predict.

4.6.5 Continuous Combustion

The preceding discussions have dealt with the discrete combustion events associated with hydrogen:air:steam mixtures in containment. There are also mechanisms for continuous combustion that are possible in some containments and for certain accident scenarios. Hydrogen may enter containment as part of a turbulent jet from a pipe break or relief valve or may enter as part of a buoyant plume from the top of a suppression pool or from core-concrete interactions. The hydrogen may be accompanied by large quantities of steam or, in the case of core-concrete interactions, carbon monoxide which is also flammable. The primary threat to nuclear power plants from continuous combustion is the temperature rise and the possible effect on equipment and structures. Pressure increases from continuous combustion will not generally threaten the containment.

Hydrogen that enters containment may start to burn as a turbulent diffusion flame. A diffusion flame is one in which the burning rate is controlled by the rate of mixing of oxygen and fuel. The nature of the flame is determined by the Froude Number, which is the ratio of the momentum forces to the buoyant forces in the jet or plume. Figure 4.6-14 shows the types of flames that can occur for different source diameters and flow rates. For the hydrogen to burn, it is necessary that at some locations the hydrogen:air:steam mixture be within flammability limits.

Combustion can begin either because of an outside ignition source, or because the mixture temperature is above the spontaneous ignition temperature. Shapiro and Moffette in 1952 presented experimental results on the spontaneous ignition temperature of hydrogen:air:steam mixtures (see Figure 4.6-15).[17] The spontaneous ignition temperature is in the range of 959-1076°F (515-580°C). Above this temperature, combustion can occur without external ignition sources such as electrical sparks. For example, continuous combustion may occur in a reactor cavity above core-concrete interactions in a dry cavity. In this case, the combustion will be limited by the availability of oxygen. However, if any oxygen is present, hydrogen and carbon monoxide can react even if the mixture is not within normal flammability limits.

Turbulent jets, such as from a pipe break, tend to autoignite at higher temperatures than buoyant plumes. Experiments have shown that such jets can autoignite at temperatures above 1166 to 1346°F (630-730°C).[18] A stable flame will occur at a distance from the orifice such that the turbulent burning velocity is equal to the gas flow velocity. There is evidence to suggest that for a particular set of conditions (temperature, pressure, and composition), there is a minimum orifice diameter for flame stability.[19] This minimum diameter is typically on the order of a few hundredths of an inch (millimeters) or less, and therefore, all practical sized orifices will support a stable hydrogen flame. Turbulent jets of hydrogen can also accompany direct containment heating. Hydrogen may already be present in containment, with additional hydrogen coming from in-vessel and from oxidation reactions during the melt ejection process. The hot particles and high temperature gases will serve to ignite the hydrogen, resulting in an additional energy contribution to the direct containment heating process. As noted in Section 4.5, very rich mixtures of hydrogen may be found at the exit of a reactor cavity, raising the possibility of a detonation.

4.6.6 Combustion at TMI-2

The TMI-2 accident was discussed at some length in Module 2. During the core heatup and degradation process, hydrogen was generated and released to containment through the pressurizer relief valve and the quench tank. Estimates of the total amount of hydrogen generated range from 594 to 814 lbm (270 - 370 kg).[20] This amount of hydrogen corresponds to oxidation of about 40% of the zirconium in the core. Approximately 9 hours and 50 minutes into the accident, a hydrogen deflagration occurred, resulting in a 28 psig peak pressure in containment (see Figure 4.6-16). The ignition source is not known, but could have been an electrical spark from a variety of sources.

The pressure rise observed at TMI-2 is consistent with the estimates of the generation and relatively complete combustion of between 7 and 8.2% hydrogen. The TMI-2 containment has a volume in excess of 2 x 10^6 ft^3 (5.7 x 10^4 m^3) and a failure pressure far in excess of 28 psig (193 kPa). However, BWR containments and PWR ice condenser containments are much smaller than TMI-2, and the same quantity of hydrogen could have resulted in a detonable mixture in those containments. The realization that hydrogen combustion could cause containment failure in smaller containments led to regulatory actions, as discussed in the following section.

4.6.7 Hydrogen Control Requirements

In general, there are very few regulations and guidelines dealing with beyond-design-basis accident phenomena in reactor containments. For example, there are no specific rules dealing with core-concrete interactions, ex-vessel steam explosions, or direct containment heating. Such phenomena are indirectly addressed by the large release safety goal discussed in Modules 1 and 2. Hydrogen control has been an exception to this approach, with significant regulations passed following the TMI-2 accident.

Limited hydrogen control was provided prior to TMI-2 in the form of hydrogen recombiners that could remove the small amounts of hydrogen that might be generated during a design-basis loss-of-coolant accident. However, these recombiners have virtually no value for the large quantities of hydrogen that could be generated during a severe accident. Therefore, the NRC took additional steps to protect the reactors considered most vulnerable to hydrogen combustion.

The hydrogen rule is contained in 10 CFR 50.44.[21] In 1981, the NRC ordered that all BWRs with Mark I and Mark II containments be inerted during normal operation to preclude the possibility of combustion. These containments are small enough that relatively low levels of zirconium oxidation could produce detonable mixtures in containment. Although inerting will prevent combustion within the containment, hydrogen can enter the surrounding reactor building of a Mark I or II containment if the containment fails or is vented through structurally inadequate flow paths. This hydrogen can burn, presenting a thermal hazard for safety equipment located in those buildings.

BWR Mark III containments and PWR ice condenser containments were the object of long and controversial examination. A variety of hydrogen control measures were considered by both the industry and the NRC. These measures included inerting, partial inerting, water fogs and foams, and deliberate ignition systems. Because of the need to enter containment for various operational activities and risks to personnel, the utilities opposed inerting approaches. Some other approaches, such as water fogs and foams, were not successfully demonstrated as practical prior to the decisions that were reached. Ultimately, the industry and NRC agreed on the deliberate ignition approach, even though other options are allowed under 10 CFR 50.44. The deliberate ignition approach is discussed in more detail below.

The acceptance of deliberate ignition as a viable strategy is based in part on a couple of controversial assumptions in the hydrogen rule. The TMI-2 accident did not result in vessel breach, and only about half of the available zirconium was oxidized. Therefore, the hydrogen rule was set up to address only degraded core accidents and not full scale melting and vessel breach. Consistent with the assumption that vessel breach does not occur, the limit of zirconium oxidation was set to 75% of the fuel cladding, not including channel boxes in BWRs. Greater amounts of hydrogen were not expected to be consistent with an accident in which most of the core did not melt or the vessel was not breached. Further, because the vessel is not breached, the release of hydrogen to containment was expected to occur over time periods of at least many minutes, if not longer. The large puff release that might accompany vessel breach or ex-vessel steam explosions does not need to be considered in meeting the hydrogen rule. It is also interesting to note that, while the fuel damage is assumed to be arrested at some point, the reflooding process is assumed to not produce oxidation in excess of 75% and to not result in a large burst of hydrogen. Therefore, only a select subset of beyond-design-basis accidents is addressed.

Deliberate ignition is based on the premise that hydrogen can be burned off in small quantities as it enters the containment. Either numerous small deflagrations or continuous combustion may occur, resulting in minimal pressure rise in containment, although the temperature effects must be considered. If the containment is not steam-inerted, then lean mixtures will be combusted until either the hydrogen or oxygen is depleted. As shown in Figures 4.1-5 and 4.1-9, igniters are located throughout containment to assure that locally high concentrations of hydrogen are avoided. These igniters are typically glow plugs, requiring AC power to function.

There are some limitations and concerns associated with igniters. First, they require AC power and will not function during station blackout. Further, if the containment is filled with hydrogen and power is later restored, they could provide a distributed ignition source if the operators do not think to keep them turned off. Second, there are two regions where higher than average hydrogen concentrations are possible. One is within an ice condenser and the other is above a Mark III suppression pool. In both cases, a steam-rich mixture may enter the condensing region, and the gas may emerge very hydrogen-rich. This is particularly true for rapid releases of hydrogen. A third concern relates to accidents beyond degraded core and to reflooding. Very rapid releases of hydrogen, such as associated with vessel breach or late reflooding, may overwhelm the igniters so that the effect is the same as for a large deflagration. A fourth possibility concerns sequences in which the containment sprays do not function and the containment becomes steam inert. If the hydrogen accumulates in the inert atmosphere, and the sprays are later recovered, a large burn may occur when the containment deinerts.

Despite the concerns raised above, hydrogen igniters are expected to have a positive benefit in many accidents. However, persons responsible for managing accidents need to be aware of the possibilities and use the igniters appropriately.

No additional hydrogen controls have been required for large dry or subatmospheric containments. These containments are large enough and strong enough that deflagrations are not expected to threaten them, except in conjunction with other phenomena. Local detonations are possible, but not considered likely for many accidents.[22] Detonable mixtures involving most of the containment can not be achieved without complete oxidation of all zirconium, **plus** additional hydrogen generation from steel oxidation or core-concrete interactions. A large detonation would require all of this hydrogen to be generated, that none of it burn previously, and that the burn undergoes a transition to a detonation. This combination of events is considered unlikely.

Table 4.6-1. Hydrogen Flammability Limits in Steam-Saturated Air at Room Temperature

	Lower Limit Vol. % of Hydrogen	Upper Limit Vol. % of Hydrogen
Upward Propagation	4.1	74
Horizontal Propagation	6.0	74
Downward Propagation	9.0	74

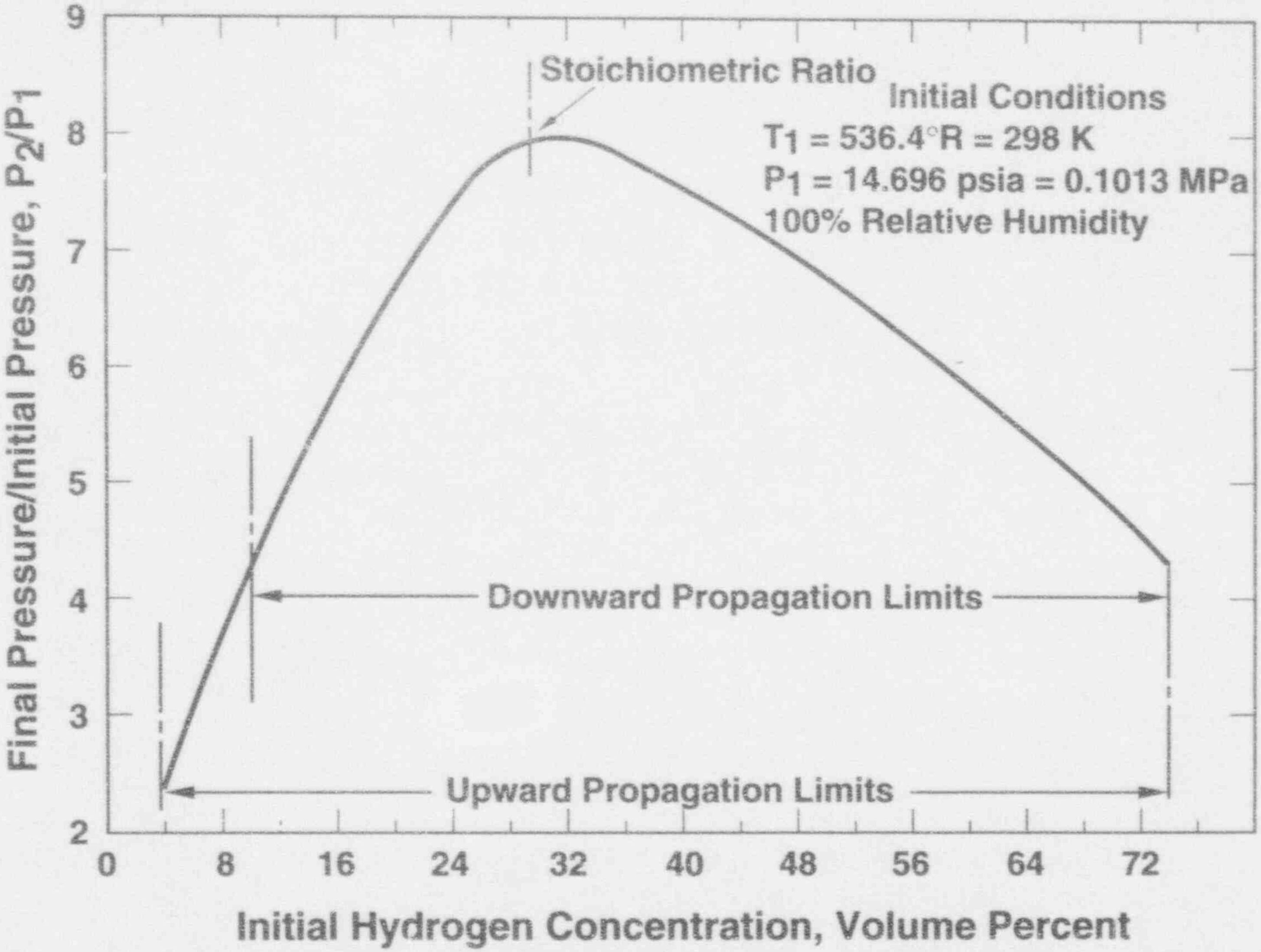


Figure 4.6-1 Theoretical adiabatic, constant-volume combustion pressure for hydrogen : air mixtures

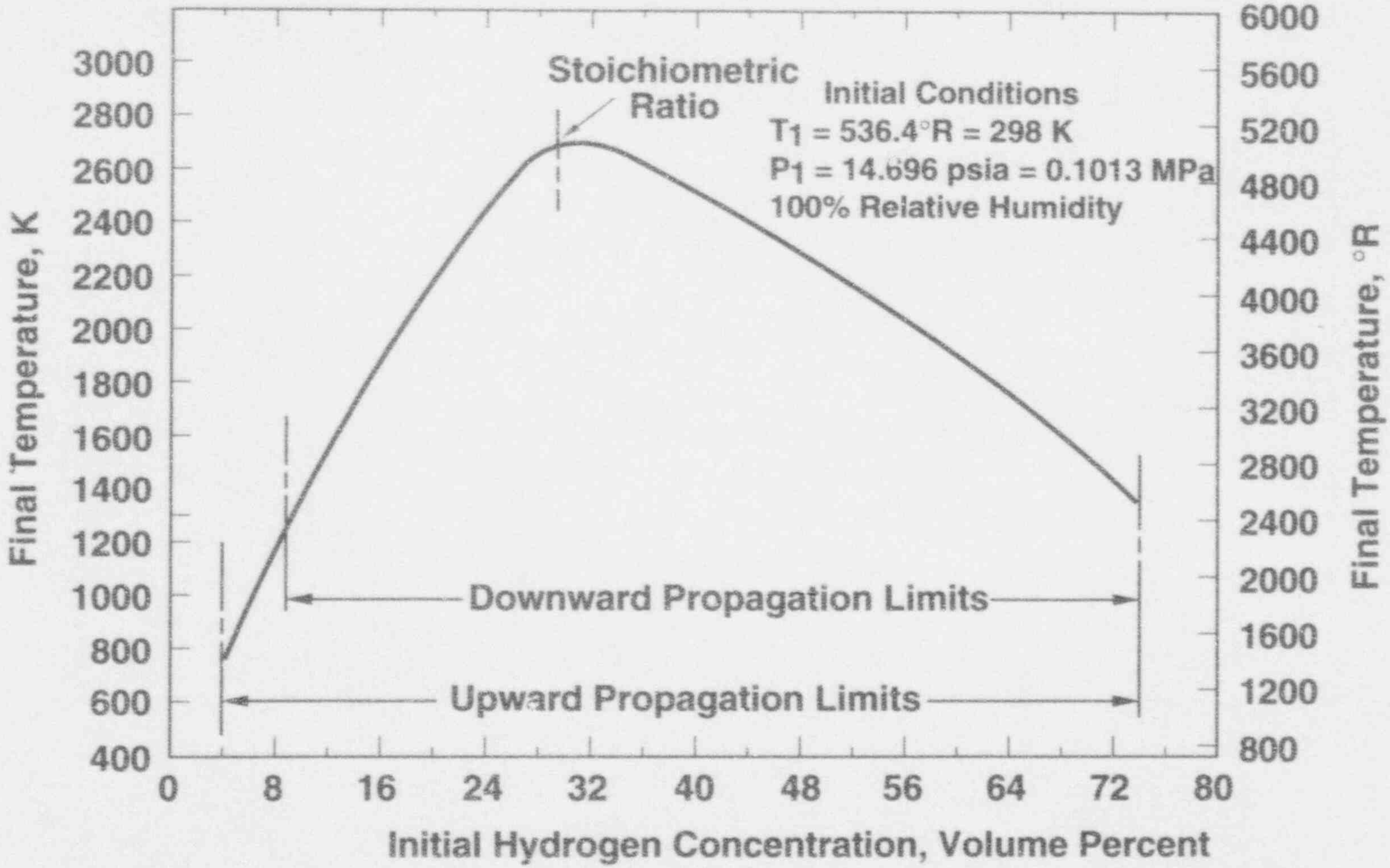


Figure 4.6-2 Theoretical adiabatic, constant-volume combustion temperature for hydrogen : air mixtures

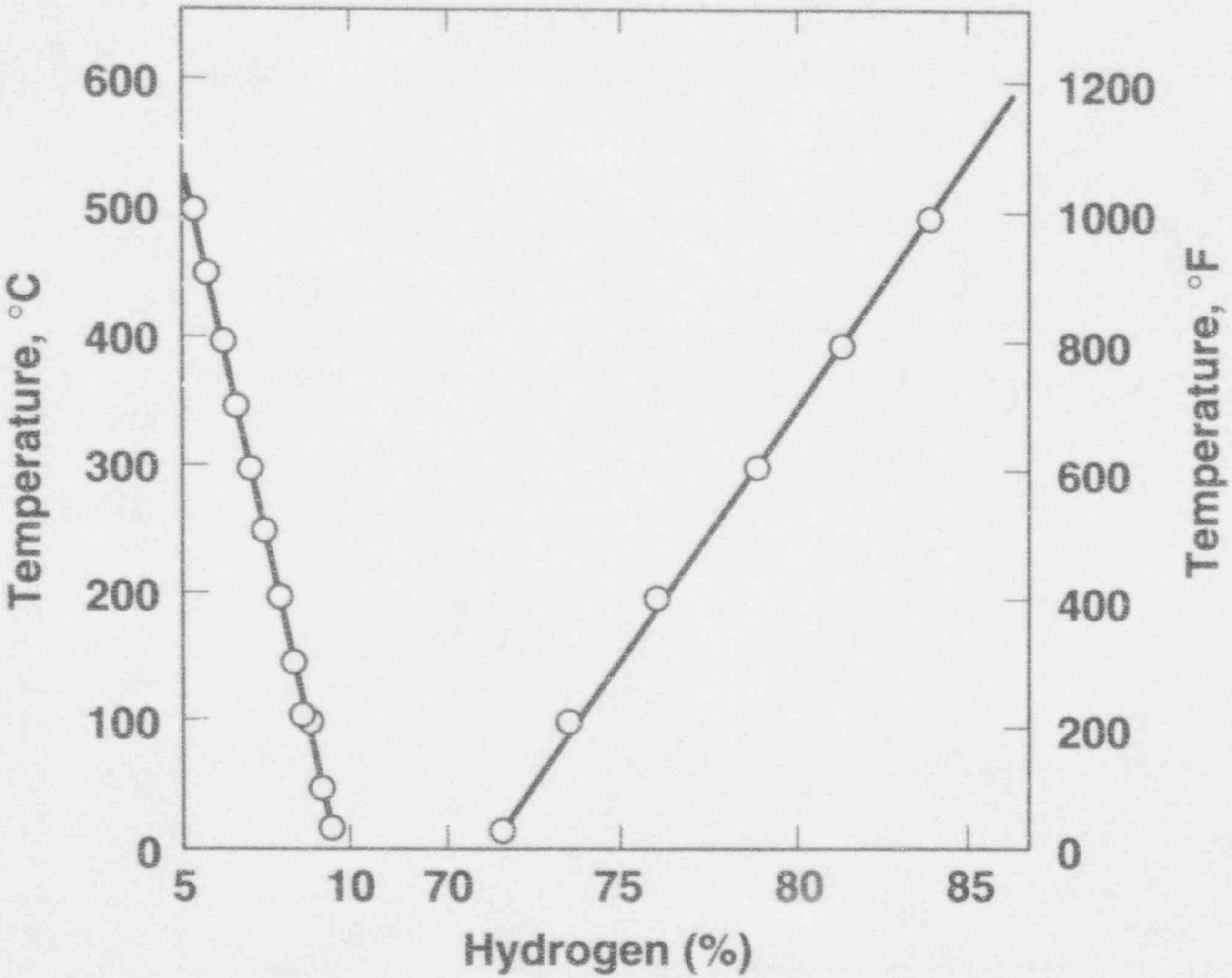


Figure 4.6-3 Effect of initial temperature on downward propagating flammability limits in hydrogen : air mixtures

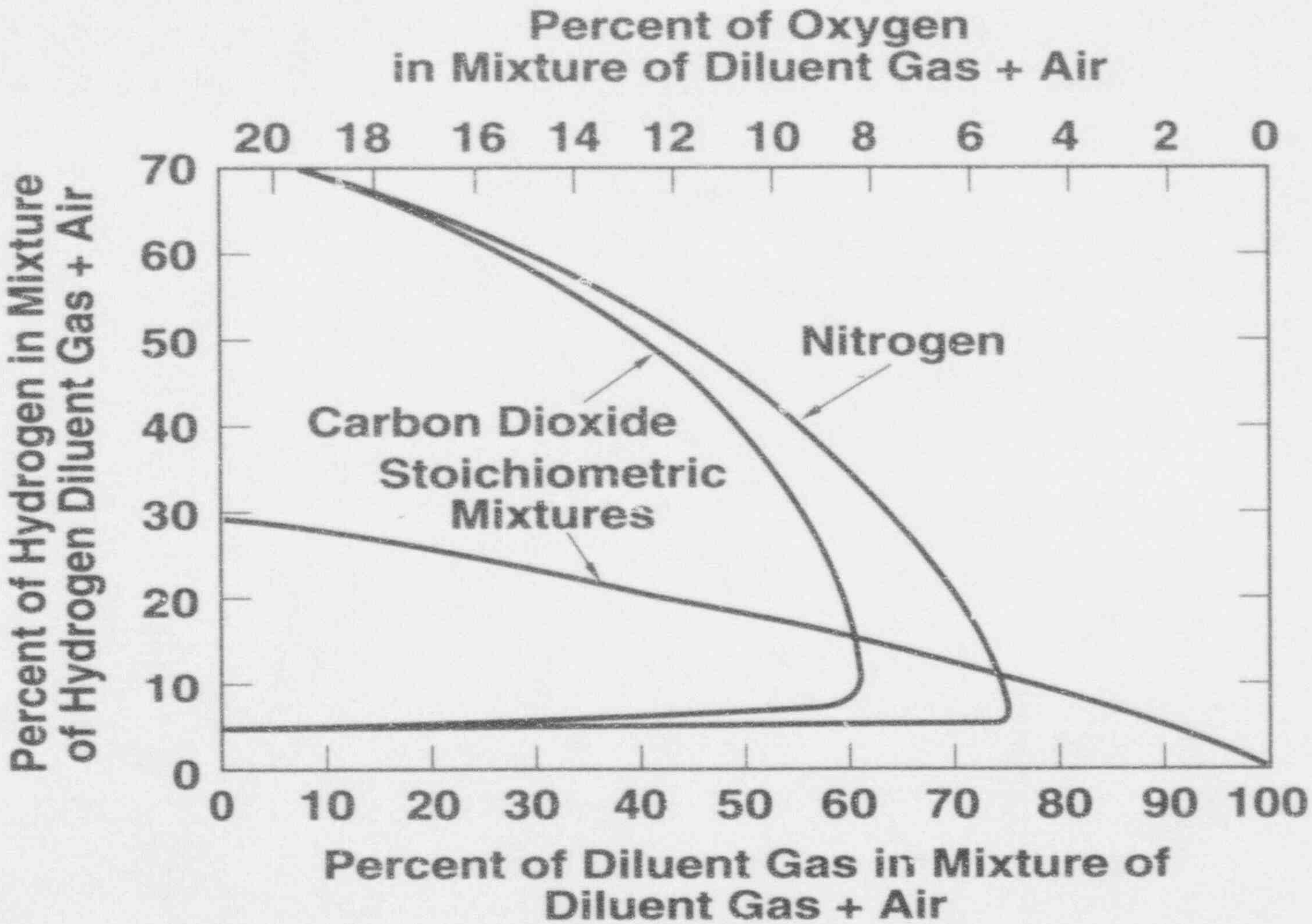
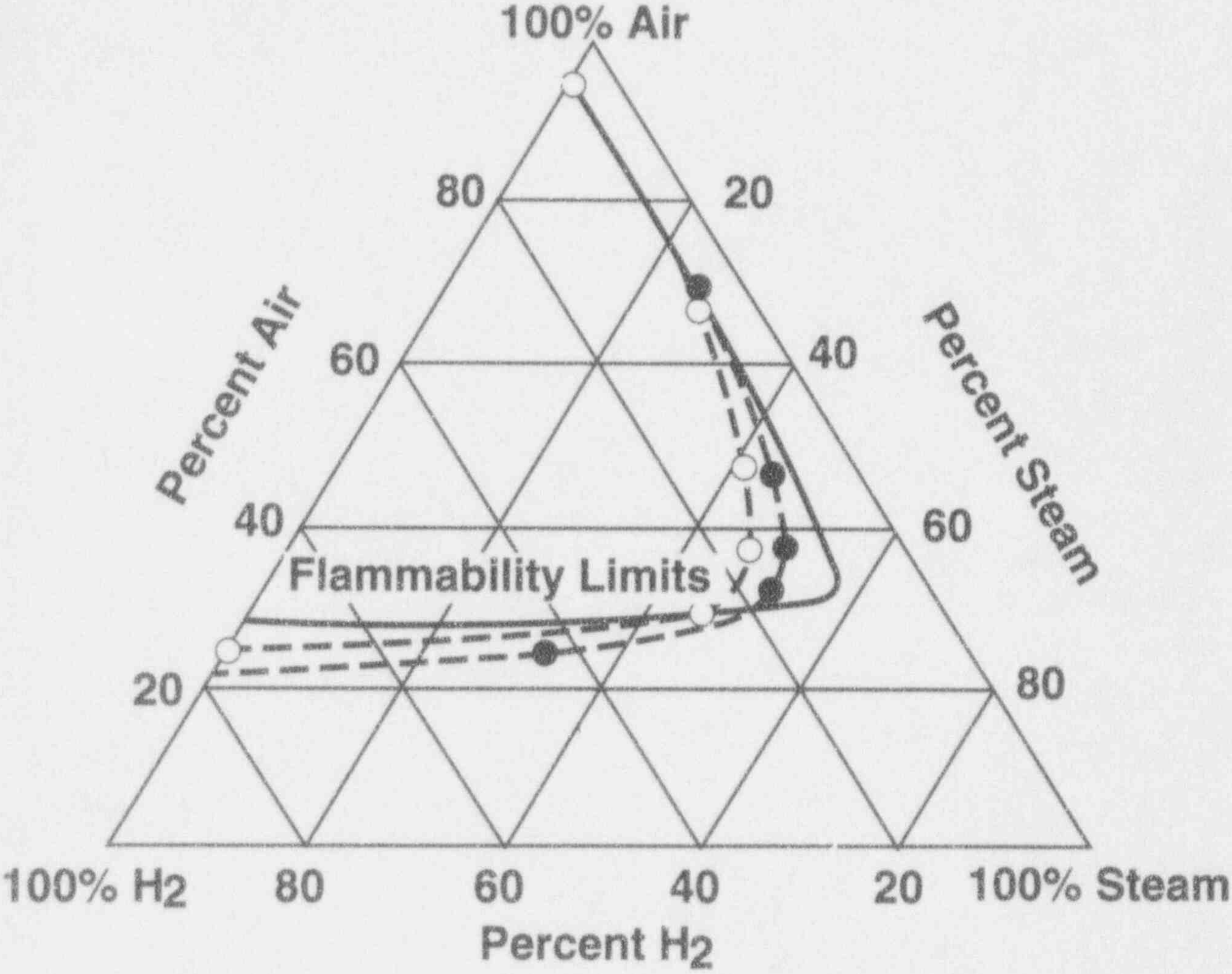


Figure 4.6-4 Flammability limits of hydrogen in air diluted with CO_2 and N_2



Flammability Limits

——— 68°F - 187°F at 0 psig (20°C - 86°C at 101kPa)

○- - - 300°F - 0 psig (149°C - 101 kPa)

●- - - 300°F - 100 psia (149°C - 892 kPa)

Figure 4.6-5 Flammability and detonation limits of hydrogen : air : steam mixtures

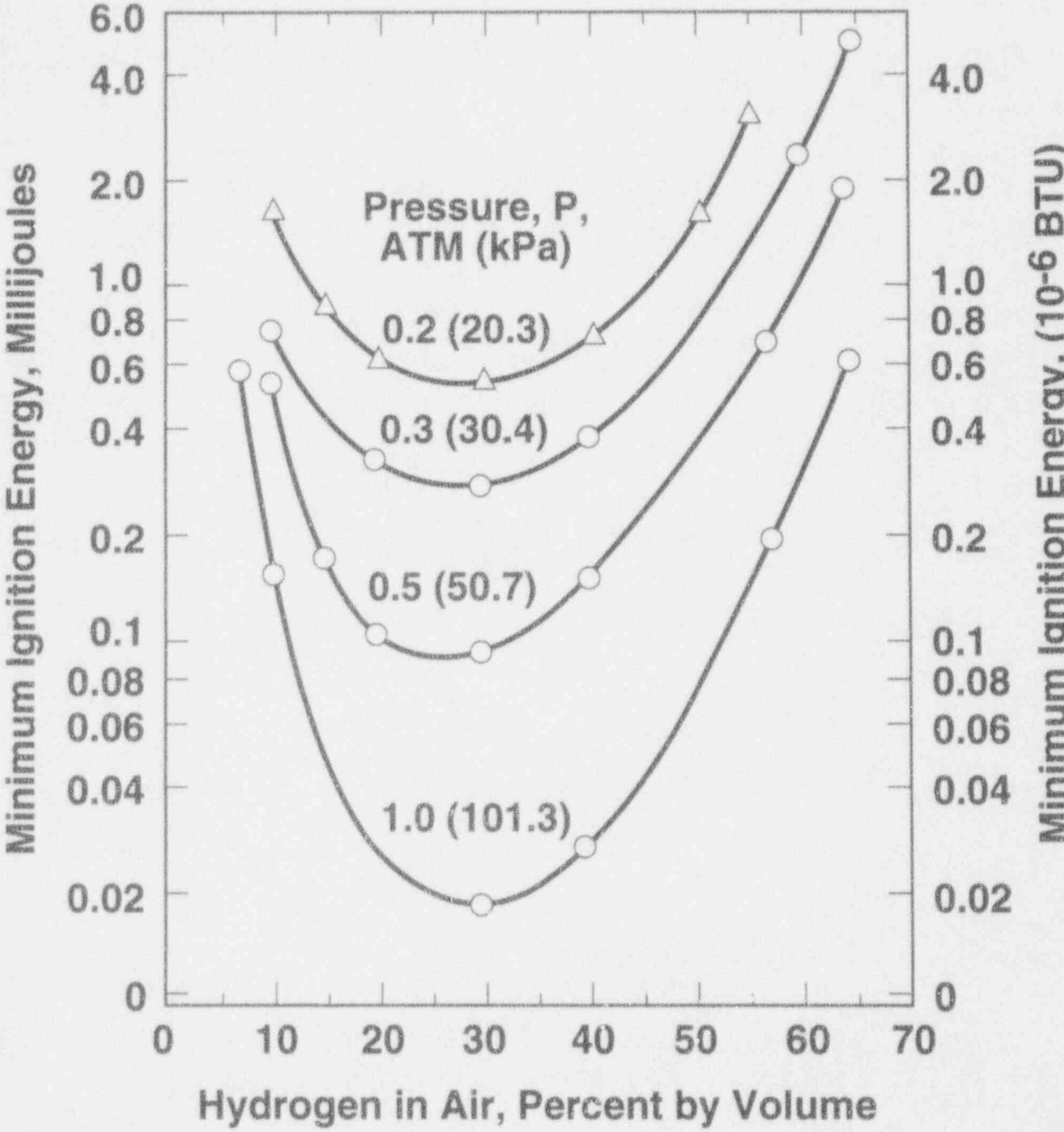


Figure 4.6-6 Spark ignition energies for dry hydrogen : air mixtures

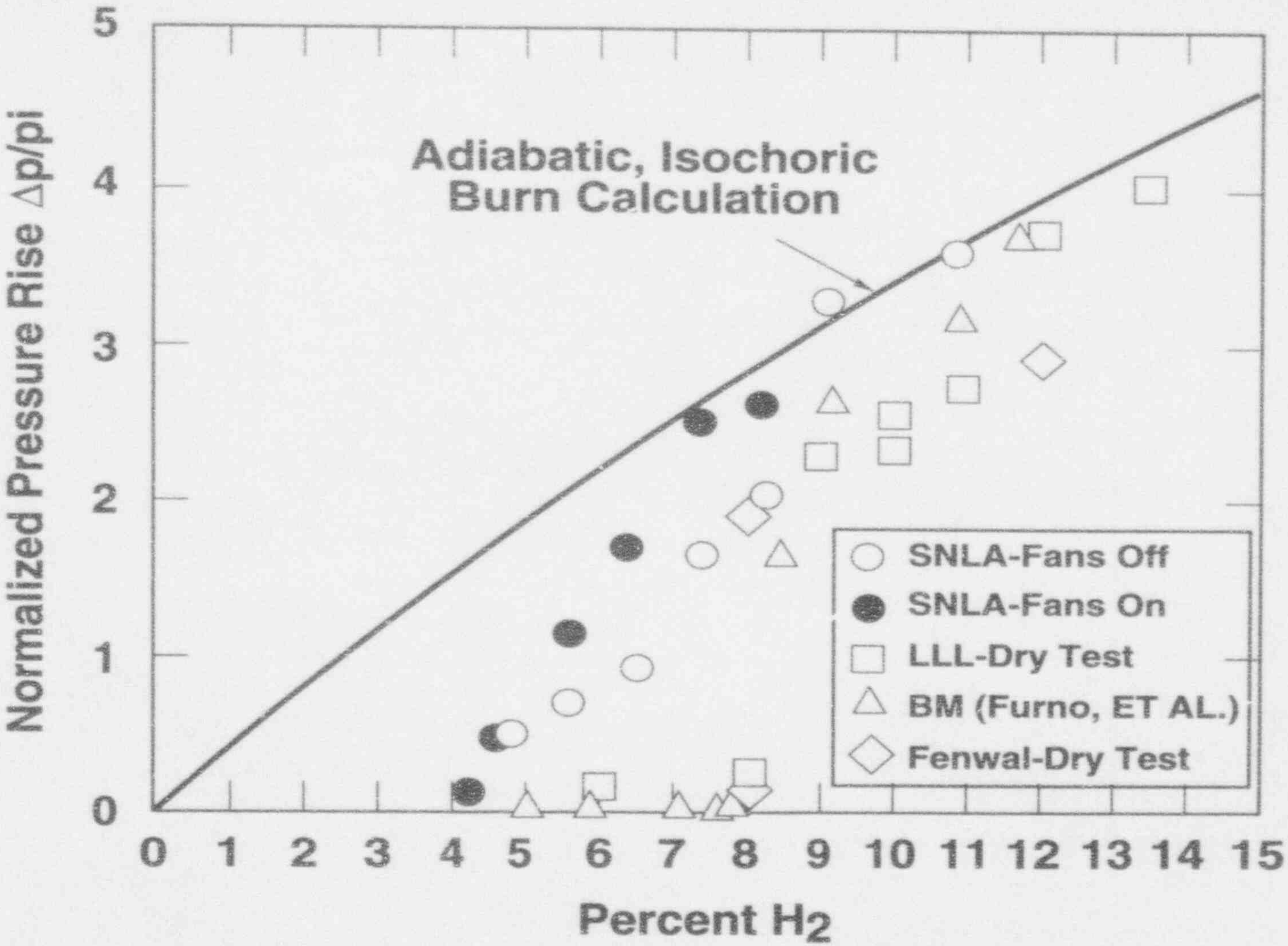


Figure 4.6-7 Normalized pressure rise versus hydrogen concentration

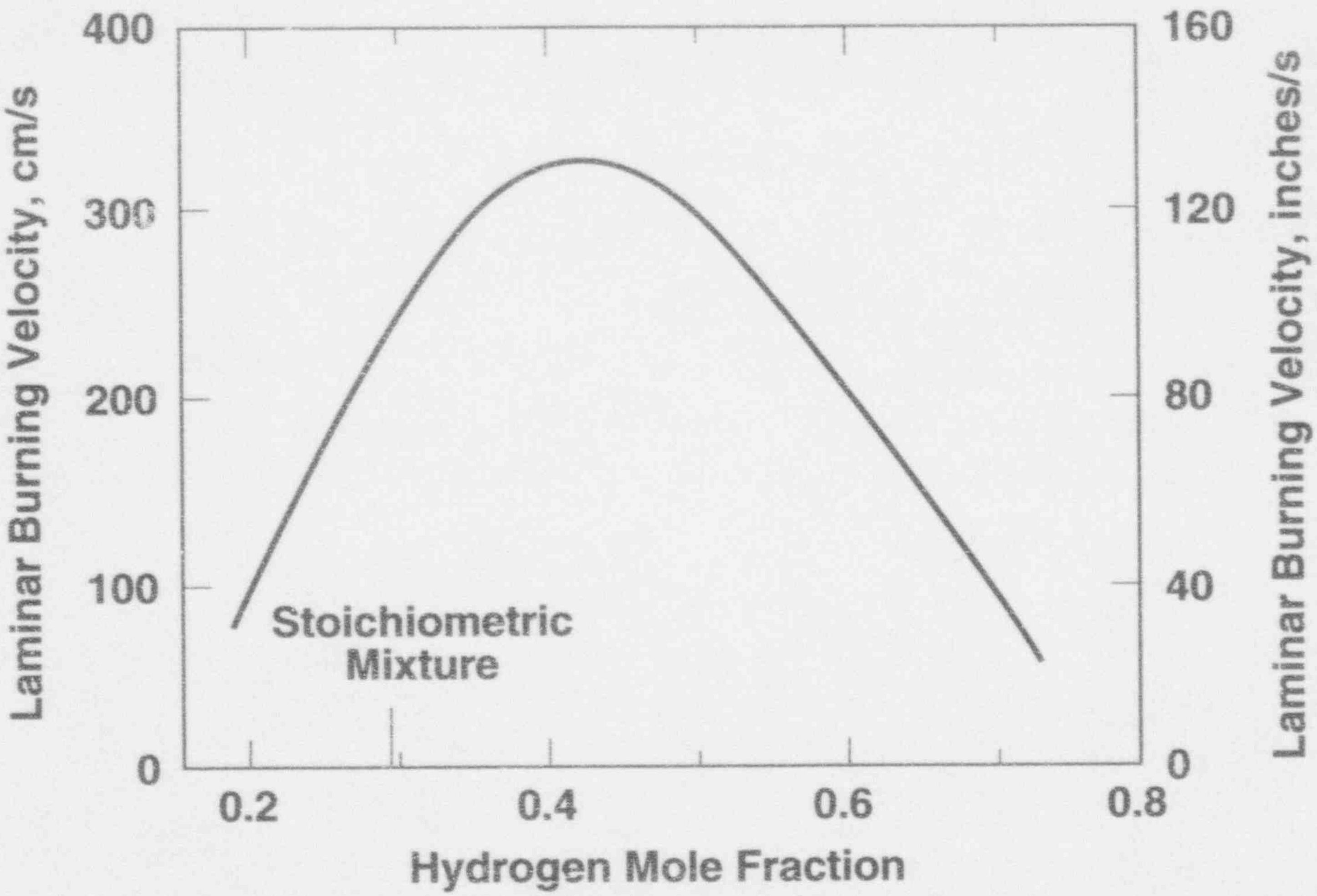


Figure 4.6-8 Laminar burning velocity of hydrogen : air mixture

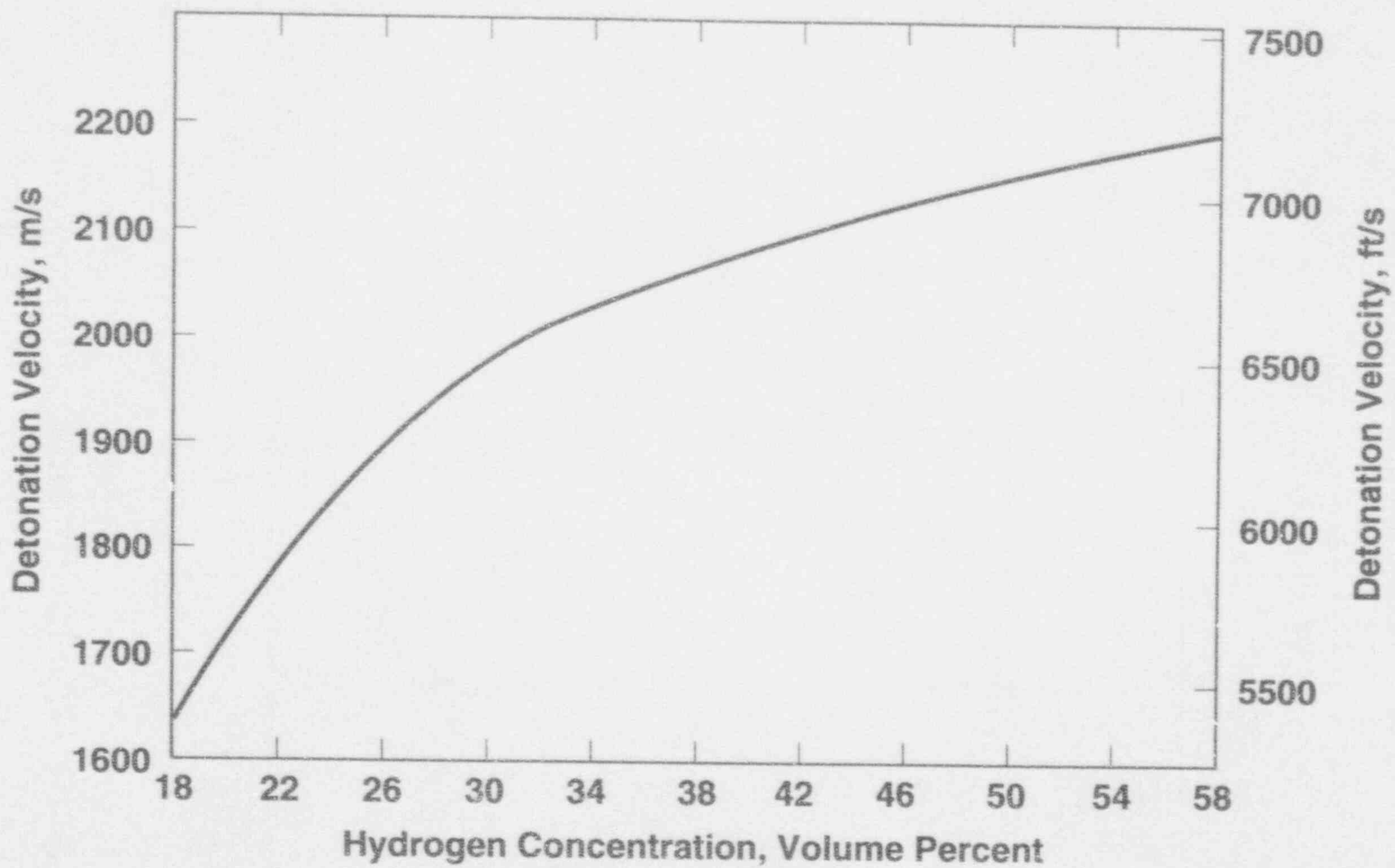


Figure 4.6-9 Theoretical detonation velocities for hydrogen : air mixture

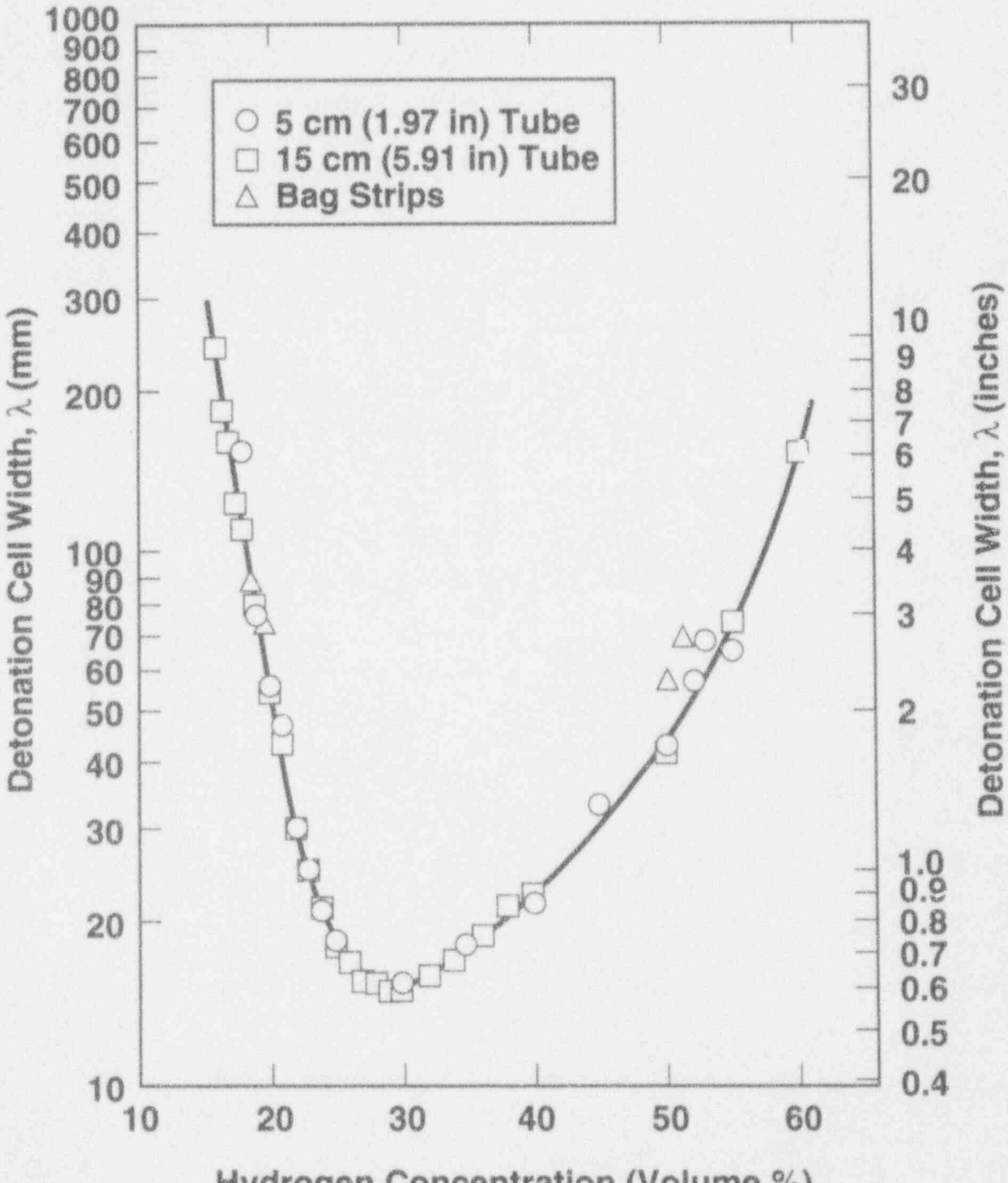


Figure 4.6-10 Measurements of detonation cell size for hydrogen : air mixtures at atmospheric pressure

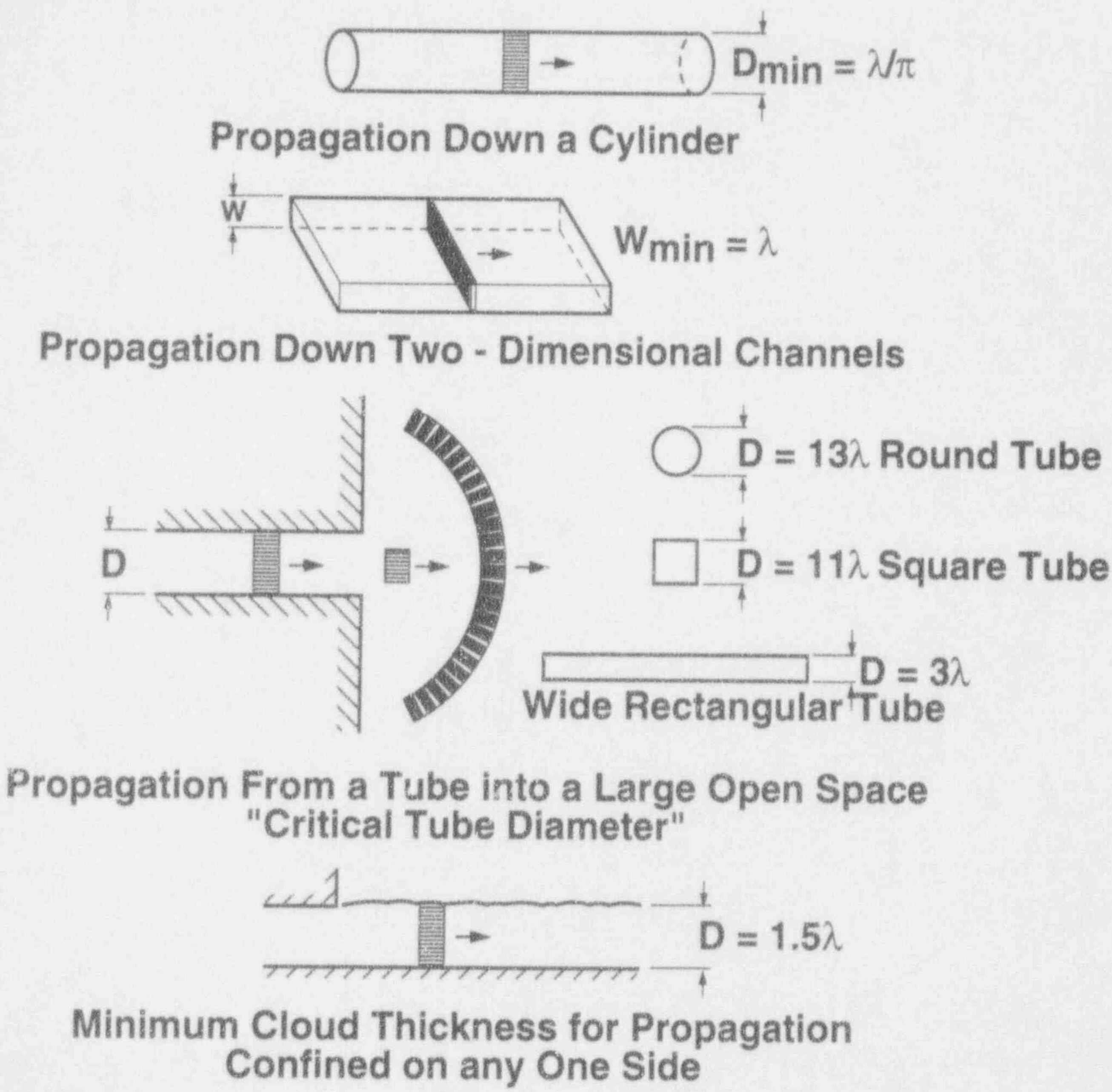


Figure 4.6-11 Dimensions required for detonation propagation in various geometries size

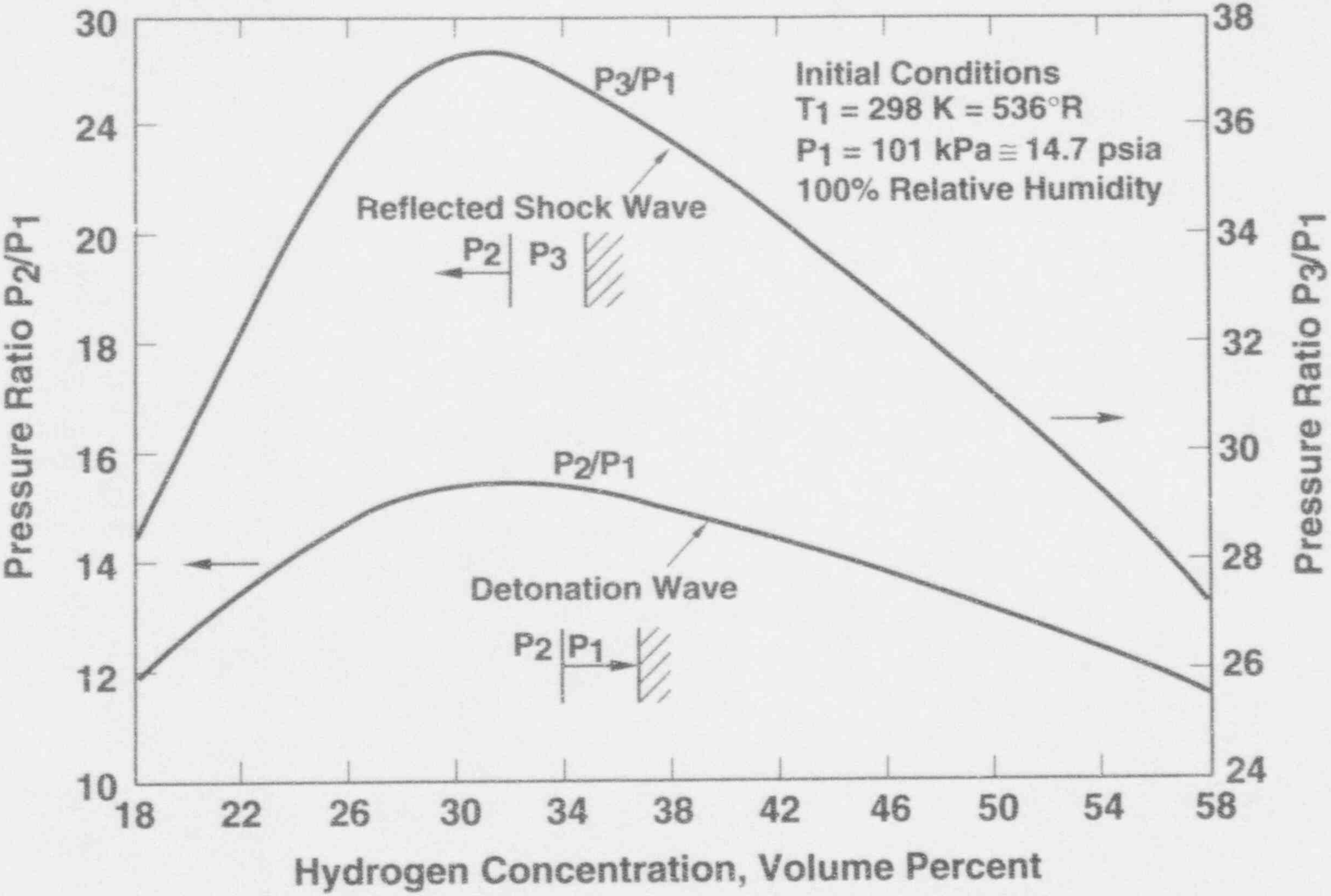


Figure 4.6-12 Theoretical detonation pressure and normally reflected pressure

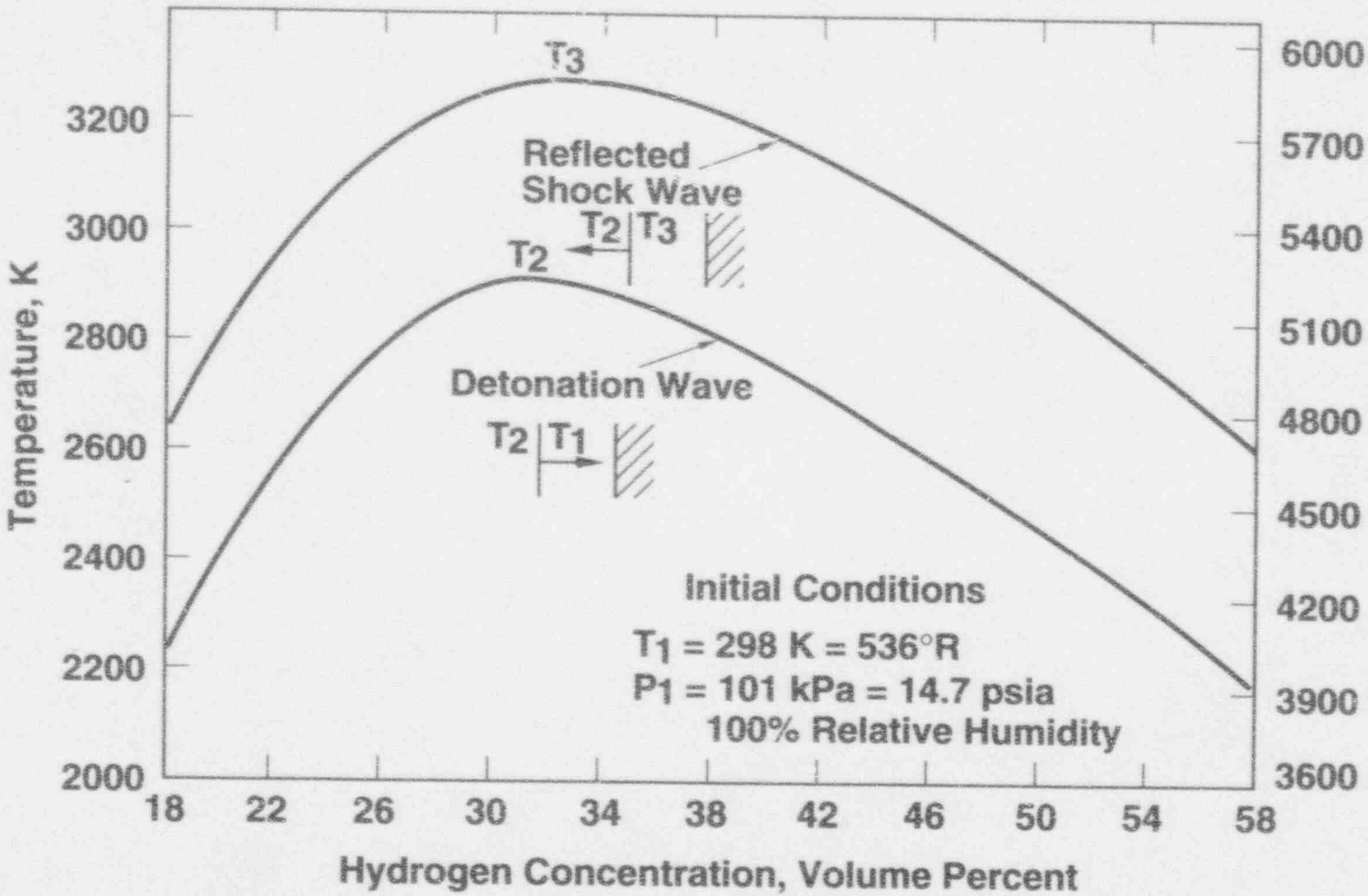


Figure 4.6-13 Theoretical detonation temperature and normally reflected detonation temperature

FLAME SCALING

Structure Determined by Source Froude Number. F

$$F = \rho U^2 / g \Delta\rho D$$

- $F \gg 1$ Jet-Like Flames
- $F \ll 1$ Plume-Like Flames

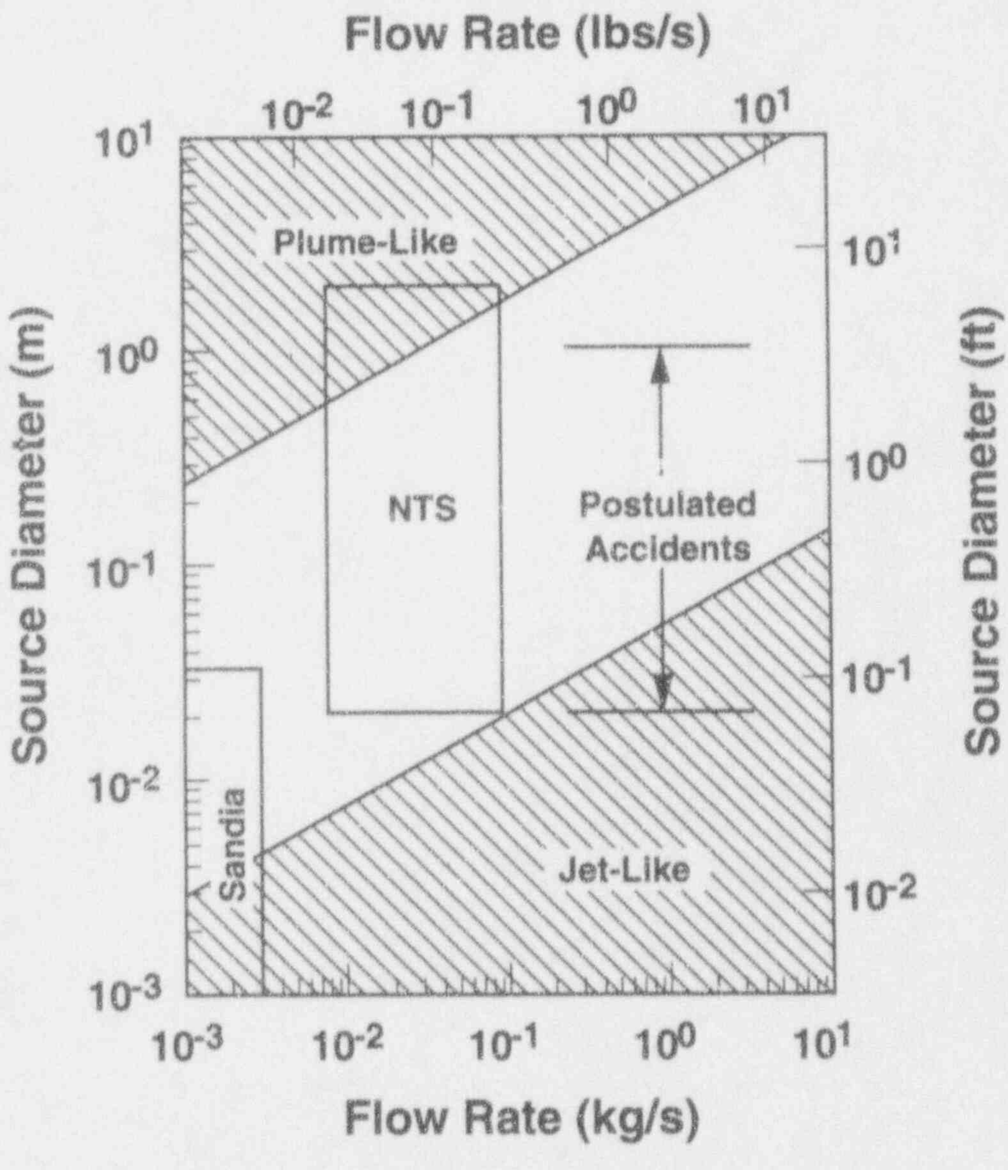


Figure 4.6-14 Flame structures for a range of geometries and flow rates

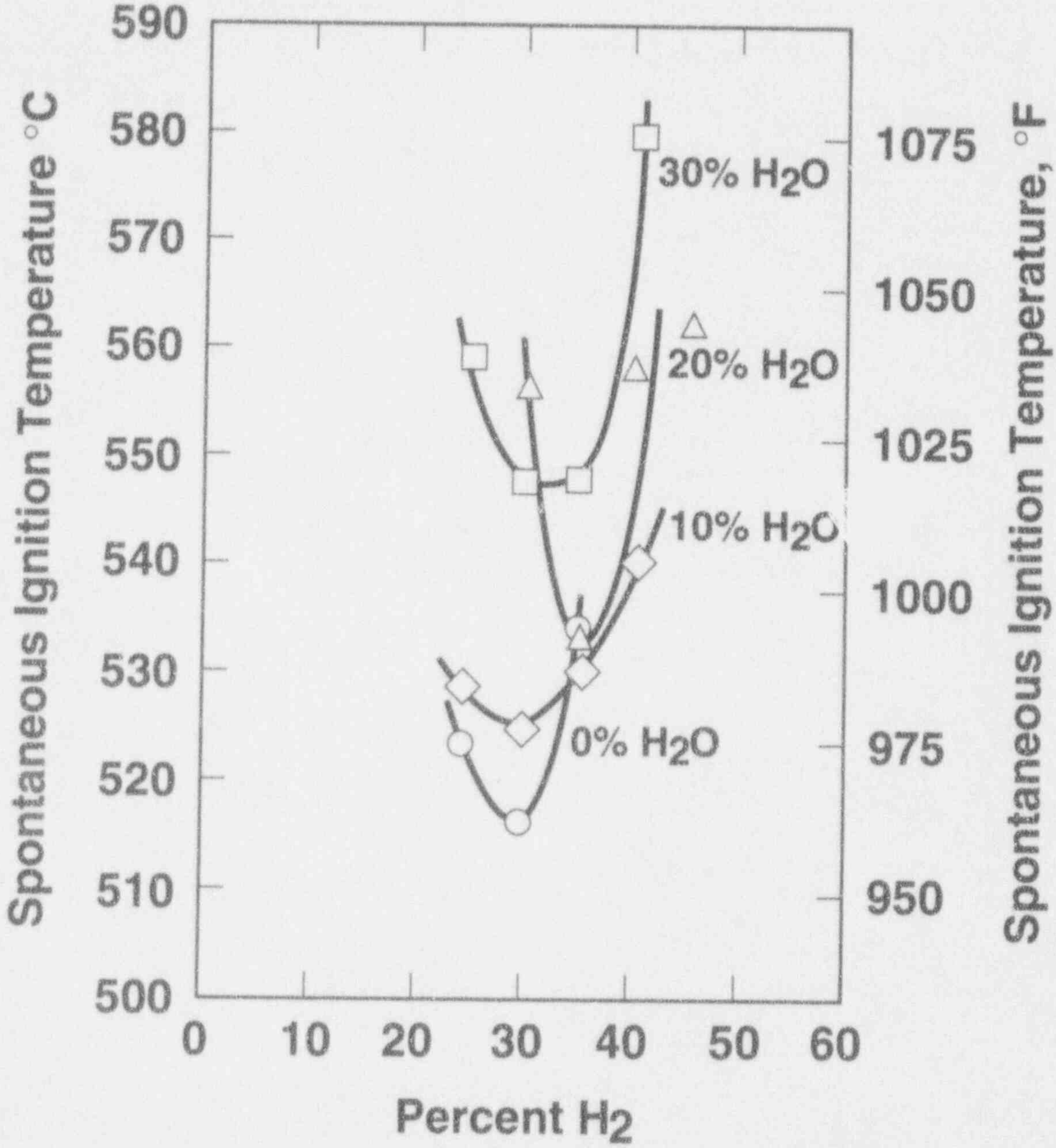


Figure 4.6-15 Minimum spontaneous ignition temperatures

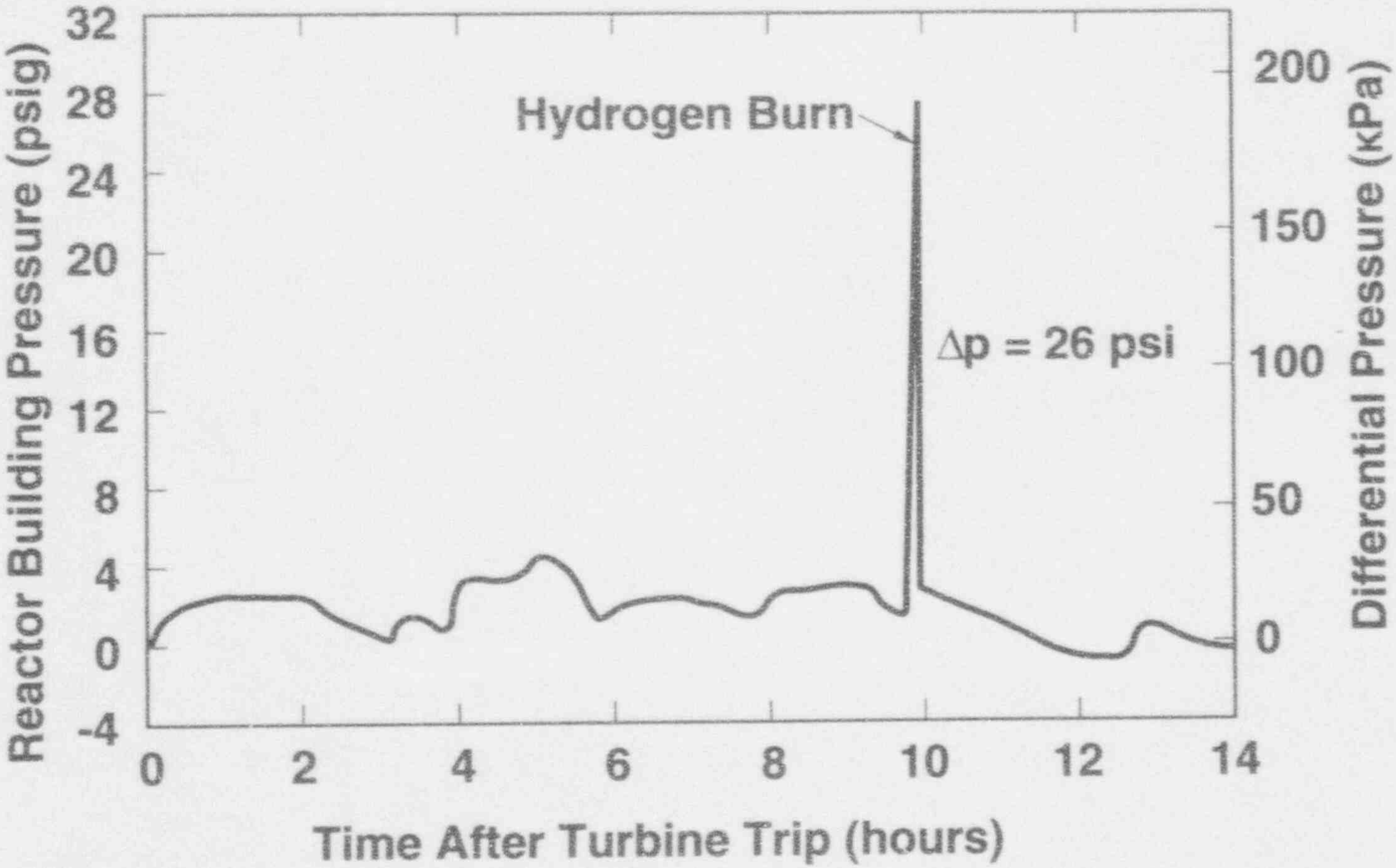


Figure 4.6-16 TMI-2 containment pressure versus time

References for Section 4.6

1. A. L. Camp, et al., *Light Water Reactor Hydrogen Manual*, NUREG/CR-2726, SAND82-1137, Sandia National Laboratories, August 1983.

2. E. P. Coward and G. W. Jones, Limits of Flammability of Gases and Vapors, Bulletin 503, Bureau of Mines, U. S. Department of Interior, 1952.

3. B. Bregeon, et al., "Near-Limit Downward Propagation of Hydrogen and Methane Flames in Oxygen-Nitrogen Mixtures," Comb. & Flame, 33:33-45, 1978.

4. Z. M. Shapiro and T. R. Moffette, *Hydrogen Flammability Data and Application to PWR Loss-of-Coolant Accident*, WAPD-SC-545, Bettis Plant, September 1957.

5. I. L. Drell and F. E. Belles, Survey of Hydrogen Combustion Properties, NACA R 1383, National Advisory Committee for Aeronautics, 1958.

6. A. L. Furno, E. B. Cook, J. M. Kuchta and D. S. Burgess, "Some Observations on Near-Limit Flames," 13 Sym. on Comb., Pittsburgh, Comb. Inst., 593-599, 1971.

7. B. C. Slifer and T. G. Peterson, Hydrogen Flammability and Burning Characteristic in BWR Containments, NEDO-10812, 73NED49, General Electric, April 1973.

8. M. P. Paulson and J. O. Bradfute, "Pressure and Temperature Transients Resulting from Postulated Hydrogen Fires in Mark III Containments," EI 75-4, Energy Inc., 1981.

9. M. Berman, Light Water Reactor Safety Research Program Quarterly Report, January-March, 1981, NUREG/CR-2163/1 of 4, SAND81-1216/1 of 4, Sandia National Laboratories, Albuquerque, NM, July 1981.

10. W. E. Lowry, et al., Final Results of the Hydrogen Igniter Experimental Program, NUREG/CR-2486, UCRL-53036, Lawrence Livermore National Laboratory, February 1982.

11. M. Berman, Light Water Reactor Safety Research Program Semiannual Report, April-September 1981, NUREG/CR-2481, SAND82-0006, Sandia National Laboratories, Albuquerque, NM, February 1982.

12. Yu. M. Annushkin and E. D. Sverdlov, "Stability of Submerged Diffusion Flames in Subsonic and Underexpanded Supersonic Gas-Fuel Streams," Translation, Combustion, Explosions, and Shock Waves, 14, 5, 1978.

13. C. M. Guirao, R. Knystautas, J. H. Lee, W. Benedick, and M. Berman, "Hydrogen-Air Detonations," presented at the 1982 Combustion (International) Symposium, Haifa, Israel, 1982.

14. D. W. Stamps and M. Berman, *A Critical Review of High-Temperature Hydrogen Combustion in Reactor Safety Applications*, SAND88-0680C, International Conference on Thermal Reactor Safety, Avignon, France, October 1988.

15. R. K. Byers, CSQ Calculations of H_2 Detonations in the Zion and Sequoyah Nuclear Plants, NUREG/CR-2385, SAND81-2216, Sandia National Laboratories, Albuquerque, NM, July 1982.

16. M. A. Delichatsios, M. B. Genadry, M. N. Fardis, Calculations of Hydrogen Detonations in Nuclear Containments by the Random Choice Method, M.I.T., R81-30, December 1981.

17. Z. M. Shapiro and T. R. Moffette, *Hydrogen Flammability Data and Application to PWR Loss-of-Coolant Accident*, Sep. 1957.

18. J. E. Shepherd, *Hydrogen-Steam Jet-Flame Facility and Experiments*, NUREG/CR-3638, SAND84-0060, Sandia National Laboratories, February 1985.

19. M. Berman, *Light Water Reactor Safety Research Program Semiannual Report, April-September 1981*, February 1982.

20. *Technical Aspects of Hydrogen Control and Combustion in Severe Light-Water Reactor Accidents*, National Academy Press, Washington, D.C., 1987.

21. *Title 10, Code of Federal Regulations, Part 50.44*, U.S. Government Printing Office, January 1, 1991.

22. M. P. Sherman and M. Berman, *The Possibility of Local Detonations During Degraded-Core Accidents in the Bellefonte Nuclear Power Plant*, NUREG/CR-4803, SAND86-1180, Sandia National Laboratories, January 1987.

APPENDIX 4A Example Calculation of Hydrogen Combustion Pressures and Temperatures

This appendix provides an approximate method for estimating hydrogen burn pressures and temperatures. The example is taken from Reference 1. With the aid of Figures 4A-1 and 4A-2, or 4A-3 and 4A-4, the pressure and temperature that would be caused by an adiabatic, constant-volume, complete combustion of a homogeneous hydrogen:air:steam mixture can be estimated. Figures 4A-1 and 4A-2 can be used for cases in which the steam mole fraction before the burn is small. This might be the case in the wetwell (or outer containment) of a Mark III BWR or the upper compartment of an ice condenser containment. Figures 4A-3 and 4A-4 are to be used when the conditions before the combustion are steam saturated. For initial temperatures not far above normal room temperature, the steam mole fraction is small even in a saturated atmosphere. In that case either set of figures could be used.

We will describe the procedure to be used in the computations in the next paragraph. For all the calculations absolute pressures and temperatures should be used.

Absolute Pressure = Gauge Pressure + Atmosphere Pressure (4A-1)

Typically, for normal atmospheric pressure,

Pressure (psia) = Pressure (psig) + 14.7 (4A-2)

or

Pressure (MPaa) = Pressure (Mpag) + 0.101 (4A-3)

For temperature,

Temperature (Rankine) = Temperature (Fahrenheit) + 460 (4A-4)

or

Temperature (Kelvin) = Temperature (Celsius) + 273 (4A-5)

The subscripts A, S and H_2 refer to air, steam, and hydrogen. The analysis considers three times: t_o, the time at the start of the accident; t_1, the time just before the combustion; and t_2, the time just after the combustion. The object of the calculation is to determine $P(t_2)$ and $T(t_2)$, the pressure and temperature just after combustion. We will assume that conditions at time t_o are known, and that sufficient information about conditions at time t_1 is known so that the unknown gas conditions at that time can be computed.

Consider the example when the conditions at the start of the accident are:

$P(t_o)$ = 14.7 psia (0.101 MPa)

$T(t_o)$ = 560°R (311 K)

Relative Humidity = 50%

Just before the combustion the temperature is 590°R (328 K), the air is saturated and a hydrogen detector measures 10 volume percent (mole fraction) hydrogen (see Table 4A-1).

For all three time periods, the total pressure is the sum of the partial pressures of air, hydrogen and steam,

$$P = P_A + P_S + P_{H2} \quad (4A\text{-}6)$$

Initially, there is no hydrogen, $P_{H_2}(t_o) = 0$. The saturation steam pressures are determined from "Steam Tables" found in thermodynamics textbooks or engineering handbooks. We have

$P_{SAT}(T_o) = P_{SAT}$(560°R (311 K)) = 0.95 psia (0.0065 MPa) (4A-7)

$P_S(t_o)$ = relative humidity * $P_{SAT}(T_o)$ = 0.48 psia (0.0033 MPa) (4A-8)

Therefore, the initial air partial pressure is

$$P_A(t_o) = 14.7 - 0.5 = 14.2 \text{ psia } (0.098 \text{ MPa}) \tag{4A-9}$$

From steam tables we obtain, at t_1,

$$P_S(t_1) = P_{SAT}(T_1) = 2.2 \text{ psia } (0.015 \text{ MPa}) \tag{4A-10}$$

The air partial pressure at t_1 is

$$P_A(t_1) = (T_1/T_O)P_A(t_O) = (590/560) * 14.2 = 15.0 \text{ psia } (0.103 \text{ MPa}) \tag{4A-11}$$

The hydrogen mole fraction is

$$X_{H_2} = P_{H_2}/P \tag{4A-12}$$

which leads to

$$P_{H_2} = (P_A + P_S) * X_{H_2}/(1.0 - X_{H_2}) \tag{4A-13}$$

Hence

$$P_{H_2}(t_1) = 17.2 * 0.1/0.9 = 1.9 \text{ psia} (0.013 \text{ MPa}) \tag{4A-14}$$

$$P_1 = 17.2 + 1.9 = 19.1 \text{ psia } (0.131 \text{ MPa}) \tag{4A-15}$$

We now estimate the postburn conditions using Figures 4A-1 and 4A-2. Figure 4A-1 gives the final/initial pressure ratio for burns with a given set of initial conditions. However, the pressure ratio is insensitive to the initial pressure, and insensitive to small changes in initial temperature. The influence of initial steam mole fraction can be greater. The figures were computed using a humidity corresponding to a steam mole fraction of 3%. At 590°R (328 K) the steam mole fraction for 100% relative humidity will be higher, but will still be small enough to use Figures 4A-1 and 4A-2. From Figure 4A-1, we determine that $P(t_2)/P(t_1) = 4.2$, hence $P(t_2) = 4.2 * 19.1 = 80.2$ psia (0.55 MPa). An approximate final temperature can be estimated from Figure 4A-2 by adding to the temperature found from the figure the difference between $T(t_1)$ and 536°R (298 K).

$$T(t_2) \approx 1230 + 30 = 1260 \text{ K } (2270°\text{R}) \tag{4A-16}$$

When applicable, the use of Figures 4A-3 and 4A-4 is simpler than using Figures 4A-1 and 4A-2. These figures are applicable when the conditions at the start of the accident are near $P(t_o) = 1$ atm (0.101 MPa), $T(t_o) = 540$°R (300 K), and the conditions just before the combustion are steam saturated. It should be noted that the curves for constant $T(t_1)$ in the two figures correspond to varying pressure, $P(t_1)$, and varying steam mole fraction. At all points on the curves, the composition has been adjusted to saturation conditions. Much of the work in describing the conditions at time t_1 is not needed here because that information has been incorporated into the figures. For a temperature of 590°R (328 K), we determine that $P(t_2) = 4.9$ atm = 72.0 psia (0.50MPa), and $T(t_2) = 2340$°R (1300 K).

The results of thermochemical calculations on a computer give values $P(t_2) = 71.4$ psia (0.51 MPa), $T(t_2) = 2401$°R (1334 K). The difference between the results (summarized in Table 4A-1) gives an indication of the accuracy to be expected from the simple graphical methods.

If the pressure and temperature before the combustion are accurately measured and the hydrogen mole fraction measurement is absent or less accurate, the hydrogen mole fraction can be estimated (assuming saturation) from the relations,

$$P_{H_2} = P - P_A - P_S \tag{4A-17}$$

$$X_{H_2} = P_{H_2}/P \tag{4A-18}$$

Some hydrogen detectors may remove the water vapor content of the hydrogen:air:steam mixture. In this case the measured hydrogen mole fraction (of the dry hydrogen:air mixture) will be larger than the value in the original mixture. The correction required to recover the original value is

$$X_{H_2} = (1 - X_S)X_{H_2}' \qquad (4A\text{-}19)$$

where X_H' is the hydrogen mole fraction in the dry hydrogen:air mixture and X_S is the steam mole fraction in the original hydrogen:air:steam mixture,

$$X_S = P_S/P \qquad (4A\text{-}20)$$

TABLE 4A-1

COMPUTATION OF ADIABATIC, CONSTANT-VOLUME
PRESSURE AND TEMPERATURE

	Time Before Accident t_o	Time Before Combustion t_1	Time After Combustion t_2 Using Figs. 4A-1 & 4A-2	Time After Combustion t_2 Using Figs. 4A-3 & 4A-4
Pressure - psia (MPa)	14.7(0.101)*	19.1(0.131)	80.2(0.55)	72.0(0.50)
Temperature - °R (K)	560(311)*	590(328)*	2270(1260)	2340(1300)
Hydrogen Mole Fraction	0.0*	0.1*		
Air Partial Pressure - psia (MPa)	14.2(0.098)	15.0(0.103)		
Steam Partial Pressure - psia (MPa)	0.48(0.0033)	2.2(0.015)		
Hydrogen Partial Pressure - psia (MPa)	0.0(0.0)	1.90(0.013)		

*Data directly from measured initial conditions

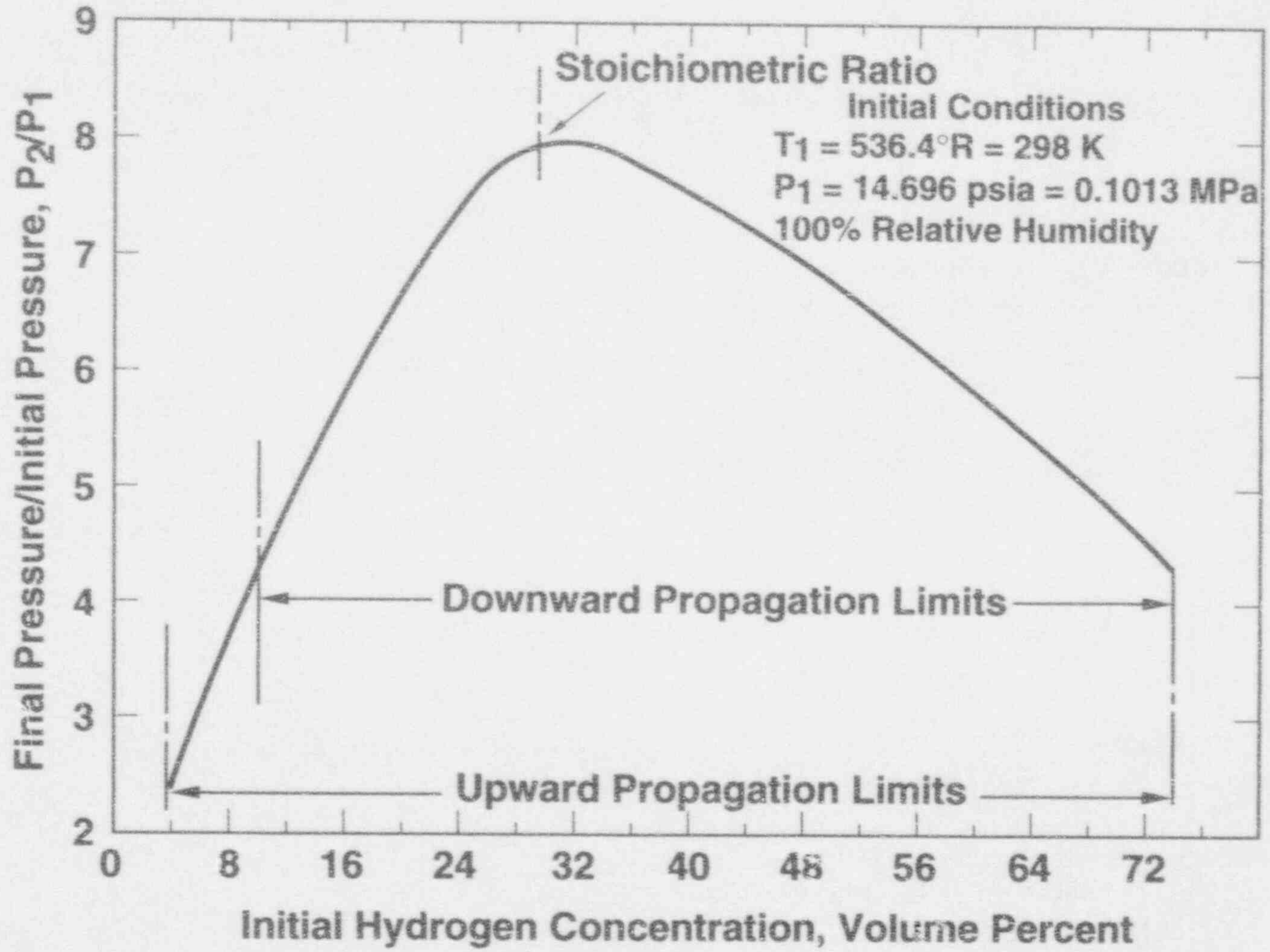


Figure 4A-1 Theoretical adiabatic, constant-volume combustion pressure for hydrogen : air mixtures

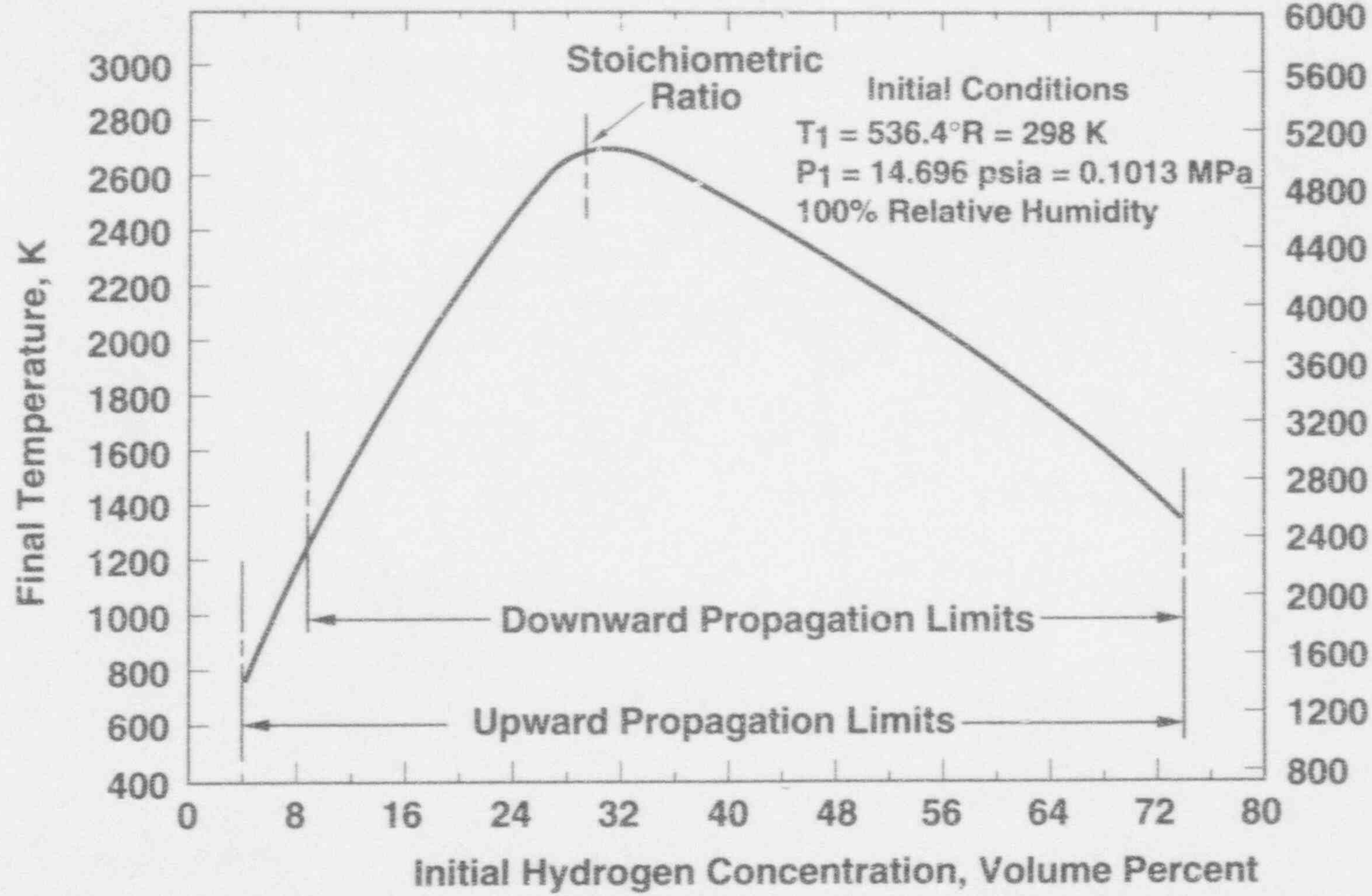


Figure 4A-2 Theoretical adiabatic, constant-volume combustion temperature for hydrogen : air mixtures

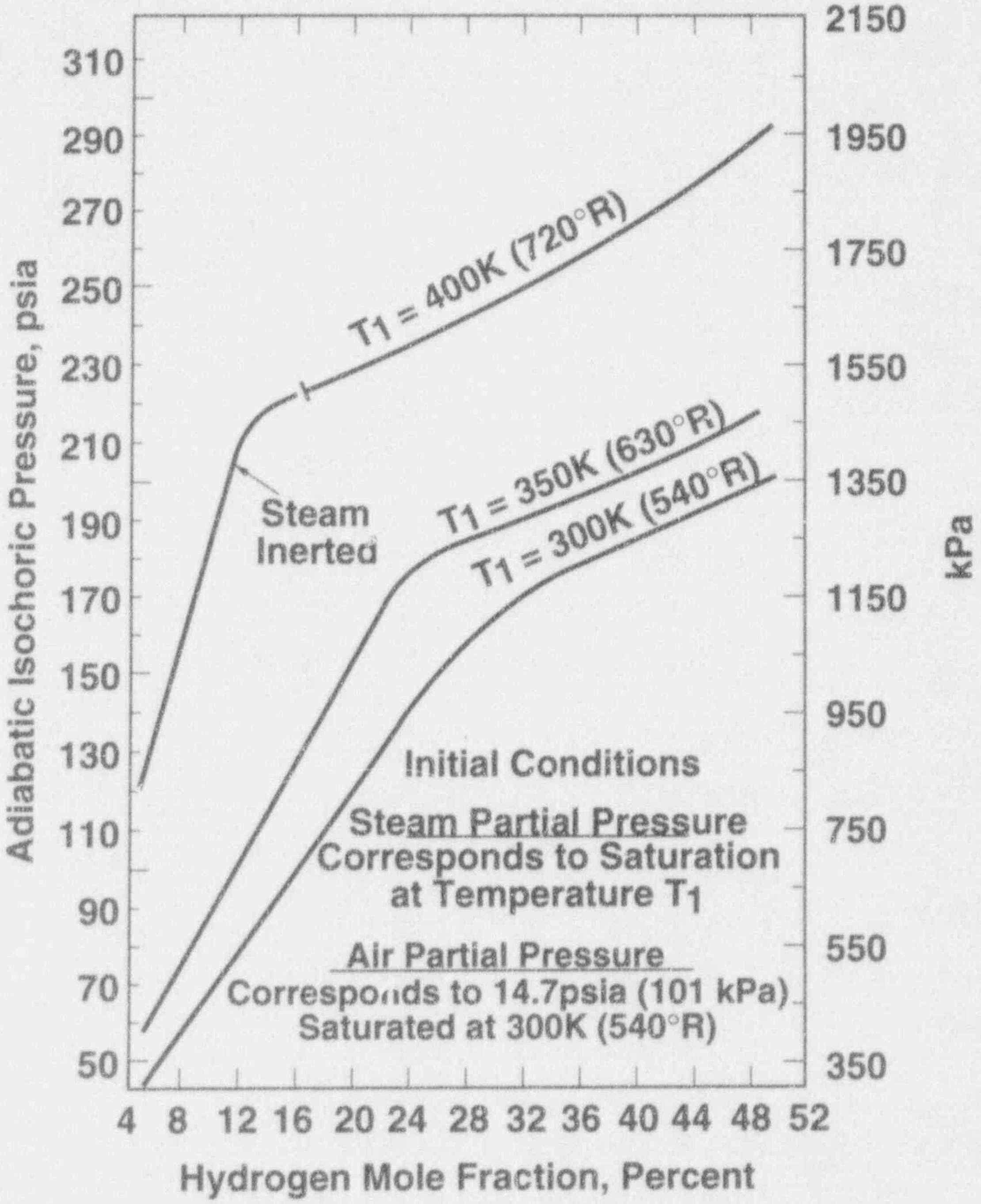


Figure 4A-3 Adiabatic, constant-volume combustion pressure for various containment initial conditions

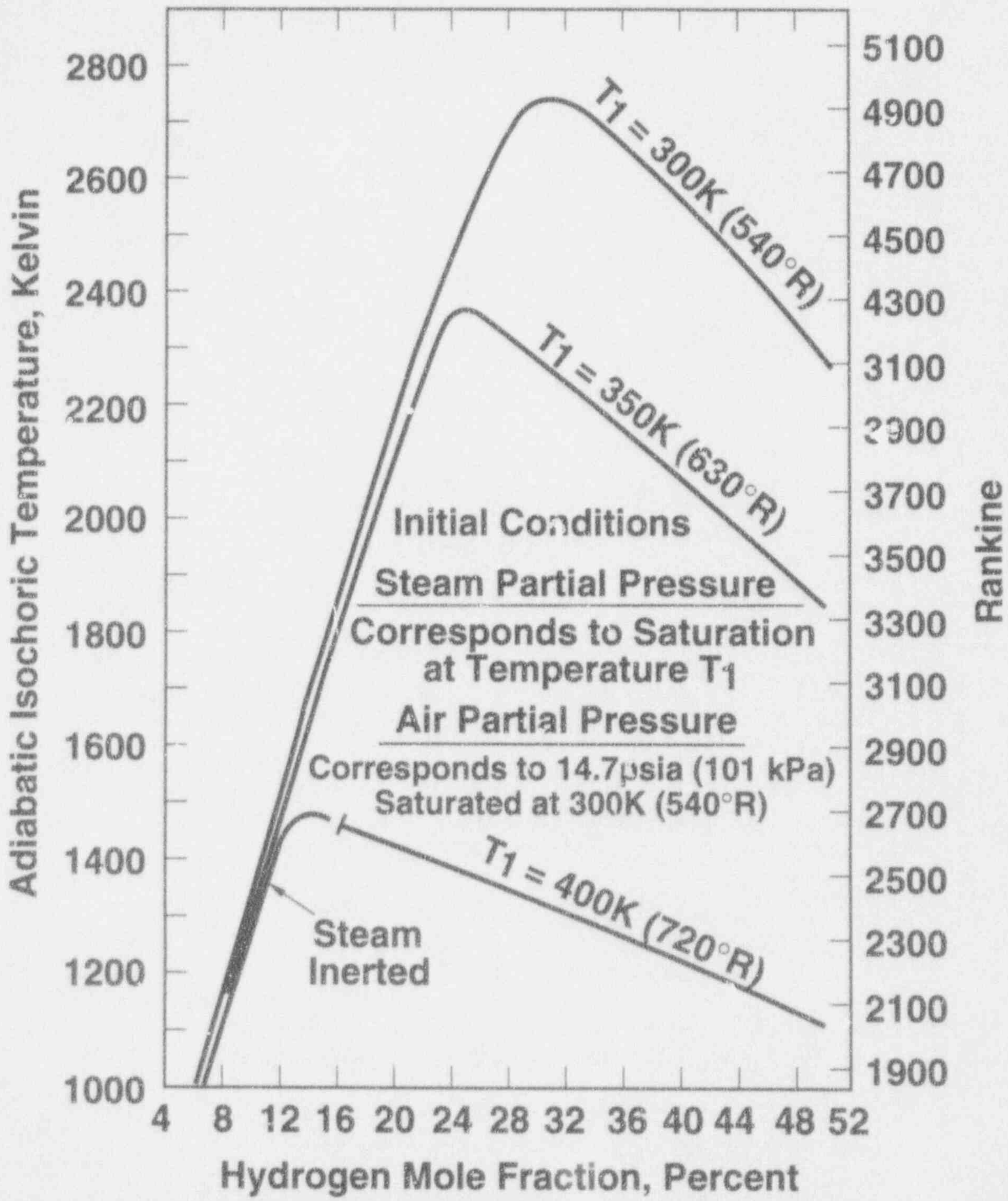


Figure 4A-4 Adiabatic, constant-volume combustion temperature for various containment initial conditions

References for Appendix 4A

1. A. L. Camp, et al., *Light Water Reactor Hydrogen Manual*, NUREG/CR-2726, SAND82-1137, Sandia National Laboratories, August 1983.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

LIST OF TABLES

LIST OF TABLES (Continued)

LIST OF ILLUSTRATIONS

LIST OF ILLUSTRATIONS (Continued)

5.1 Source Terms

As indicated in Modules 3 and 4, if the energy contained in the core of a nuclear power plant is not controlled, considerable damage can be done to the fuel, cladding, reactor vessel, and even the containment--the plant barriers that normally contain the core radionuclides. Even if the reactor is shut down, the substantial energy generated by the decay of fission products (decay heat) can lead to damage to these barriers. If sufficient quantities of radionuclides are released to the environment as a result of such damage, various off-site health effects may result. This subsection discusses the quantities and characteristics of radionuclide releases to the environment (source terms) and the corresponding levels of plant damage required to produce significant off-site health effects. It also introduces the concept of protective actions, actions that can be taken to reduce the number of off-site health effects that might otherwise result given a severe accident.

5.1.1 Objectives

After completing this module, the student should be able to:

1. explain why radionuclides of krypton, xenon, iodine and cesium would be expected to contribute to any early off-site health effects that might result from a severe accident;
2. describe the dose levels required to produce early health effects,
3. indicate the curies of noble gases and radioiodine that must be released to produce early health effects and to exceed the Environmental Protection Agency protective action guides,
4. describe the location in the plant of radioactive material that could induce early health effects and the plant damage required for its release to the environment,
5. describe the basic radiation protection criteria, the federally mandated protective action guide (PAG) levels and the relationship of these PAG levels to health effects,
6. describe the information upon which early off-site protective action decisions should be based.

5.1.2 Radionuclide Inventories

The conventional unit used to quantify the radioactivity of a material is the curie (Ci). One curie of material undergoes radioactive decay at the rate of 3.7×10^{10} nuclear disintegrations per second, which is the radioactivity of one gram of pure radium. The corresponding Standard International (SI) unit of radioactivity is the becquerel (Bq). One becquerel is one nuclear disintegration per second, so 1 Ci = 3.7×10^{10} Bq.

Table 5.1-1 shows the principal components of the 5 billion or so curies of radioactive materials in the core of a light water reactor 30 min after shutdown according to their relative volatilities.[1,2] Of the groups listed, radionuclides of the noble gases Krypton (Kr) and Xenon (Xe) are the most volatile and, consequently, the most likely to be released from the plant to the environment during an accident. Up to 100% of the noble gases could be released in severe accidents involving containment failure or bypass. Radioactive iodine and cesium, which rank second in volatility, could also be released in substantial quantities during a severe accident. Radioiodine can concentrate in the thyroid and in the food chain (i.e., milk). As a result, small quantities of radioiodine can cause damage to the thyroid gland. Radioactive cesium is a potential source of long-term offsite dose (e.g. from Chernobyl).

Table 5.1-2 shows radionuclide inventories of the volatile noble gases and iodine in various plant systems.[2] Note that the vast majority of this volatile radioactive material is contained in the core. All other reactor systems contain less than one-half of 1% of the xenon, krypton, and iodine activity in the core. Because radioactive cesium is long-lived, the spent fuel pool can contain more than the core; however, the driving force (decay heat) for release is much larger in the core.

5.1.3 Dose Pathways

Radionuclides would be released to the environment as gases (Kr, Xe, I_2) or aerosol particles of water soluble substances such as cesium iodide (CsI), cesium hydroxide (CsOH), and Sr(OH) or slightly soluble oxides of tellurium, ruthenium and lanthanum. Generally, a major release (source term) from a nuclear power plant can be viewed as a cloud (called the plume) of radioactive gases, aerosol particles, and water vapor (mist). As indicated in Figure 5.1-1, the plume could be released continuously over a long time period, or it could be released as a very short puff. It could be released at ground level or higher. As the radioactive plume moves away from the reactor site, radioactive aerosols will settle out on the ground, vegetation, buildings, vehicles, etc. This is called ground contamination.

Although the curie is an appropriate unit for quantifying amounts of radioactive materials (e.g., curies in the core), it is not an appropriate unit for quantifying the potential health effects that may result from the release of radioactive materials to the environment. The number of curies required to induce a specific health effect can vary considerably, depending on the types of radiation emitted by the decaying nuclei and how the radiation enters the body (i.e., the pathway). Radiation absorbed by a human body is called dose. A unit of dose (or more precisely dose equivalent) is the rem. The dose in rems to the whole body or to a particular organ is a measure of potential biological damage induced by exposure of the body or organ to radiation. Hence, the dose in rems is directly relevant to health effects. The corresponding Standard International (SI) unit is the sievert (Sv), and 1 Sv = 100 rems.

As indicated in Figure 5.1-2, a person can receive a radiation dose from a plume in several ways, usually called pathways. First, dose can be received externally from the radiation given off by the passing plume or the ground contamination. Such doses are called cloud shine and ground shine, respectively. The dose due to radioactive particles that settle directly onto the skin or clothing of persons immersed in the cloud is called the skin dose. Dose can also be received by inhaling the radioactive material in the plume; this is called inhalation dose. Some of the inhaled material may concentrate in particular organs such as the lungs or thyroid and thus become a special threat to those organs. Cloud shine, ground shine, and inhalation are generally considered parts of the exposure pathway. Dose can also be received from eating or drinking contaminated food or water. This is called the ingestion dose. As in the case of inhaled material, ingested material can concentrate in various organs. Ingestion of milk receives special attention because radioiodine from a plume can contaminate grass eaten by dairy herds. This radioiodine, which can be greatly concentrated in the milk, can then concentrate in the drinker's thyroid gland.

The actual doses received by individuals off-site as a result of an accidental release would depend primarily on three sets of factors:

1. the release (source term) characteristics,

2. the weather during and after the release, which would determine the concentrations of airborne radionuclides and ground contamination off-site, and

3. the protective actions taken by individuals located off-site.

Source term classes are discussed below. The impact of weather on off-site consequences is discussed in Section 5.2. Subsection 5.1.11 discusses rationale for implementing protective actions. The impact of protective actions on off-site health effects is discussed in Section 5.4.

5.1.4 Source Term Characteristics

Source terms are typically characterized by the fractions of the core inventory of radionuclides that are released to the environment, as well as the time and duration of the release, the size distribution of the aerosols released, the elevation of the release, and the energy released with the radioactive material. Although the illustrations and comparisons of source terms in this section emphasize the magnitudes of estimated releases, it is important to recognize that the other characteristics of the source term noted above can also have an important effect on the ultimate off-site doses. For example, if the plume is hot, buoyancy (plume rise) may loft the plume over nearby populations, which would greatly reduce short-term population doses. Also, if the release is slow (takes a long time), shifts in wind direction may mean that no single group of people would be exposed to the entire plume. Such effects are discussed further in Section 5.2.

The isotopic composition of a source term is important because it determines decay rates and thus radiation exposure rates. Rapidly decaying nuclides deliver most of their dose quickly at short distances from their release point. Conversely, slowly decaying nuclides deliver dose over many years out to great distances from their release point. The chemical and physical form of the released radioactive materials will also influence off-site doses. For example, if only noble gases are released, deposition to the ground and incorporation into the food chain will not take place thereby eliminating several important long-term exposure pathways. Conversely, if the radioactive materials released were all in the form of water insoluble particles that are too large to be respirable, then lung exposures due to inhalation would not occur.

5.1.5 Health Effects

Radiation exposures can effect the health of exposed individuals. The type of effect, its severity, and the length of time until the effect appears are determined by the total dose received, the rate of exposure, and the exposed organs, and the degree of medical treatment received.

5.1.5.1 Chronic (Latent) Effects

Small doses or moderately large doses received at low dose rates (e.g., long term exposure to low levels of ground contamination) can cause health effects such as cancer, which appear later in time and are not directly observable following the exposure. Such effects are called chronic effects.

The risk of cancer is generally presumed to be proportional to dose, no matter how small. Computer models assume that a collective dose of about 2,000 person-rem (0.1 rem to 20,000 people, 0.01 rem to 200,000 people, etc.) will result in one radiation-induced cancer in the affected population.[3] Because the release is spread over a larger area and therefore over a larger population the farther it moves from the plant, a sizable fraction of the radiation-induced cancers could result from very small exposures beyond 50 miles from the plant. This is illustrated in Figure 5.1-3.

5.1.5.2 Acute Health Effects

Large doses received over short time periods threaten both the short and long term health of exposed individuals. If exposures are sufficiently intense, exposed organs are damaged causing radiation sickness or death within days or months. As a class, such early health effects are called acute. Radiation sickness includes vomiting, diarrhea, loss of hair, nausea, hemorrhaging, fever, loss of appetite, and general malaise. Deaths can be caused by failures of the lungs, small intestine, or blood forming bone marrow. Barring death or complications, recovery from radiation sickness occurs in a few weeks to a year depending on the dose received. Exposed individuals who survive radiation sickness are still subject to increased risk of latent effects such as cancers.

Because damage sufficient to impair organ functioning does not occur if exposures are small, short term health effects usually have dose thresholds. That is, the effect does not appear until the dose received is greater than the threshold dose (D_{th}). Once the threshold dose has been exceeded, the fraction of the exposed population in which the health effect occurs (the health effect's incidence) rises rapidly with increasing dose until the effect appears in all of the exposed individuals. The dose at which a health effect is induced in half of the exposed population is called the D_{50} dose (LD_{50} if the dose is lethal).

Figure 5.1-4 depicts the average dose equivalents in millirems received from natural background, common medical procedures, and frequent human activities.[4] As indicated in the figure, early injuries generally would appear at doses above 50 to 100 rem to the whole body, and early deaths would be expected at much higher doses (250 rem or more). It has been estimated that, with minimal medical treatment, about 50% of the people who receive a whole-body dose (LD_{50}) of 300 rem would die within 60 days. LD_{50} has been estimated to increase to 450 rem with supportive medical treatment.[5]

In considering off-site protective actions against releases from nuclear power plant accidents, both acute dose to the bone marrow and thyroid doses are important. Dose to the bone marrow (mostly from shine) is controlling in terms of early deaths for reactor accidents. Thyroid dose is important because inhalation or ingestion of small amounts of radioiodine can result in damage or destruction of the thyroid. However, unlike bone marrow dose, dose to the thyroid will not be fatal in the short term in most cases. There would, of course, be increased risk of death due to thyroid cancer.

5.1.6 Protective Actions

The public can usually be protected from an uncontrolled release of radiological material only by some form of intervention (e.g. evacuation) that disrupts normal living. Such intervention is termed protective action. This subsection presents basic radiation protection objectives and protective action guides that establish the magnitude of radionuclide releases requiring early protective action. A more complete discussion of protective actions that may be appropriate during or after a severe reactor accident is presented in Section 5.4.

5.1.6.1 Basic Radiation Protection Objectives

Any protective actions taken in response to a severe accident at a nuclear power plant should have the following objectives:

1. to <u>avoid</u> (prevent) doses sufficient to cause early health effects (injuries or deaths) that would be seen at specific organ (e.g., bone marrow or thyroid) doses above 50 rem;

2. to reduce early off-site doses that would, without protective action, exceed the limits established by the U.S. Environmental Protection Agency (EPA) and U.S. Department of Health and Human Services (HHS) Food and Drug Administration (FDA) protective action guides (see next subsection); and

3. to control total long-term health effects (e.g. cancers).

These objectives are listed in decreasing order of importance. Obviously, initial protective actions should be directed toward meeting the first objective by keeping the acute doses from the passing plume (cloud shine, ground shine, and inhalation) below levels that could result in early injuries or deaths. The NRC has developed guidance for meeting this first objective based on numerous severe accident studies. This guidance, which calls for the initiation of offsite protective actions before or shortly after the start of a major release, is discussed in Section 5.4.3.

5.1.6.2 Protective Action Guides

A Protective Action Guide (PAG) is the projected dose to reference man, or other defined individual, from an unplanned release of radioactive material at which a specific protective action to reduce or avoid that dose is recommended.[6] The Environmental Protection Agency (EPA) and Food and Drug Administration (FDA) have established PAGs that are applicable to severe reactor accidents. These PAGs must be considered in licensees emergency plans and decisions as discussed in Sections 5.3 and 5.4.

Protective actions whose implementation early in an accident (before or shortly after an accidental release of radionuclides to the environment) would be crucial to their effectiveness include evacuation, sheltering, improvised respiratory protection, and the use of potassium iodide to block iodine uptake by the thyroid. These protective actions are discussed in Section 5.4. The Environmental Protection Agency has established PAGs for early protective actions. These PAGs pertain to the second of the basic radiation protection objectives (i.e. reduce doses) rather than the first objective (i.e., avoid early fatalities and serious injuries). The PAG levels are well below the levels that would cause early health effects. At PAG levels, no health effects would be detectable, even for sensitive populations such as pregnant women.

There are currently two different sets of Environmental Protection Agency PAGs in use for early protective actions. The older PAGs, which were promulgated in 1980, are summarized in Table 5.1-3a. Reactor licensees continue to use the older PAGs until they revise their Emergency Plans to adopt new EPA PAGs. The new PAGs were published in 1991 and are summarized in Table 5.1-3b. The new EPA PAGs are based on the sum of the effective dose equivalent resulting from external exposure to the plume and the committed effective dose equivalent from inhalation. In contrast, the older PAGs in Table 5.1-3a are based on the external gamma dose from plume exposure and the committed dose to the thyroid from inhalation. For reactor accidents, the new EPA PAGs should not have any impact on protective action decisions because the thyroid dose is the controlling factor and the method for projecting the thyroid dose does not change.

It is important to emphasize that protective action guides are based on projected doses--future doses that can be avoided by the specific protective action being considered. Doses incurred prior to initiation of the protective action should not normally be included. Similarly, in considering early protective actions such as evacuation or sheltering, doses that could be avoided by intermediate or long term protective actions such as control of contaminated food and water are excluded.

5.1.7 Radionuclide Releases Requiring Protective Action

It is not obvious in examining a specified radionuclide source term what the potential health impact would be to the public. Based on the compilation of a number of consequence analyses, however, Table 5.1-4 shows the number of curies of radioiodine (I-131) or noble gases that would have to be released to the atmosphere to result in doses equal to the protective action guides under average meteorological conditions.[2] It is instructive to compare the inventory of radionuclides in various plant locations the amounts that would have to be released to induce doses equal to the protective action guide levels.

Table 5.1-5 summarizes annual releases of noble gases and radioiodine during normal light water reactor operation. As indicated in the table, a 1-hr release rate more than 100,000 times normal release rates would be required for protective action guides to be exceeded.

Comparisons of Tables 5.1.2 and 5.1.4 show that the release of even a very small fraction of the core radioactive material inventory to the atmosphere could result in doses exceeding the protective action guides near the site. However, only the core, spent-fuel storage pool, and the reactor coolant contain the requisite inventory of radionuclides. Accidents not involving one of these three regions (e.g., gas-decay tank rupture) should not result in off-site doses in excess of the Environmental Protection Agency protective action guides.*

Dose levels ten or more times higher than the protective action guides are required to induce early injuries or fatalities. Only the reactor core contains sufficient radioactive material and energy (e.g., decay heat) to result in prompt atmospheric releases that could result in early deaths and injuries off-site. Under average meteorological conditions, about ten times more radioactive material than indicated in Table 5.1-4 would have to be released. Iodine release fractions of 0.1 and 0.01 would be required to exceed the thresholds for early fatalities and early injuries respectively.[7]

In addition to core damage, a release sufficient to result in early injuries and/or fatalities would require a direct pathway to the environment and a driving force (e.g., steam). In essence, all three fission product barriers--cladding, reactor coolant system and containment would have to fail. The radioactive material released from the core would have to move through the reactor coolant system (second barrier) and containment (third barrier) without being significantly filtered or removed by other methods such as containment sprays, ice condensers, fan coolers, or suppression pools. Even if such engineered safety features failed, over time natural removal processes (e.g., condensation and scrubbing) would remove most particulate fission products from the atmosphere of an intact containment. Therefore, if the containment holds for several hours and the containment sprays or other removal systems work, early injuries or fatalities would be highly unlikely.

Figure 5.1-5 uses the concept of an event tree to display the potential public health consequences due to severe accidents. Moving from left to right in the figure, "yes/no" answers to questions at the top result in a series of branches, possibly to off-site consequences. For example, if only the radioactive material contained in the fuel pins (gaps) is released with late containment failure, the off-site consequences would be small (branch 7 in Figure 5.1-5). If all answers are yes, branch 1 indicates extremely severe off-site consequences. Figure 5.1-5 emphasizes two fundamental public health questions that must be considered during a severe accident: 1) What is the status of the reactor core?, and 2) What is the status of the reactor containment?

* One caveat is important: the Food and Drug Administration has proposed a preventative protective action guide of 1.5 rem for the milk pathway. At this level, dairy animals should be removed from likely or actually contaminated pasture. Catastrophic accidental releases of ^{131}I from the waste gas storage tank at a pressurized water reactor site or from the effluent treatment system at a boiling water reactor could result, especially during a period of precipitation, in pasture contamination leading to a projected dose of 1.5 rem or greater via the contaminated milk ingestion pathway.

5.1.8 Status of Core and Containment

During an accident, the principal focus of the control room staff is on maintaining critical safety functions required to prevent core damage. Instrumentation, information-display, and operating procedures assist in maintaining critical safety functions and provide sufficient information to permit the threat or actual occurrence of core damage to be assessed.

Some of the information available in the control room to assess the core status is listed in Table 5.1-6. Means of detecting fission product barrier failures and gross radionuclide movements prior to and after a major release are depicted in Figure 5.1-6. Critical safety functions and activities of the control room staff during an accident are discussed further in Section 5.3.

Containment isolation failure or containment bypass, which would occur at the start of an accident, minutes to hours before a major release, would generally be detectable. However, most severe accident scenarios would involve an initially intact containment that would be challenged by beyond-design-basis pressure and temperature loads. Actual containment failure would be fairly easy to detect, but this might be too late for initiating effective off-site protective actions (see Section 5.2). Predicting the mode and timing of containment failure would not be possible for most severe accident sequences.

Figures 5.1-7 and 5.1-8 show the uncertainty in the probability of early containment failure conditional on the occurrence of three different classes of accident sequences for the plants analyzed in NUREG-1150.[7] Containment bypass scenarios are not included in these figures, and the results are for internally initiated accidents only. The plant-specific mean frequency of the accident class is listed to the right of each uncertainty interval. For some of the plants (e.g., Zion and Surry) the best estimate of the conditional probability of early containment failure is quite small (about 1%); however, for all plants the uncertainty in the estimated likelihood of early containment failure is quite large. This uncertainty arises as a result of corresponding uncertainties in both the pressures and temperatures that would exist within the containments and the ability of the containments to withstand these pressures and temperatures. In addition, for several of the containments there is uncertainty regarding the mode (structural mechanism, location, size of opening, etc.) by which containment would fail.

During a severe accident it would be very difficult or impossible to predict with confidence the performance of the containment. However, based on NUREG-1150, the conditional probability of containment failure and a release requiring protective action under EPA PAG ranges may be as high as 0.5 for some plants. The conditional probability of a release that could result in early health effects is much lower, about 0.001 or less.

5.1.9 Design Features That Impact Source Terms

In Module 4, performance of the containment was described with respect to the timing of the onset of containment failure and the magnitude of leakage to the environment. In particular, the likelihood of early containment failure was used as a measure of containment performance. However, as indicated in Figure 1.6, off-site health effects are "possible" not "certain" given early containment failure. In part, this is because environmental source terms are affected by more than just the mode and timing of containment failure. The following paragraphs describe the effect of different safety systems and plant features on the magnitude of source terms. In addition, uncertainties exist in our ability to quantify source terms and to predict off-site doses given source terms. These uncertainties are discussed in Sections 5.1.10 and 5.2, respectively.

5.1.9.1 Suppression Pools

Suppression pools can be very effective in the removal of radionuclides in the form of aerosols or soluble vapors. Some of the most important radionuclides, such as isotopes of iodine, cesium, and tellurium, are primarily released from fuel while it is still in the reactor vessel. Because risk-dominant accident sequences in BWRs are typically initiated by transients rather than pipe breaks, the in-vessel release is directed to the suppression pool rather than being released to the drywell. As a result, the in-vessel release is subjected to scrubbing in the suppression pool, even if containment failure has already occurred. For the Peach Bottom plant, decontamination factors used in NUREG-1150 for suppression pool scrubbing of the in-vessel releases ranged from approximately 1.2 to 4000, with a median value of 80. Since the early release of volatile radioactive material is typically the major contributor to early health effects, the effect of the suppression pool in depressing this component of the release is one of the reasons the likelihood of early fatalities is low for the BWR designs analyzed in NUREG-1150.

Although the decontamination factors for suppression pools are typically large, radioactive iodine captured in the pool will not necessarily remain there. Reevolution of iodine was found to be important in accident scenarios in which the containment fails and the suppression pool is boiling.

5.1.9.2 Drywell-Wetwell Configuration

Depending on the timing and location of containment failure, the suppression pool may also be effective in scrubbing the release occurring during core-concrete attack or reevolved from the reactor coolant system after vessel failure. In the NUREG-1150 analyses for Peach Bottom (Mark I containment), containment failure was found to be likely to occur in the drywell early in the accident. Thus, in many scenarios the suppression pool was not effective in mitigating the delayed release of radioactive material.

The Mark III design has the apparent advantage, relative to the Mark I and Mark II designs, of the wetwell boundary completely enclosing the drywell, in effect providing a double barrier to radioactive material release. As long as the drywell remains intact, any release of radioactive material from the fuel would be subject to decontamination by the suppression pool. With the Mark III drywell intact, the environmental source terms is reduced to a level at which early fatalities would not be expected to occur, even for early failure of the outer containment. However, for Grand Gulf (Mark III containment), drywell failure accompanied containment failure in approximately one-half the early containment failure scenarios analyzed and the suppression pool was found to be ineffective in mitigating ex-vessel releases in such scenarios.

5.1.9.3 Containment Sprays

Given adequate time, containment sprays can also be effective in reducing airborne concentrations of radioactive aerosols and vapors. In the Surry (subatmospheric) and Zion (large, dry) designs, approximately 20 percent of the NUREG-1150 core meltdown sequences were predicted to eventually result in delayed containment failure or basemat meltthrough. The effect of sprays, in those scenarios in which they are operational for an extended time, is to reduce the concentration of radioactive aerosols airborne in the containment to negligible levels in comparison with non-aerosol radionuclides (e.g., noble gases). Typically sprays can reduce airborne aerosol activities by an order of magnitude in 15 to 20 minutes. For shorter periods of operation, sprays would be less effective but could still have a substantial mitigative effect on the release. Without sprays, an order of magnitude reduction in airborne aerosol activities would typically take about 10 hours.

The Sequoyah (ice condenser) design has containment sprays for the purpose of condensing steam that might bypass the ice bed, as well as for use after the ice has melted. The effects of the sprays and ice beds in removing radioactive material are not completely independent since they both tend to preferentially remove larger aerosols.

5.1.9.4 Ice Condenser

The ice beds in an ice condenser containment remove radioactive material from the air by processes that are very similar to those in the BWR pressure-suppression pools. The decontamination factor is very sensitive to the volume fraction of steam in the flowing gas, which in turn depends on whether the air-return fans are operational. For a typical case with the air-return fans on, the magnitude of the decontamination factor was assessed to be in the range from 1.2 to 20, with a median value of 3. Thus, the effectiveness of the ice bed in mitigating the release of radioactive material is likely to be substantially less than for a BWR suppression pool.

5.1.9.5 Reactor Cavity Flooding

The configuration of PWR reactor cavity or BWR pedestal regions affects the likelihood of water accumulation and water depth below the reactor vessel. The Surry reactor cavity is not connected by a flowpath to the containment floor. If the spray system is not operating, the cavity will be dry at vessel failure. In the Peach Bottom (Mark I) design, there is a maximum water depth of approximately 2 feet on the pedestal and drywell floor before water would overflow into the suppression pool via the downcomer. Other designs investigated such as Sequoyah and Zion have substantially greater potential for water accumulation in the pedestal or cavity region. In the Sequoyah design, the water depth could be as much as 40 feet.

If a coolable debris bed is formed in the cavity or pedestal and makeup water is continuously supplied, core-concrete release of radioactive material would be avoided. Even if molten core-concrete interaction occurs, a continuous overlaying pool of water can substantially reduce the release of radioactive material to the containment.

5.1.9.6 Building Retention

In NUREG-1150, radionuclide retention was evaluated for the Peach Bottom reactor building. (An evaluation was not made for the portion of the reactor building that surrounds the Grand Gulf containment, which was assessed to have little potential for retention.) The range of decontamination factors for aerosols for the Peach Bottom reactor building subsequent to drywell rupture was 1.1 to 80 with a median value of 2.6. The location of drywell failure affects the potential for reactor building decontamination. Leakage past the drywell head to the refueling building was assumed to result in very little decontamination. Failure of the drywell by meltthrough resulted in a release that was subjected to a decontamination factor of 1.3 to 90 with a median value of 4.

In the NUREG-1150 analyses of PWR interfacing LOCA sequences, some retention of radionuclides was assumed in the auxiliary building (in addition to water pool decontamination for submerged releases). In the Sequoyah analyses, retention was enhanced by the actuation of the fire spray system.

5.1.9.7 BWR Containment Venting

In the Peach Bottom (Mark I) and Grand Gulf (Mark III) designs, procedures have been implemented to intentionally vent the containment to avoid overpressure failure. By venting from the wetwell air space (in Peach Bottom) and from the containment (in Grand Gulf), assurance is provided that, subsequent to core damage, the release of radionuclides through the vent line will have been subjected to decontamination by the suppression pool.

As discussed in Module 4, containment venting to the outside can substantially improve the likelihood of recovery from a loss of decay heat removal and, as a result, reduce the frequency of severe accidents. The results of NUREG-1150 indicate, however, only limited benefits in consequence mitigation for the existing procedures and hardware for venting. Uncertainties in the decontamination factor for the suppression pool and for the ex-vessel release and in the reevolution of iodine from the suppression pool are quite broad. As a result, the consequences of a vented release are not necessarily minor. Furthermore, the effectiveness of venting in the Peach Bottom (Mark I) and Grand Gulf (Mark III) designs is limited by the high likelihood of mechanisms leading to early containment failure that cannot be prevented by venting.

5.1.10 Uncertainty in Source Term

As expected, the magnitude of the source term varies depending on whether or not containment fails, when it fails, and the effectiveness of engineered safety features in mitigating the release. However, even within a given accident progression bin, which represents a specific set of accident progression events, the uncertainty in predicting severe accident phenomena is great.

5.1.10.1 NUREG-1150 Insights

A major shortcoming of the 1975 Reactor Safety Study was the limited treatment of the uncertainties in severe accident source terms. In the intervening years, particularly subsequent to the Three Mile Island accident, major experimental and code development efforts have broadly explored severe accident behavior. In the comprehensive NUREG-1150 study, which was published in 1989, care was taken to assess and display the uncertainties associated with the analysis of accident source terms. Many of the severe accident issues that are now recognized as the greatest sources of uncertainty were completely unknown to the earlier Reactor Safety Study analysts.

In the 1975 Reactor Safety Study, source terms were developed for nine release categories ("PWR-1" to "PWR-9") for the Surry plant and five release categories for the Peach Bottom plant ("BWR-1" to "BWR-5"). In NUREG-1150, source terms were developed for a much larger number of accident progression bins. For each accident progression bin, an estimate of the uncertainty in the release fractions for each of the elemental groups was obtained. Figure 5.1-9 provides a comparison of an important large release category (PWR-2) from the Reactor Safety Study with a comparable aggregation of accident progression bins (early containment failure, high reactor coolant system pressure) from NUREG-1150. Figure 5.1-10 compares results for an isolation failure in the wetwell region from the Reactor Safety Study, release category BWR4, with the venting accident progression bin from NUREG-1150. The Reactor Safety Study results are very similar to the mean release terms for the venting bin, with the exception of the iodine group, which is higher because of the late release mechanisms (reevolution from the suppression pool and the reactor vessel) considered in the NUREG-1150 study. Overall, the comparisons indicate that the source terms in the Reactor Safety Study were in some instances higher and in other instances lower than those in the current study. However, for the early containment failure scenarios that have the greatest impact on risk, the Reactor Safety Study source terms are larger than the mean values of the NUREG-1150 study and are typically at the upper bound of the uncertainty range.*

*Additional comparisons with the Reactor Safety Study are presented in NUREG-1150 Reference 10.9.

5.1.10.2 On-Line Monitoring

As indicated above, it is not possible to predict with certainty the source term that would result from a given plant damage state. What, then, is the feasibility of on-line monitoring to measure source term characteristics required to project off-site doses?

As part of the upgrades that followed the TMI-2 accident, on-line radiation monitors capable of measuring the noble gases released through plant vents were installed. On-line monitors for iodine and other particulates were not considered practical. Therefore, the presence of iodine and particulates in a release is determined through analysis of samples taken during the release. Unfortunately, this could require several hours. Note that noble gases are not considered as great a threat to the public as radioactive iodine and other particulates. Although current systems can characterize most releases, they cannot provide fast estimates of those very unlikely releases that pose the greatest threat to the public.

Plants are designed to accommodate routine releases of radioactivity and to minimize releases resulting from abnormal conditions and accidents. However, as indicated in Figure 5.1-11, because an accident resulting in off-site early health effects (death and injuries) would have to be fast, direct, and unfiltered, such a release would most probably be via an unmonitored pathway to the atmosphere. The most important example is a release due to a major containment failure or major containment penetration failure. As a result, effluent-monitoring systems located in routinely monitored release pathways (e.g., stacks) would not be able to assess the extent and the characteristics of such a severe release.

For accidents where the total release is through a monitored pathway (e.g., the stack), it may be possible to obtain a good characterization of the release. At a minimum, the magnitude in relative terms (e.g., this release has the possibility to exceed EPA PAGs) can be estimated-if the monitors stay on scale. By their very nature, however, releases resulting in off-site dose high enough to cause early health effects most likely cannot be characterized by effluent monitors.

5.1.11 Bases for Recommending Protective Action

As indicated in Section 5.1.6, a protective action guide is the projected offsite dose at which a specific protective action to reduce or avoid that dose is recommended. To make real-time offsite dose projections during an accident would require:

1. Assessing the current and projected status of the core

2. Predicting the occurrence, mode, and timing of containment failure

3. Predicting the source term including the radionuclide release fractions, the energy of the release, and the duration of the release; and

4. Predicting the atmospheric dispersion, ground contamination, and resulting exposure pathway doses to individuals off-site.

Actions to protect the public must be initiated before or upon a major release to the atmosphere for them to be fully effective (see Section 5.2). As explained in the following paragraphs, only the first of the four steps listed above can be performed with certainty in time to initiate effective off-site protective actions. Consequently, protective action decisions should be based on actual indications of core damage rather than real-time dose projections.

It is important to remember (Figure 5.1-5) that core damage is necessary for early off-site health effects. Given core damage, there must have been major human error or equipment failure. Under these conditions, there may be little assurance that further failures or a major release is not possible because the plant parameters are well beyond their design limits. Some have estimated that as many as one in ten core melt accidents would result in a major release sufficient to cause death and severe injuries off-site if effective protective actions were not taken early in the accident sequence.[2] Certainly, considering the uncertainties discussed in Sections 5.1.8 and 5.1-10, the possibility of early containment failure and a large release given core damage should be taken very seriously in considering whether to initiate off-site protective actions.

Even if it were somehow possible to predict the exact mode and timing of containment failure and all of the source term characteristics during a severe accident, real time projections of off-site doses and health effects would still be uncertain due to uncertainties in predicting atmospheric dispersion and ground contamination resulting from a given source term. These uncertainties are discussed in Section 5.2.

In the event of a severe accident, early, precautionary protective action decisions should be based on in-plant observables (control room indicators of core damage) and conservative, precalculated dose projections rather than on early, real-time dose projections. This conclusion is based on the relatively high probability of a major release given core damage, the relative ease (of using a few key indicators) for the plant staff to detect major core damage, the large uncertainties associated with projecting containment failure and associated source terms, the great difficulties in making accurate and timely dose projections, and the fact that off-site protective actions would be most effective if initiated before a major release occurred (e.g., precautionary evacuation).

Current regulations require nuclear power plants to establish four classes of emergencies for which various levels of response are preplanned. Licensees have established and incorporated into their procedures emergency action levels (EALs) based on control room instrumentation that would indicate the class of emergency. An emergency in the most serious class is called a General Emergency. Declaration of a general emergency indicates that immediate off-site protective actions should be taken. Severe core-damage accidents have a very real potential for causing significant off-site health effects and are, therefore, to be classified as General Emergencies. While some events have been postulated that could quickly lead to a major release, most severe accidents would be classified as general emergencies by the emergency action levels well before a major release. Emergency classification and emergency action levels are discussed further in Section 5.3.

5.1.12 Major Points

The major points covered in this section are summarized as follows:

1. The release to the atmosphere of only a small fraction of the inventory of radionuclides in the core of an operating light water reactor could result in off-site health effects.

2. Core damage and a fast, direct release pathway are required for inducing early fatalities or injuries off-site. Accidents or incidents less grave than significant core damage, or the imminent threat thereof, would not warrant predetermined protective actions off-site.

3. In many severe accident scenarios, containment and or associated safety features such as containment sprays, suppression pools, and ice condensers would reduce the magnitude of a severe accident source term to levels that would preclude off-site health effects; however,

4. Given conditions leading to core melting, the possibility of early failure of containment or associated safety features cannot be precluded.

5. Even given a specific set of accident progression events, the uncertainty in predicting severe accident source terms and associated off-site doses is very large.

6. Early off-site protective actions must be driven by knowledge of actual core damage for which there would be clear indicators in the control room.

Table 5.1-1. Radioactive materials in a large [3300-MW(t)] light water reactor core grouped by relative volatility.

Volatility	Inventory (Ci)
Noble Gases (100% release possible)	
Krypton (Kr)	1.7E+8
Xenon (Xe)	2.2E+8
Very Volatile	
Iodine (I)	7.5E+8
Cesium (Cs)	2.3E+7
Moderately Volatile	
Tellurium (Te)	1.8E+8
Strontium (Sr)	3.5E+8
Barium (Ba)	3.4E+8
Less Volatile	
Ruthenium (Ru)	2.4E+8
Lanthanum (La)	4.7E+8
Cerium (Ce)	3.9E+8

Table 5.1-2. Typical inventories of noble gases and iodine in reactor systems.

Location	Inventory (Ci)	
	Noble gases (Xe, Kr)	Iodine (I)
Reactor core total	4.0E+8	7.5E+8
Reactor core gap[a]	3.0E+7	1.4E+7
Spent fuel storage pool	1.0E+6	5.0E+5[b]
Primary coolant[c]	1.0E+4	6.0E+2[c]
Pressurized Water Reactor--other systems Waste gas storage tank	1.0E+5	1
Boiling Water Reactor--other systems Steam line Waste gas treatment system	1.0E+4[d] 5.0E+3	25[d] 0.25
Shipping cask	1.0E+4	1

[a]Gap between UO_2 fuel and Zircaloy cladding.
[b]One-third of the core is 30 days old; the rest is 1 year old.
[c]Nominal value at normal iodine levels can be much higher or lower (factor of 10) depending on fuel leakage.
[d]Ci/hr (circulating).

Table 5.1-3a. Environmental Protection Agency recommended protective actions[a] to reduce whole-body and thyroid dose from exposure to a gaseous plume

Projected Dose (rem) to the Population		Recommended actions[b]	Comments
Whole Body[c] Thyroid	< 1 < 5	No planned protective actions[d] State may issue an advisory to seek shelter and await further instructions. Monitor environmental radiation levels.	Previously recommended protective actions may be considered or terminated.
Whole Body Thyroid	1 to < 5 5 to < 25	Seek shelter as a minimum. Consider evacuation. Evacuate unless constraints make it impractical. Monitor environmental radiation levels. Control access.	If constraints exist, special consideration should be given for evacuation of children and pregnant women.
Whole Body Thyroid	5 and above 25 and above	Conduct mandatory evacuation. Monitor environmental radiation levels and adjust area for mandatory evacuation based on these levels. Control access.	Seeking shelter would be an alternative if evacuation were not immediately possible.

[a]EPA Manual of Protective Action Guides and Protective Actions for Nuclear Incidents, 1980.

[b]These actions are recommended for planning purposes. Protective action decisions at the time of the incident must take existing conditions into consideration.

[c]Effective dose from external sources (cloud and ground) is approximately equal to whole body dose.

[d]At the time of the incident, officials may implement low-impact protective actions in keeping with the principle of maintaining radiation exposures as low as reasonably achievable.

Table 5.1-3b. Environmental Protection Agency recommended protective actions[a] to reduce external gamma dose from plume exposure and committed dose to the thyroid from inhalation.

Projected Dose (rem) to the Population	Recommended actions[b]	Comments
1-5 rem[c]	Evacuation[d] (or sheltering)	Evacuation (or for some situations, sheltering[b]) should normally be initiated at one rem.
25 rem[d]	Administration of stable iodine	Requires approval of state medical officials.

[a]EPA Manual of Protective Action Guides and Protective Actions for Nuclear Incidents, 1991.

[b]Sheltering may be the preferred protective action when it will provide protection equal to or greater than evacuation, based on consideration of factors such as source term characteristics, and temporal or other site-specific conditions.

[c]The sum of the effective dose equivalent resulting from exposure to external sources and the committed effective dose equivalent incurred from all significant inhalation pathways during the early phase. Committed dose equivalents to the thyroid and to the skin may be 5 and 50 times larger respectively.

[d]Committed dose equivalent to the thyroid from radioiodine.

Table 5.1-3c. Food and Drug Administration (FDA) protective action guides (PAGs)

Organ	FDA PAG[b] dose (rem)	Protective Action
Whole body (bone)	0.5-5	At lower projected dose, use of grazing land should be restricted. At higher projected dose, contaminated milk should be impounded.
Thyroid	1.5-15	
Other body organs	0.5-5	

Table 5.1-4. Atmospheric release (Ci) necessary under poor meteorological conditions[a] to result in protective action guide levels at 1 mile

Radioactive Material	Pathway	Curies released[b]	
		15 rem--thyroid[c]	5 rem--whole body
Iodine (I-131)	Milk ingestion	2	-
	Inhalation	600	-
Noble gases (gamma emitters; Xe, Kr)	Cloud shine	-	1,500,000

[a]Conditions that result in doses higher than those projected under average conditions.
[b]Approximate minimum.
[c]Child's thyroid.

Table 5.1-5. Typical releases during normal operation

Source	Release	
	Noble gases	Radioiodine
Boiling water reactor		
Annual total	$1x10^6$	1
Release rate to equal annual total, Ci/hr[a]	$1x10^1$	$1x10^{-4}$
Factor by which normal release rate would have to be increased to give a 1 hour release that would exceed federal protective action guide level	$1.5x10^5$	$6x10^6$
Pressurized water reactor		
Annual total, Ci	$2x10^2$	$2x10^{-2}$
Release rate to equal annual total, Ci/hr[a]	$2x10^{-2}$	$2x10^{-6}$
Factor by which normal release rate would have to be increased to give a 1 hour release that would exceed federal protective action guide level	$7.5x10^7$	$3x10^8$

Table 5.1-6. Examples of instrumentation and information available for determination of fuel (core) status.

Instrumentation and Information	Type of reactor
Immediately available in control room	
Core temperatures--thermocouple	PWR
Containment radiation level	BWR, PWR
Radiation levels from condenser/air ejector	BWR, PWR
Neutron fluxes in core	BWR, PWR
Available after several hours	
Concentration or radiation level in circulation reactor coolant	BWR, PWR
Analysis of primary coolant--gamma spectrum	BWR, PWR
Containment hydrogen level (from samples)	BWR, PWR

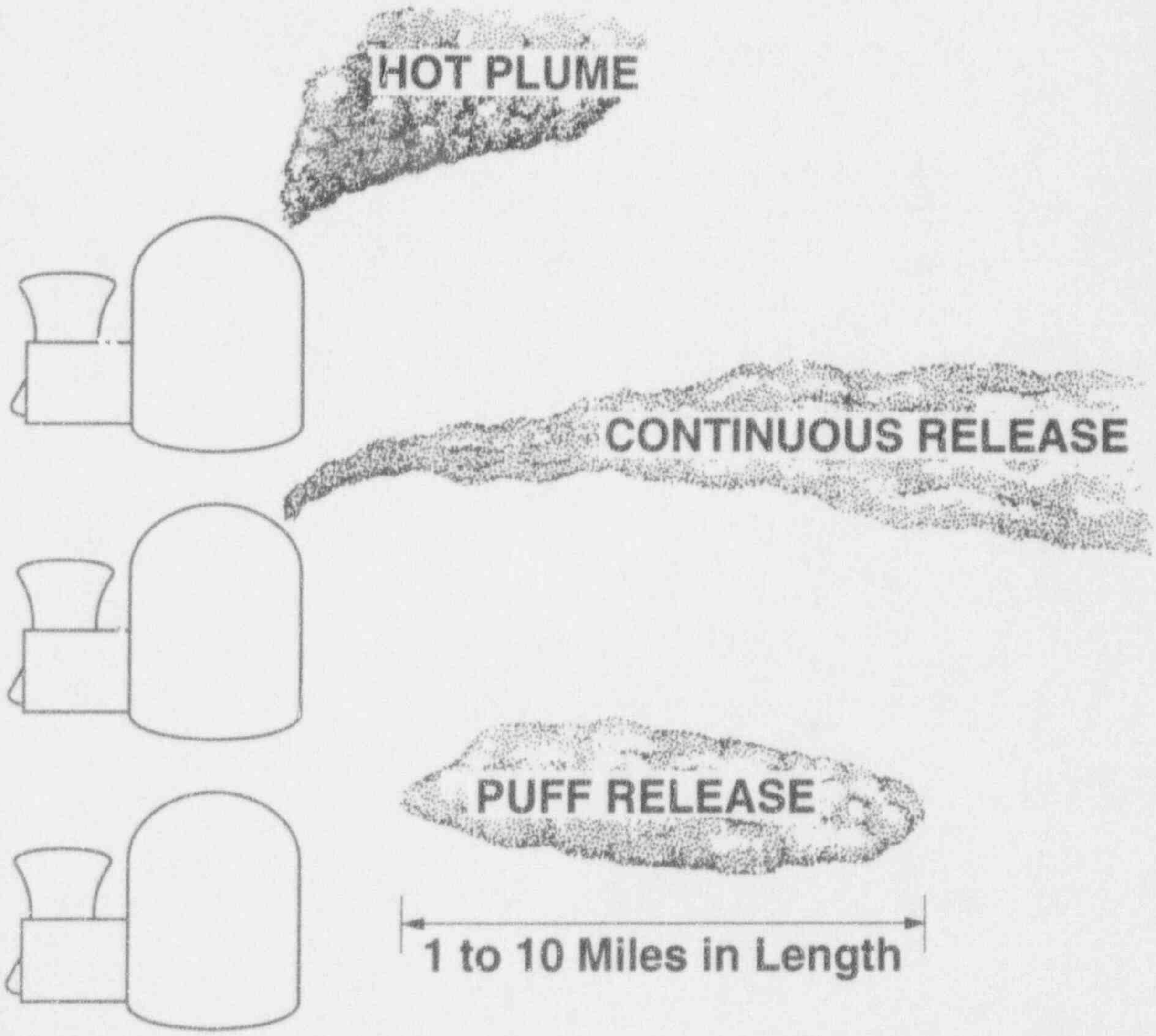


Figure 5.1-1 Examples of plume types

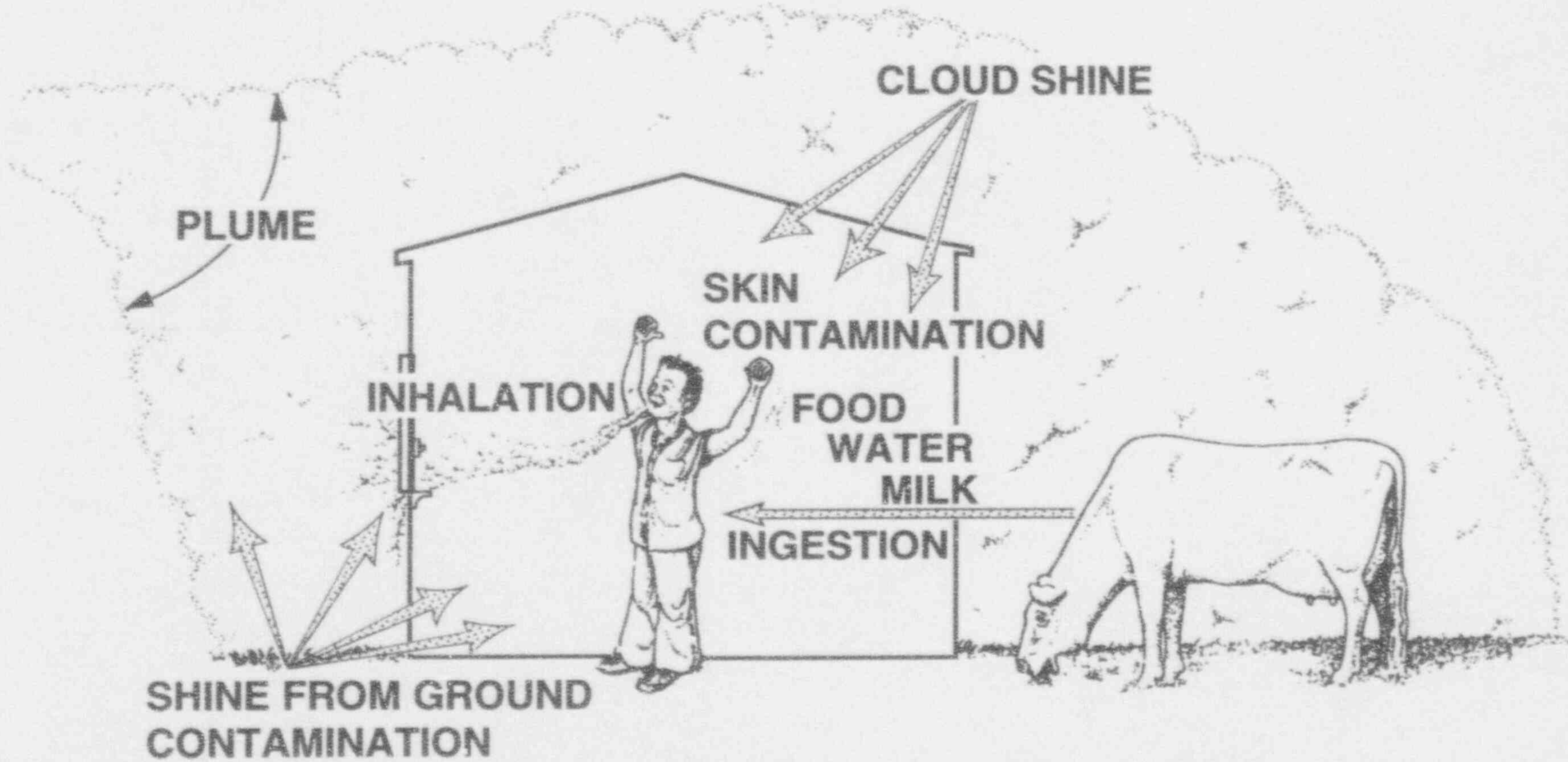


Figure 5.1-2 Radiation dose pathways

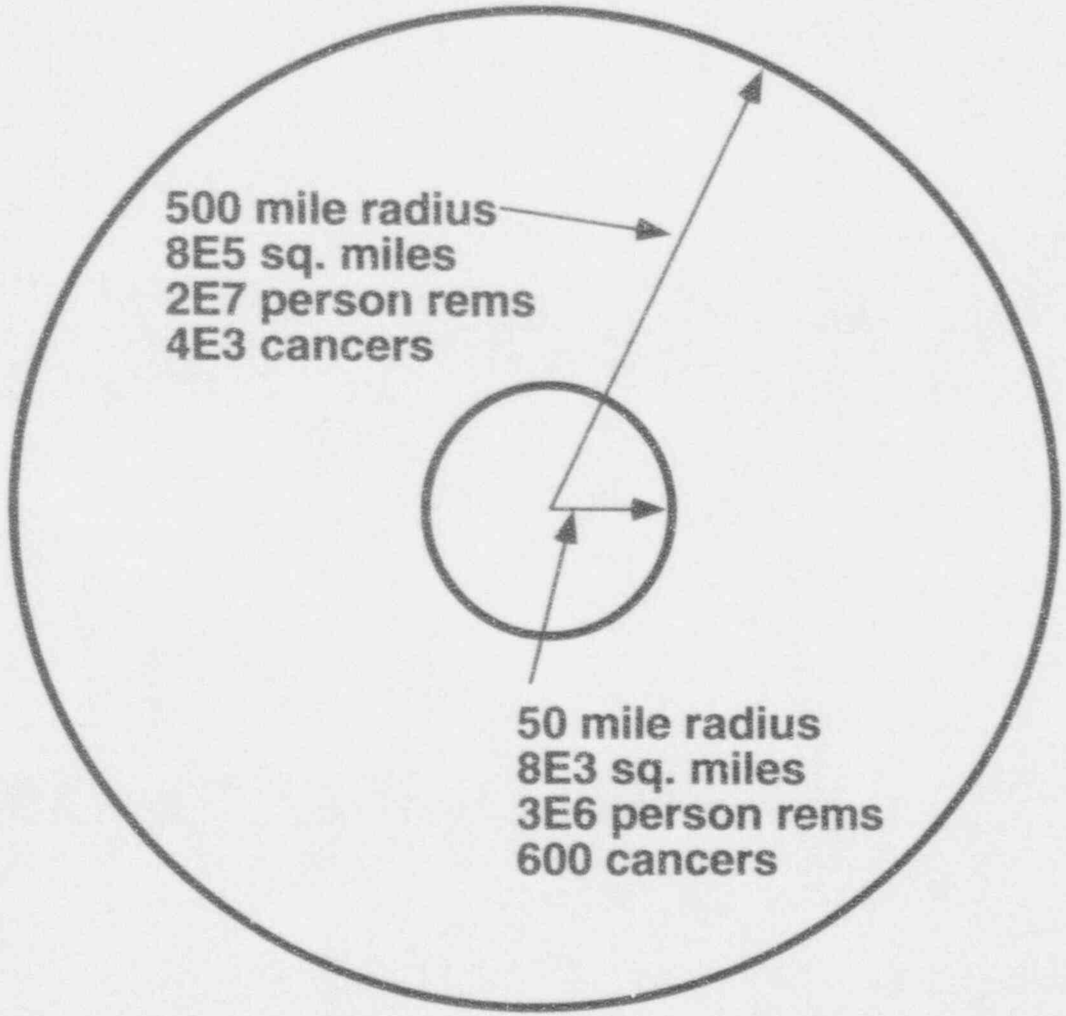


Figure 5.1-3 Illustration of person-rems and cancers within 50 and 500 mile radii. [Source: Reference 11]

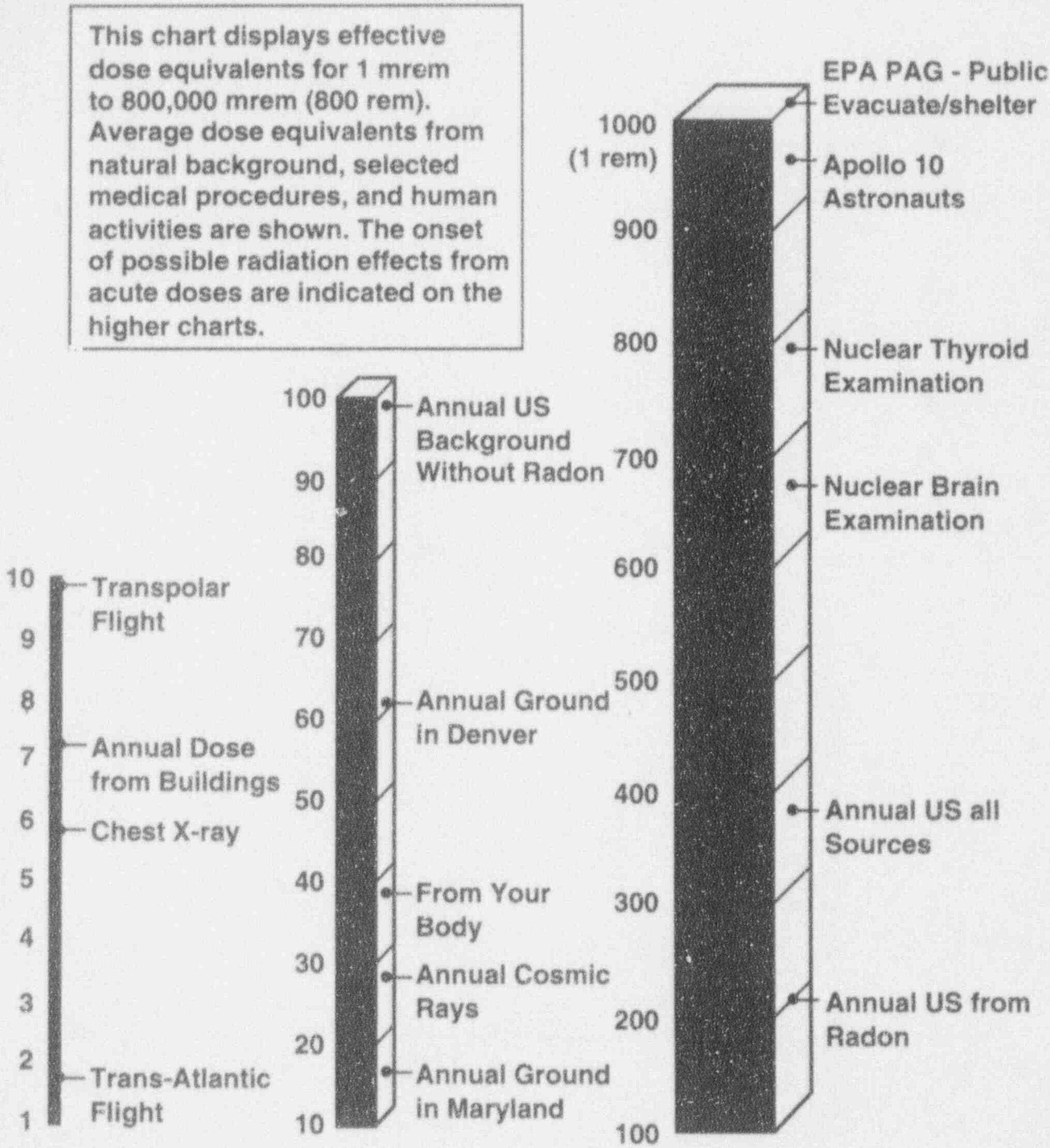
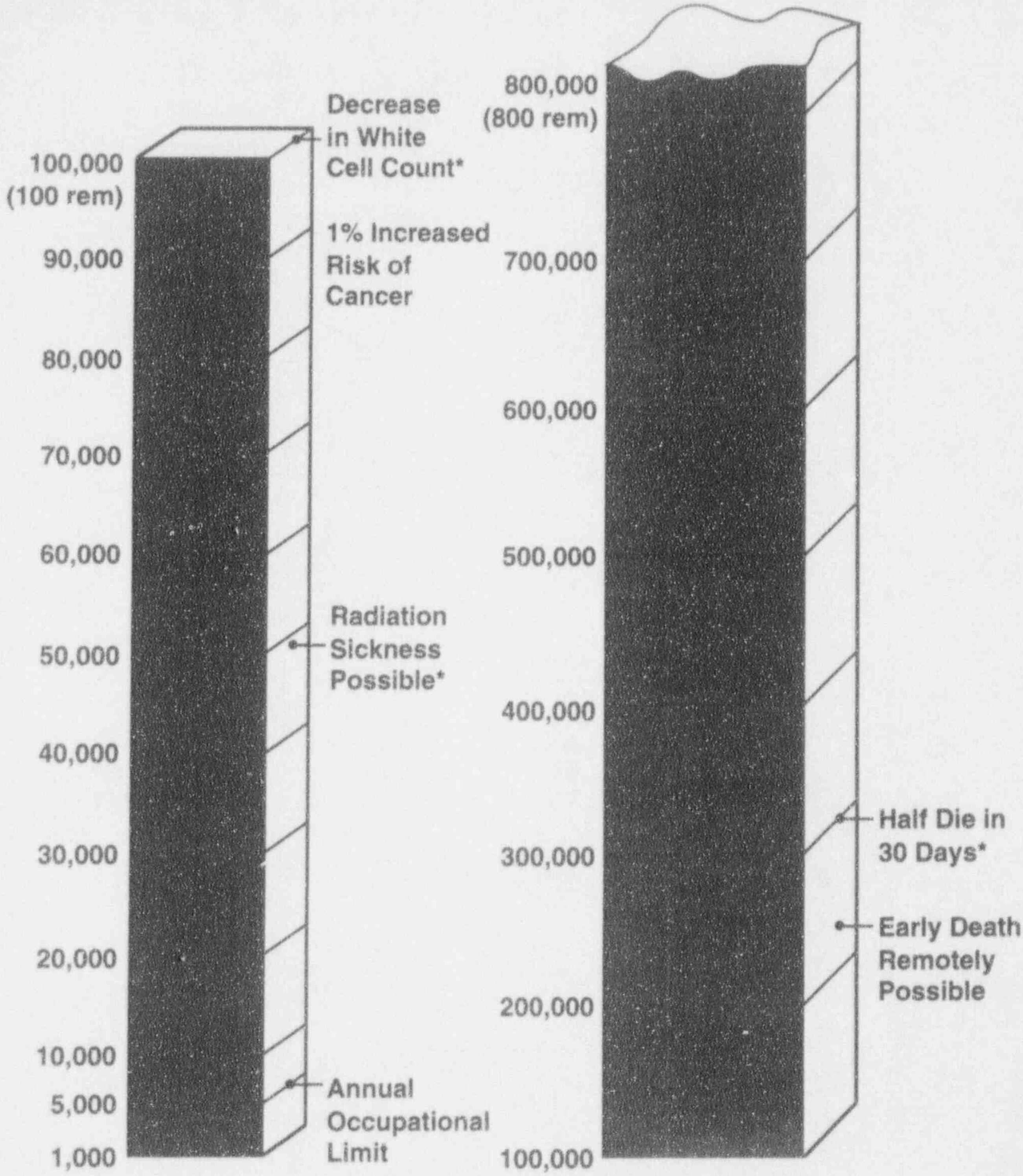


Figure 5.1-4a Putting radiation in perspective for the public (mrem)



* Onset of possible radiation effects due to doses received over a short time period at high dose rates (acute doses)

Figure 5.1-4b Putting radiation in perspective for the public (mrem)

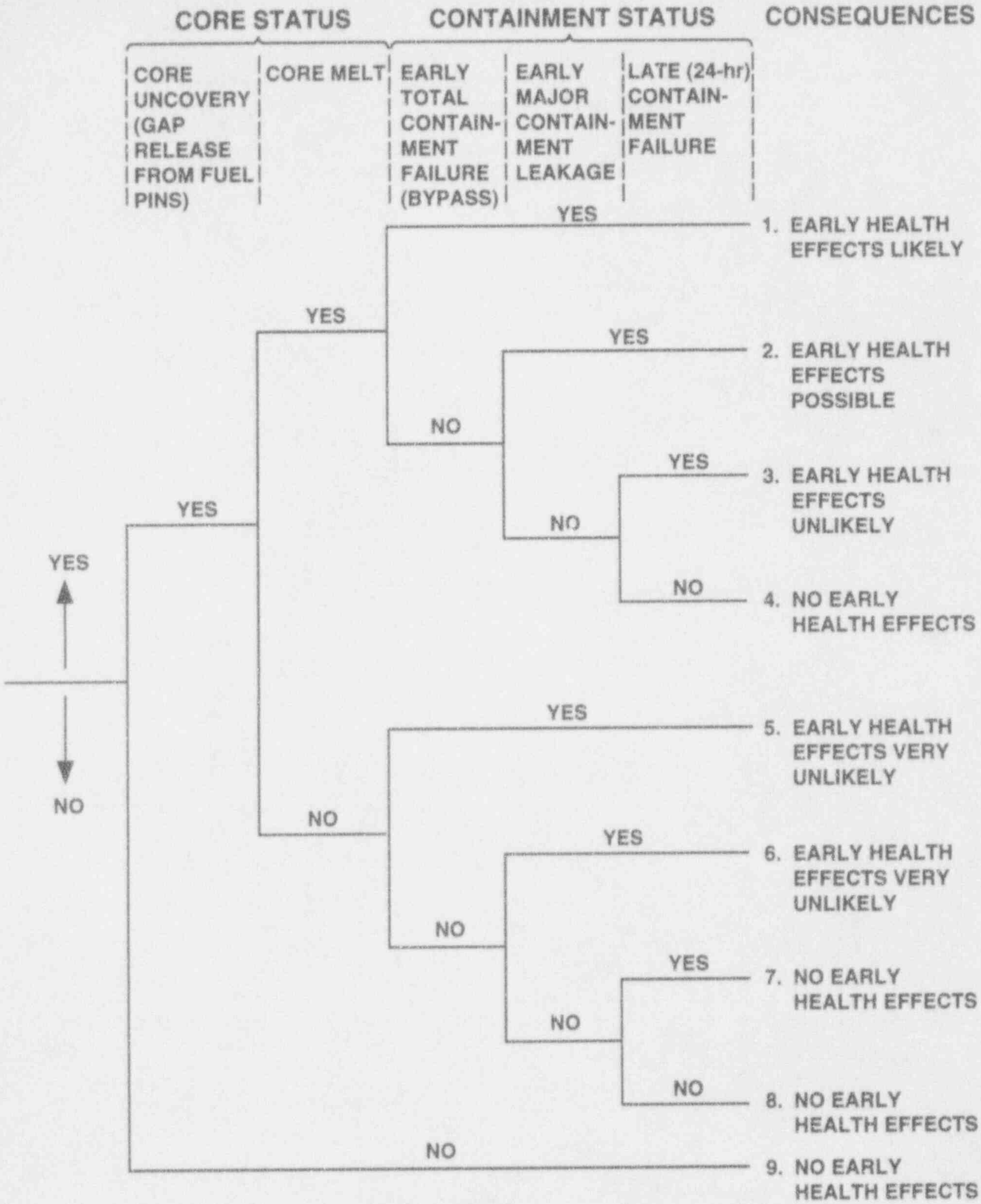
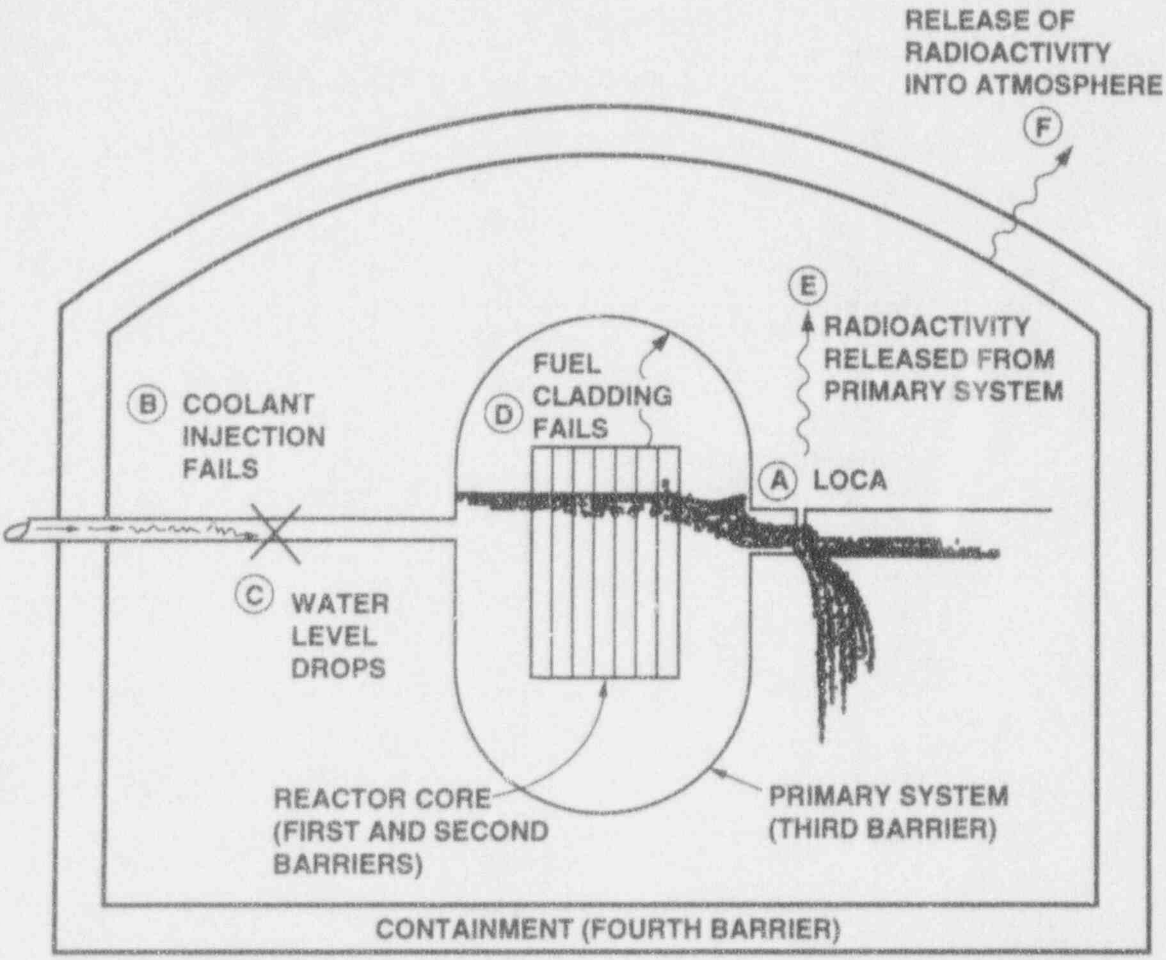


Figure 5.1-5 Event tree for severe accident consequences



LOSS OF COOLANT ACCIDENT (LOCA)	EXAMPLE CONTROL ROOM INDICATORS
A SYSTEM FAILURE - START OF ACCIDENT	PRESSURE, TEMPERATURE
B ENGINEERING SAFETY FEATURE (ESF) FAILURE	FLOW, TEMPERATURE
C CRITICAL SAFETY FUNCTION (CSF) FAILURE	CORE TEMPERATURE
D BARRIER FAILURE	RADIATION, TEMPERATURE
E MOVEMENT OF RADIOACTIVE MATERIAL	RADIATION
F RELEASE TO ATMOSPHERE (CONTAINMENT LEAKAGE)	OFF - SITE DOSE RATE (e.g., AT GUARD SHACK)

Figure 5.1-6 Example of control room indication before a release

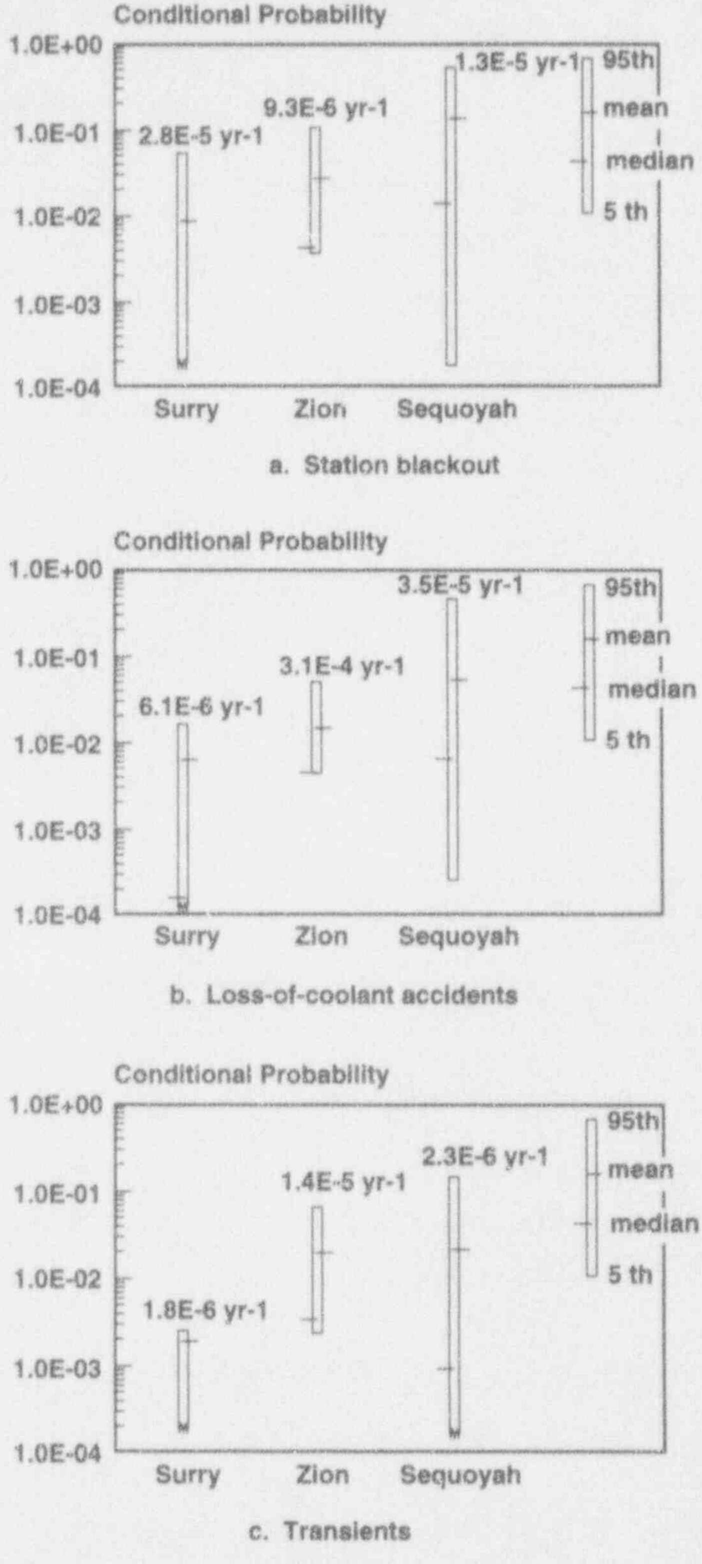


Figure 5.1-7 Conditional probability of early containment failure for key plant damage states (PWRs)

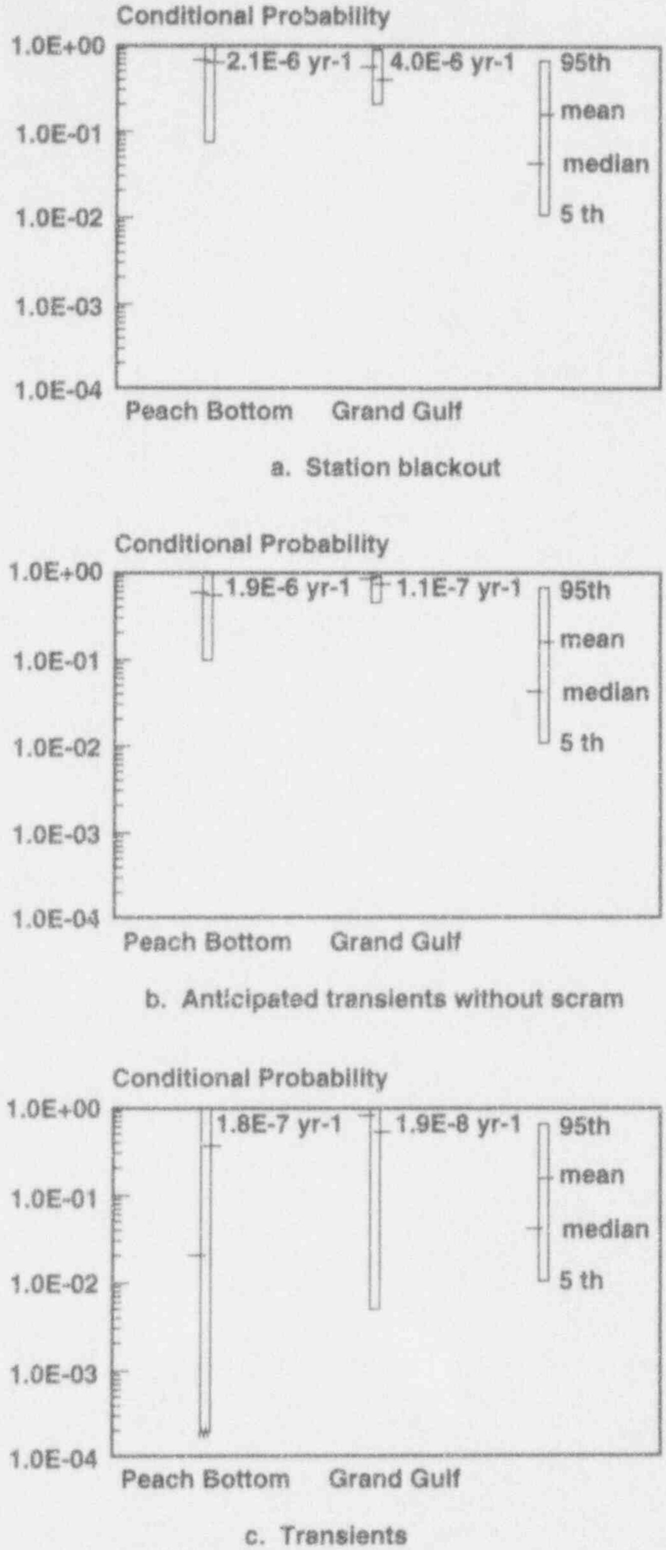


Figure 5.1-8 Conditional probability of early containment failure for key plant damage states (BWRs)

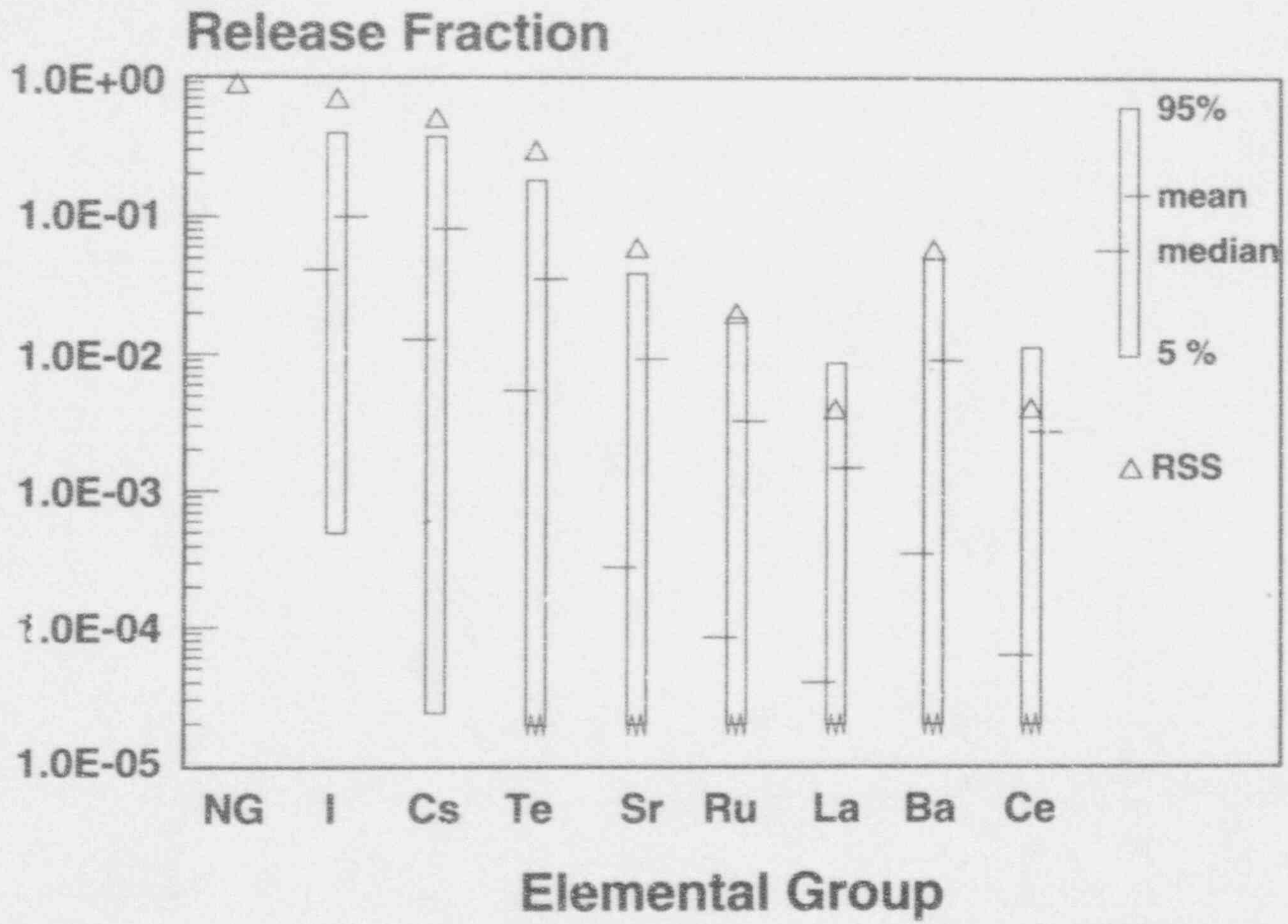


Figure 5.1-9 Comparison of NUREG-1150 source terms with Reactor Safety Study (Surry) bin PWR2

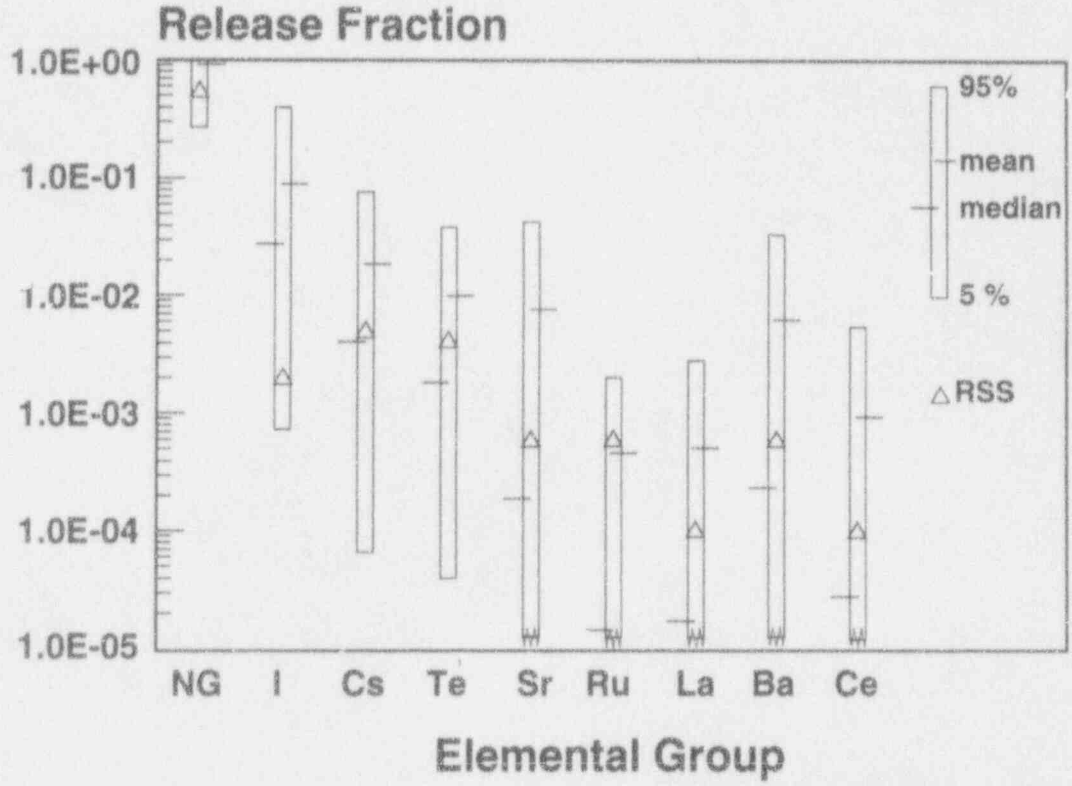


Figure 5.1-10 Comparison of NUREG-1150 source terms with Reactor Safety Study (Peach Bottom) bin BWR4

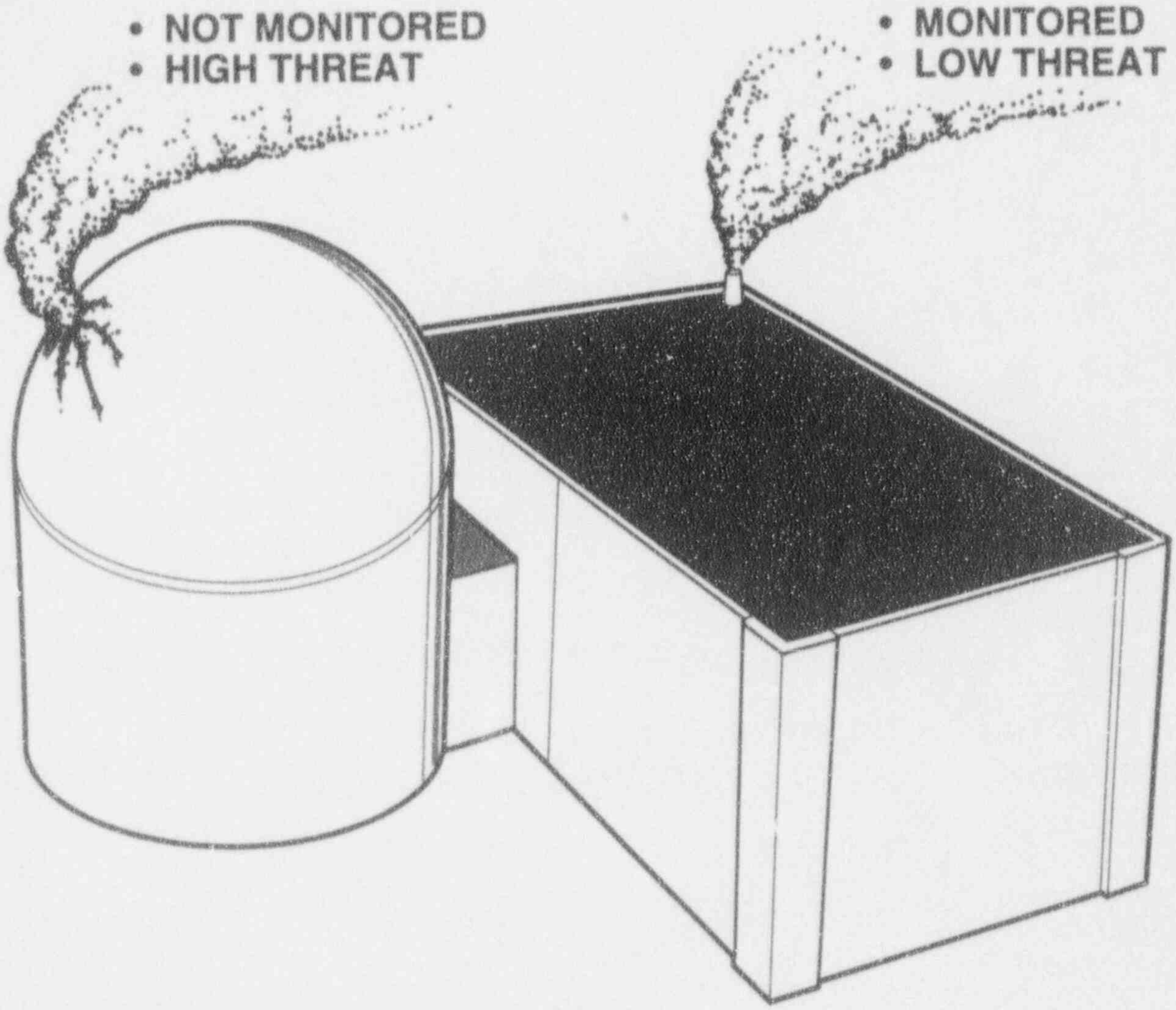


Figure 5.1-11 Types of release

References for Section 5.1

1. D. J. Alpert, et al, *Relative Importance of Individual Elements to Reactor Accident Consequences Assuming Equal Release Fractions*, NUREG/CR-4467, SAND85-2575, March 1986.

2. T. J. McKenna, et al, *Pilot Program: NRC Severe Reactor Accident Incident Response Training Manual, Vol. 2, Severe Reactor Accident Overview*, NUREG-1210, February 1987.

3. S. Abrahamson, M.A. Bender, B.B. Boecker, E.S. Gilbert, B.R. Scott, Inhalation Toxicology Research Institute, Lovelace Biomedical and Environmental Research Institute, *Health Effects Models for Nuclear Power Plant Accident Consequence Analysis, Modifications of Models Resulting from Recent Reports on Health Effects of Ionizing Radiation, Low LET Radiation, Part II Scientific Bases for Health Effects Models*, prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-4214, Rev. 1, Part II Addendum 1, LMF-132, August 1991.

4. U.S. Nuclear Regulatory Commission, *RTM-92 Response Technical Manual*, Vol. 1, Rev. 2, October 1991, pp. S-2 to R-4.

5. S. Abrahamson, et al, *Health Effects Models for Nuclear Power Plant Accident Consequence Analysis, Low LET Radiation, Part II: Scientific Bases for Health Effects Models*, NUREG/CR-4214, SAND85-7185, Rev. 1, Part II, May 1989, Tables 2.7 and 2.8.

6. U.S. Environmental Protection Agency, *Manual of Protective Action Guides and Protective Actions for Nuclear Incidents*, EPA 400-R-92-001, October 1991, p. 1-2.

7. U.S. Nuclear Regulatory Commission, *NUREG-1150, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, Vol. 1, December 1990, p.10-1.

5.2 Consequence Projections

Projecting the consequences of a severe accident involves (1) estimating the source term, (2) predicting the environmental transport of radionuclides, (3) estimating the resulting doses to the public, and (4) assessing the consequences of these doses. This process is depicted in Figure 5.2-1.

In the past, considerable attention has been given to the use of real-time dose projections as the primary basis for initiating offsite protective actions. The broader term consequence projection, which is used as the title of this section, reflects not only an enlightened interest in the spectrum of possible results (exceed protective action guide levels, early health effects, latent health effects, financial costs) but also the inherent limitations associated with the use of real-time dose projections for decision making. Section 5.1 highlights the difficulty of predicting the source term with sufficient accuracy to justify this use of real-time dose projections during a severe accident. In addition, this section explains why, even if one could accurately predict the radioactive material that may be or is being released from a plant during a severe accident, significant uncertainties would still be associated with dose projections to offsite areas. Nevertheless, it will be shown that both precalculated and real-time consequence projections in conjunction with early field monitoring would play a useful role in responding to a severe accident.

5.2.1 Learning Objectives

After completing this section, the student should be able to explain:

1. the general impact of the following factors on the rate of decrease in offsite dose versus distance: wind speed, stability class, radioactive decay, ground deposition, rainfall, wind stagnation;

2. the uncertainties associated with dose assessment, including those between (a) what is predicted and what may actually be measured and (b) different model estimates;

3. why early protective actions for the population at greatest risk (those nearest the plant) should always be recommended for all directions near the plant and not just downwind.

4. the role of dose projection during a severe nuclear power plant accident (i.e., General Emergency) and during lesser events; and

5. the role of field monitoring during a severe nuclear power plant accident.

5.2.2 Meteorology

In the absence of significant heat transfer with the ground or between adjacent layers of air, the temperature in a well-mixed atmosphere decreases linearly with altitude at a rate of about 5.4°F/1000 ft (1°C/100 m). This is called the adiabatic lapse rate (or adiabatic temperature distribution) because it is derived by treating the expansion of air with altitude as an adiabatic expansion.[1] As indicated in Figure 5.2-2, other temperature distributions such as isothermal, superadiabatic and inversions may exist over particular ranges of altitudes. The actual temperature profile at any time is determined by a number of factors including heating and cooling of the earth's surface, the movements of large air masses (highs and lows), the existence of cloud cover, and the presence of large topographical obstacles. For example, on clear days with light winds, superadiabatic conditions may exist in the first few hundreds of meters of the atmosphere due to the heat transferred to the air from the hot surface of the earth. Conversely, on a cloudless night, when the earth radiates energy most easily, the earth's surface may cool down faster than the air immediately above it, and the result is a *radiation inversion*.

The degree to which pollutants are dispersed in the atmosphere depends to a large extent on the atmospheric temperature profile. Consider the case of dispersion in a superadiabatic atmosphere. If a small parcel of polluted air is released at some altitude h and the same temperature T as the atmosphere, as indicated in Figure 5.2-3a, the parcels will remain in equilibrium at that point if not disturbed. Suppose, however, that a fluctuation in the atmosphere moves the parcel upward. The parcel will cool adiabatically as it rises; that is, the temperature of the parcel will follow the adiabatic curve shown by the dashed lines in Figure 5.2-3a. Although the temperature of the parcel decreases as it rises, it becomes increasingly hotter than the surrounding superadiabatic atmosphere. This means the parcel becomes increasingly buoyant, causing it to move more rapidly upward. On the other hand, if the parcel is pushed downward, its temperature will fall more rapidly and it will become increasingly more dense than the surrounding superadiabatic air. This will accelerate the downward motion at the parcel. Clearly, the superadiabatic atmospheric conditions are inherently unstable and are highly favorable for dispersing pollutants.

In contrast, if the parcel is released into an isothermal or inversion profile as indicated in Figure 5.2-3b, a fluctuation upward will make it cooler and hence more dense than the surrounding atmosphere, tending to return the parcel to its original position. Similarly, a downward fluctuation will make the parcel hotter and more buoyant than the surrounding air. This will also tend to return the parcel to its equilibrium point. Atmospheres characterized by isothermal or inversion profiles are therefore said to be stable. This is undesirable for pollutant dispersal.

Frequently, the parcel is hotter than its surroundings when released, and it will initially rise due to its greater buoyancy. Various types of dispersal patterns can be observed depending on the conditions in the surrounding atmosphere as illustrated in Figure 5.2-4. Plumes emitted into an inversion layer (stable atmosphere) disperse horizontally much more rapidly than they disperse vertically (vertical dispersion is inhibited in an inversion layer). Therefore, the plume spreads out horizontally but not vertically, which produces a fan shape when viewed from below (fanning). If a hot plume is emitted into an unstable atmosphere that is capped by an inversion layer, the plume rises to the inversion layer and then spreads rapidly downward, fumigating the ground below (fumigation). Plumes emitted into an uncapped unstable atmosphere tend to breakup because vertical displacements of plume parcels are enhanced (looping). Plumes emitted into a neutral atmosphere (lapse rate equal to the adiabatic lapse rate) are dispersed smoothly both vertically and horizontally, and therefore have a conical profile in the crosswind direction (coning). Plumes emitted into a neutral layer that overlies an inversion layer can spread upward but not downward (lofting).

It is possible to estimate the stability conditions in the lower atmosphere by simply measuring the temperature at two or more heights on a meteorological tower. The slope of the temperature profile can then be compared by dividing the temperature difference ΔT by the difference in height Δz of the measurements. Alternatively, stability can be estimated by monitoring fluctuations (standard deviation σ_θ) in the angle of a wind vane. Based on Pasquill experimental data on atmospheric dispersion, stability regions are often divided into the seven stability classes listed in Table 5.2-1[2] depending on the indicated ranges of $\Delta T/\Delta z$ or σ_θ.

Other meteorological conditions that can have a strong impact on atmospheric dispersion or ground contamination include wind speed, precipitation and humidity. Data on these factors are also measured on the meteorological tower. The significance of such factors is discussed in the following section.

5.2.3 Dispersion of Effluents

Plumes disperse as they are transported downwind, which means that concentrations of released radionuclides would decrease with plume travel distance. Because dispersion causes plume materials (droplets, particles, gas molecules) to move away from the plume centerline by random steps, plume concentrations tend to assume normal (Gaussian) distributions in both the vertical and horizontal directions. The rate of spreading depends on atmospheric stability and is usually different in the vertical and horizontal directions.

Models of atmospheric dispersion range in complexity from simple to sophisticated. Perhaps the simplest model is the straight-line Gaussian plume model. As illustrated in Figure 5.2-5, this model assumes a constant wind direction and a Gaussian shaped spreading of the plume with distance. It also assumes a constant wind speed, and it does not account for the effects of local topography. According to this model, the center of the plume originating from a puff (short duration) release moves downwind at the wind speed u. The plume spreads in all directions due to turbulent diffusion as it moves. This spreading is characterized by empirically determined standard deviations in vertical and cross wind pollutant concentrations. These standard deviations increase with downwind distance and atmospheric instability.

The inhalation and immersion doses that would be received by an individual standing in the path of the plume increase with the magnitude of χ_T, the time-integrated concentration at the point in question. According to the straight-line Gaussian plume model

$$\chi_T \propto Q \frac{\Phi}{u}$$

where

χ_T = time integrated radionuclide concentration at point in question (Ci•s/m^3)

Q = quantity of radionuclide released (Ci)

u = wind speed (m/s)

Φ = Gaussian shape function, which depends on the location, the stability class, and the release height (m^{-2})

Figure 5.2-6 shows the quantity χ_T/Q along the plume centerline for effluent released at a height of 100 ft under Pasquill stability classes B, C, and D for a 6 mile/hr wind. χ_T/Q is also shown for a 2 mile/hr wind speed for stability class D. It will be observed that at reasonable distances from the plant χ_T/Q decreases more or less exponentially. With the more unstable conditions (B), the maximum of χ_T/Q occurs nearer the release point (within a few hundred meters), then drops rapidly to very low values. On the other hand, under more stable conditions (D), the peak of χ_T/Q is located much further from the source. In the dispersion of effluents from nuclear power plants, the concentration of the effluent is therefore usually higher in the more important, populated offsite regions under stable conditions, and stable conditions are often assumed in calculations of such effluent dispersion.

The preceding discussion ignored the effects of radioactive decay and ground deposition on plume concentrations. Radioactive decay and deposition, both wet and dry, are each first order processes (i.e., their rates are proportional to the local concentration). Both processes cause atmospheric concentrations to decrease more rapidly with distance. Ground deposition causes groundshine.

Changes in wind speed and atmospheric stability cause the falloff with distance of plume concentrations to be uneven without causing the preceding generalizations to be seriously violated. However, rainfall and wind stagnation each have the potential to cause concentrations at the distance where these events occur to be higher than nearby upwind concentrations. In particular, rain can have a major impact on accident consequences. Rain decreases plume concentrations, which decreases cloudshine, inhalation, and skin doses, but greatly increases ground concentrations (producing hot spots). Rain can result in very high local ground concentrations distributed in very complex patterns as seen at Chernobyl, Figure 5.2-7.

Wind stagnation causes cloudshine, inhalation, and skin doses at the stagnation distance to increase because the exposure times for these doses all increase. In addition, prolonged stagnation can produce a hot spot on the ground at the stagnation distance because of the greatly increased time period during which deposition occurs at that distance.

5.2.4 Dose Versus Distance

Only a <u>very</u> severe reactor accident involving core damage and containment failure could result in early death or injury. To examine the potential consequences of such a severe accident, dose calculations based on the straight-line Gaussian plume model are presented for the PWR 4 source term from the Reactor Safety Study. The PWR 4 release includes about 60% of the noble gases and 5% to 10% of the iodine and cesium in the reactor core. This source term, is representative of a typical late containment failure case in NUREG-1150.

The PWR 4 example assumes a catastrophic failure of the containment. As a result, a large part of the radioactive material in the containment atmosphere would be released in a short period (a puff release). Such a puff release could expose people near the plant to substantial cloud shine and inhalation doses within an hour or so of the release.

Figure 5.2-8 shows the relative contribution of various pathways to whole-body and thyroid doses as a function of distance for the PWR 4 source term and the indicated meteorological conditions. These meteorological conditions represent an average day for this accident. Doses could be higher or lower depending on the actual weather at the time of the release.[3]

The top right figure shows the contributions to the 24-hr whole body dose. The inhalation pathway would contribute the least to projected whole body dose; the cloud shine dose would be sublethal, but the additional 24-hr ground shine contribution would lead to projected doses in excess of the early injury threshold (50 to 100 rem) out to 7 miles or so and the early fatality threshold (250 rem) out to about 3 miles.

In this example, the early doses (cloud shine and inhalation) are not sufficient to cause early injuries, but they do exceed Environmental Protection Agency protective action guides. Other source terms have been postulated (no matter how unlikely) that could cause early injuries close to the plant resulting from cloud shine and inhalation. This shows the importance of early protective actions. For large source terms like PWR 4 involving a puff release of short duration (a few minutes to an hour), the population close to the plant must take actions before or shortly after the start of the release to avoid a major portion of the dose from the cloud shine and inhalation. Actions taken after the puff's passage are effective only in reducing dose from ground contamination.

Most of the total dose increase between 4 hr and 7 days (shown in the top left part of Figure 5.2-8) results from ground contamination deposited by the passing plume. This shows the importance of ground contamination. In this example, the direct dose from the plume (cloud shine and inhalation) is not sufficient to result in early deaths or injuries; but if people remain on contaminated ground, their dose will increase until, at about 6 hr, the dose could result in injuries and, at 12 hr, cause death. Obviously, after a major release, areas of substantial ground contamination must be identified, and the population must be evacuated.

From the bottom figures, it can be seen that projected thyroid doses are dominated by inhalation doses. The ground and cloud shine contributions increase the thyroid dose only marginally within 24 hr. Thyroid ablation would occur at thyroid doses above about 1000 rem. This would not be expected beyond about 3 miles for the postulated (PWR 4) source term and weather conditions. Whole-body dose (not thyroid dose) would be the most important dose for most accidents in terms of early fatalities and injuries.

The PWR 4 source term is not the worst conceivable source term. Accidents that involve core melt followed by early containment failure would not allow for removal of the nongaseous fission products and could result in a much larger source term with correspondingly larger off site doses. As indicated in previous modules, any accident involving both core melting and early containment failure is very unlikely; however, such accidents would require prompt and effective protective actions to preclude off site health effects. Dose projections for one of the worst source terms postulated (PWR 1 from the Reactor Safety Study) are presented to illustrate the efficacy of evacuation and sheltering protective actions in Section 5.4.

In virtually all cases, the greatest effluent concentrations occur within the first 2 to 3 miles. Therefore, independent of the size of the release, the greatest need for protective actions most likely will be within 2 to 3 miles of the plant. For large releases, these actions will be to prevent early deaths and, for lesser releases, to keep doses below Environmental Protection Agency protective action guides.

Another point to be made from Figure 5.2-8 involves the plume exposure emergency planning zone (EPZ). Many think that the public risk stops at the boundary of the emergency planning zone. But, it is clear that this accident would result in doses in excess of the Environmental Protection Agency's protective action guides (whole body (5 rem) and thyroid (25 rem)) doses. At these levels, evacuation would be appropriate beyond the plume emergency planning zone.

This module discusses mainly those actions that must be taken early in an accident to protect the population at greatest risk. Ingestion dose is not considered a major contribution to early health effects. For the ingestion pathway, the early protection actions are designed to minimize subsequent contamination of milk or other foods (e.g., remove cows from pasture and put them on stored foods). In this sense, the ingestion pathways can be of concern at considerable distances from the release point (e.g., 50 miles or more). The specific actions and criteria for vegetables are addressed by the Food and Drug Administration protective action guides.

5.2.5 Uncertainties in Dose Projections

In a 1981 study conducted at the Idaho National Engineering Laboratory, a nonradioactive tracer (SF_6) was released and the resulting air concentrations were compared with predictions made by various models to evaluate their potential use in emergency response situations. Figure 5.2-9 shows the actual air concentration (plume) pattern observed for one of the tests and the plume pattern predicted by three of the models tested under this program: (a) a simple, straight-line Gaussian plume model of the type used by many emergency response organizations, (b) a Gaussian-puff trajectory model, which accounts for wind shift, and (c) a more sophisticated wind field and topographic model used in the DOE's Atmospheric Release Advisory Capability (ARAC) program. Even the most complicated ARAC model could not reproduce what actually occurred.

This result points out two concerns. First, typically, only one local meteorological tower is in the site vicinity. The initial transport of radioactive material from a site after it is released to the atmosphere will be dominated by local conditions (e.g., hills, valleys, lakes, and precipitation). This single source of weather and wind information cannot give a definitive indication of winds away from the plant. Nuclear power plants are typically located in very complex areas (e.g., in river valleys or on the coast) where wind direction and flows can vary considerably within a short distance of the plant. As an example, a 180° difference in wind direction could result from sea breeze effects at a coastal site. This is the basis for taking protective actions in all directions near (within 2 or 3 miles of the plant). The events that occurred early in the TMI-2 incident, as discussed in Section 5.2.6, further illustrate the problems inherent in taking protective actions only in the downwind direction.

Second, differences should be expected in the estimates produced by various analysts. Various response organizations may be performing analyses based on different assumptions. For example, the NRC may be concentrating on dose projections based on possible additional plant failures, while the state is making dose projections based on estimates of actual releases. As Figure 5.2-9 indicates, even if the same input conditions (e.g., source terms and meteorology) are used, dose estimates may differ.

For lesser accidents (non-core damage) where the total release is through a monitored pathway and consists mostly of noble gases, the source term uncertainty can be reduced. However, the transport and dose uncertainties would remain. Overall, the best that should be expected in the early time frame is that projected dose estimates may be within a factor of 10 of the true dose value; more likely, they will be even less accurate.[4] Unanticipated catastrophic containment failure is an example of a case where source term could be underestimated by a factor of 100,000.

It is clear that one should not expect close agreement when comparing various dose projections with each other or with early field monitoring data. Dose projections should be viewed only as rough estimates.

What may be more important than relying on a dose model in estimating plume movement is a knowledge of local meteorological conditions and trends (e.g., the winds shift every morning at about 9:00 a.m.).

The basic point here is that the analyst needs to understand the problem, the models, and the results. Indiscriminate use of technical aids such as dose projection models without access to staff who understand the unpredictability of local conditions can provide misleading input to protective action decision making.

5.2.6 Early Protective Action Decisions During the TMI-2 Accident

To highlight some of the points discussed in this section, certain aspects of the assessments of the TMI-2 accident merit discussion. Figure 5.2-10 presents the hourly wind vector as measured by the site meteorological system during the first day of the accident. Actually, these measurements were not available to the NRC until three days later because the plant computer crashed early in the accident. It is evident that wind direction at the site varied dramatically throughout the 12-hr period.

A Site Emergency was declared at 6:56 a.m., followed by a General Emergency at 7:23 a.m. Between 7:30 and 8:00 a.m., the State of Pennsylvania did issue warnings of imminent evacuation to the west of the site. At 8:10 a.m., this preparedness was reduced to a standby notice because dose rate measurements to the west were "only" about 30 millirem/hr (i.e., about 10,000 times higher than the dose rate resulting from normal effluent releases.) This reduction-to-standby notice came while the core was still uncovered.

If an evacuation to the west of the site had been initiated around 8:00 a.m., the wrong people would have been told to evacuate, local wind conditions would have shifted the potentially affected area to the north by 9:00 a.m., and then to the east by 11:00 a.m. As the NRC Special Inquiry Group noted later, based on in-plant observations as set forth in the emergency plans and as emphasized in NRC emergency planning guidance in place even at the time (R.G. 1.101), omnidirectional evacuation of the total low-population zone (2.5-mile-radius area surrounding the site) would have been warranted no later than 7:30 a.m.

By 9:00 a.m., indications of severe core damage were indisputable. Some of the core thermocouples showed temperatures over 2000°F (800°F beyond that required for cladding failures, and the containment dome monitor increased from 600 to 6000 R/hr between 8:20 and 9:00 a.m. However, as indicated, the decision not to take action was made based on field-monitoring results. The NRC Special Inquiry Group found that the state offices should have been advised at 9:00 a.m. that "*the core has been badly damaged and has released a substantial amount of radioactivity. <u>The plant is in a condition not previously analyzed for cooling system performance</u>.*" The Inquiry Group went on to state, "*The difficult question in this situation is whether to advise precautionary evacuation of the nearby population or to advise only an alert for possible evacuation. The recommendation to evacuate is consistent with what we think would then be the case, a prudent doubt that the core-cooling passages were still sufficient for cooldown. <u>In addition, the containment building was now filling with intensely radioactive gas and vapors, leaving the nearby public protected by only one remaining barrier, the containment</u>, a barrier with a known leak rate that needed only internal pressure to drive the leakage.*" Finally, the Inquiry Group stated, "*Present emergency plans are inadequate because they do not provide a clear requirement to evaluate the need for protective actions based on deterioration of plant conditions.*"

This example illustrates the importance (for core melt accidents) of implementing protective actions in the nearby areas as soon as core damage is detected and without regard for wind direction or detection of actual major releases. These are two of the foundations of current NRC staff emergency planning guidance. Early precautionary evacuation of the immediate area (approximately 2-mile radius) should <u>not</u> be recommended in only "downwind" directions because of the inability to determine where downwind will be when the protective actions are actually implemented or when a significant release occurs. In addition, when core damage is detected, the early recommendation to evacuate should not be based on early real-time dose projections but on the status of the core. Indeed, the predetermined, early, initial evacuation for a severe core damage accident is called "precautionary" because a major release may never actually occur, as was the case at TMI-2. On the other hand, no immediate, early evacuation would be warranted for sequences less serious than core-melt accidents.

5.2.7 The Role of Consequence Assessment During Severe Accidents

The role of consequence projection during a nuclear power plant accident will depend on the type and phase of the accident. Precalculated doses provide useful information regarding potential offsite health effects (the event tree presented as Figure 5.1-5 in Section 5.1 is a very simple example). In the early emergency response phase, dose projections for protective action decision making should be secondary to assessment of plant conditions and general weather at the time.

Consequence projections during the initial phase of a severe core damage accident provide a basis to establish priorities for the use of limited resources in the implementation of offsite actions such as deployment of field-monitoring teams. In an actual uncontrolled release of radioactive material to the environment, it would be imperative to obtain offsite monitoring team data as quickly as possible. However, for a core-melt sequence, early protective actions in nearby areas (2 to 3 miles) should not await such results. In particular, the evacuation of nearby areas for a severe core damage accident should be initiated on the basis of plant conditions.

After implementation of protective actions near the plant (based on an assessment of plant conditions), potential consequences should be assessed to determine whether these actions should be extended. The assessments may indicate the maximum distance from the plant where further actions are required. However, because of the difficulty of projecting plume movement, actions should not be limited to just the downwind areas. Actions should be taken in all directions or at least in all areas considered to be the possible limits of the plume under various conditions (e.g., inside a valley).

Bounding calculations may be very useful in comparing the consequences of various plant response options (e.g., venting the containment versus allowing later containment failure).

After early protective actions have been implemented for the population near the plant, the roles of consequence assessment differ significantly from those discussed earlier. The first role is to assess the areas that may warrant implementation of protective actions according to radiation protection objectives. The second role of consequence assessment under these conditions is to provide feedback regarding the magnitude and composition of a release based on the analysis of offsite samples and field monitoring results.

5.2.8 Role of Field Monitoring

Environmental monitoring would be the best way to characterize a release after it occurs. However, one must be sensitive enough to the differences between actual plume behavior and that simulated by models. Consequence projection models project the <u>average</u> dose as the result of plume meander over a 15- to 30-min period. Therefore, as indicated in Figure 5.2-5 and 5.2-7, a monitoring team within the actual plume may observe <u>greater</u> doses than projected or, if the team is out of the plume (point A), <u>lower</u> doses than projected. Even if the model projections are "correct," actual field-monitoring results could differ considerably from projections because the projections show averages. One would not expect the first preliminary field monitoring results to agree with model projections, even under the best circumstances.

Actual field monitoring can be used to determine the actual dose rates and projected offsite consequences as the result of an accident. The role of field monitoring during the early phases of a severe accident would be to identify areas that may require further protective actions following a release. Reliance should be on field monitoring as soon as possible.

Because the actual location of the plume or resulting ground contamination may not be known for some time, early, limited field-monitoring results should be used with great care. Even if the monitoring team is in the path of the release, the plume could meander or loop around the team. It will be difficult to obtain readings that are considered representative of the release.

The biggest problem with field monitoring, as shown in Figures 5.2-5 and 5.2-9d is that the actual distribution of offsite dose could be very complex. The dose rate could change over very short distances (hundreds of feet). "Hot spots" could be surrounded by areas of lower dose rates. Therefore, an aircraft or large numbers of monitor teams would be needed to fully characterize a major release in a short time.

The teams should have instruments designed to monitor all radioactive material (iodine, cesium, strontium, and tellurium) that may be released during an accident. If air samples are taken, their analysis could take several hours. Monitoring teams typically will be dispatched into the emergency planning zone (EPZ) within an hour after initiation of a severe release.

5.2.9 Major Points

The major points covered in this section are summarized as follows:

- It is not wise to await a major release to the atmosphere (i.e., a major containment failure) before making protective action recommendations to the public.
- Early in a severe core-melt accident, it would be difficult, if not impossible, to make a confident projection of offsite doses.
- Protective actions near the site (2 to 3 miles), if warranted at all, should be implemented in all directions, not just in the downwind direction.
- Dose projections and actual field measurements will differ considerably, even if the dose projection model is doing a good job.
- Results of various dose models may be considerably different, even if each model is using the same inputs.
- For the initial stages of a severe core damage accident, offsite dose projection has a secondary role, independent of initiating protective actions near the plant.
- Field-monitoring results would be the most accurate indicator of offsite radiological impacts and their extent, but early field-monitoring results should be used with caution.

Table 5.2-1
Relationship between Pasquill category and $\Delta T/\Delta z$ and σ_θ*

Pasquill category	$\Delta T/\Delta z$ (°C/100 m)	σ_θ (degrees)
A - Extremely unstable	$\Delta T/\Delta z \leq -1.9$	$\sigma_\theta \geq 22.5$
B - Moderately unstable	$-1.9 < \Delta T/\Delta z \leq -1.7$	$22.5 > \sigma_\theta \geq 17.5$
C - Slightly unstable	$-1.7 < \Delta T/\Delta z \leq -1.5$	$17.5 > \sigma_\theta \geq 12.5$
D - neutral	$-1.5 < \Delta T/\Delta z \leq -0.5$	$12.5 > \sigma_\theta \geq 7.5$
E - Slightly stable	$-0.5 < \Delta T/\Delta z \leq 1.5$	$7.5 > \sigma_\theta \geq 3.8$
F - Moderately stable	$1.5 < \Delta T/\Delta z \leq 4.0$	$3.8 > \sigma_\theta \geq 2.1$
G - Extremely stable	$4.0 < \Delta T/\Delta z$	$2.1 > \sigma_\theta$

*From Regulatory Guide 1.23, U.S. Nuclear Regulatory Commission, 1980.

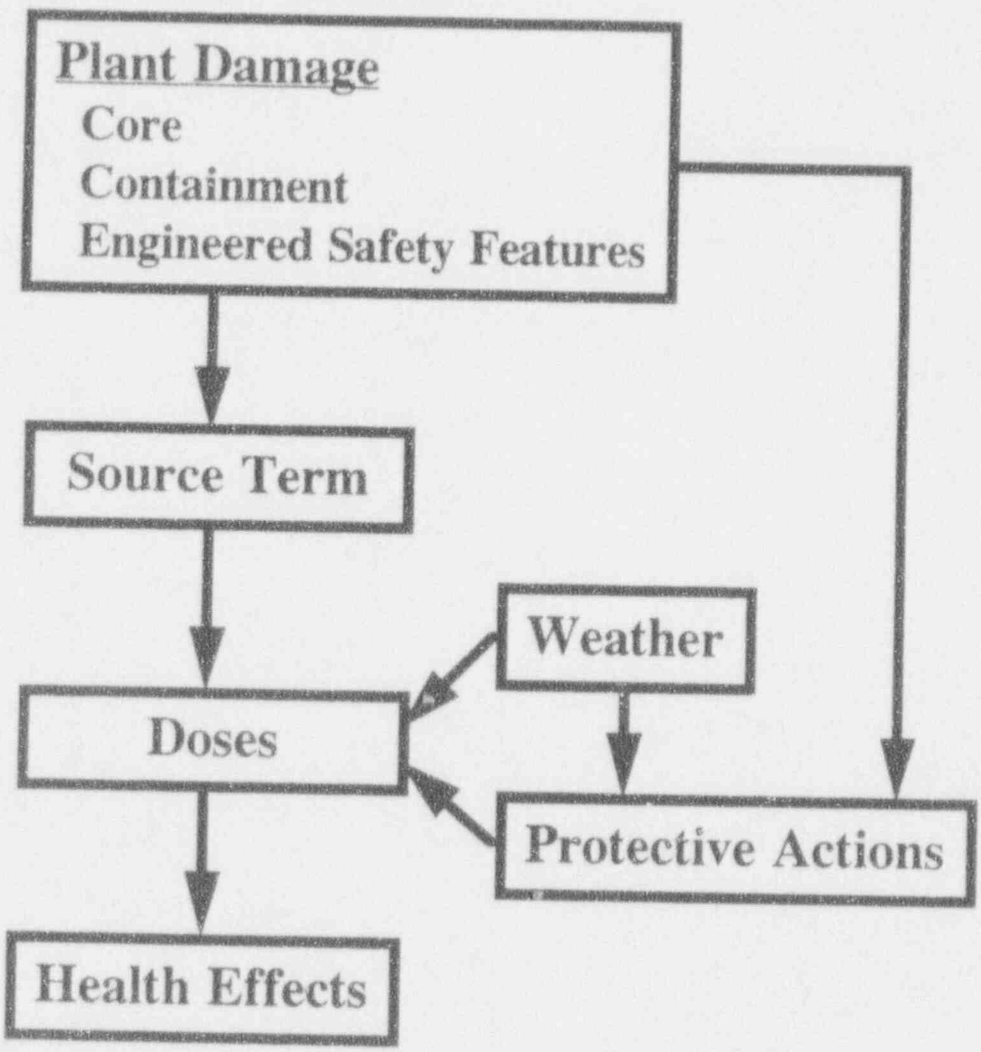


Figure 5.2-1 Steps in projecting offsite consequences

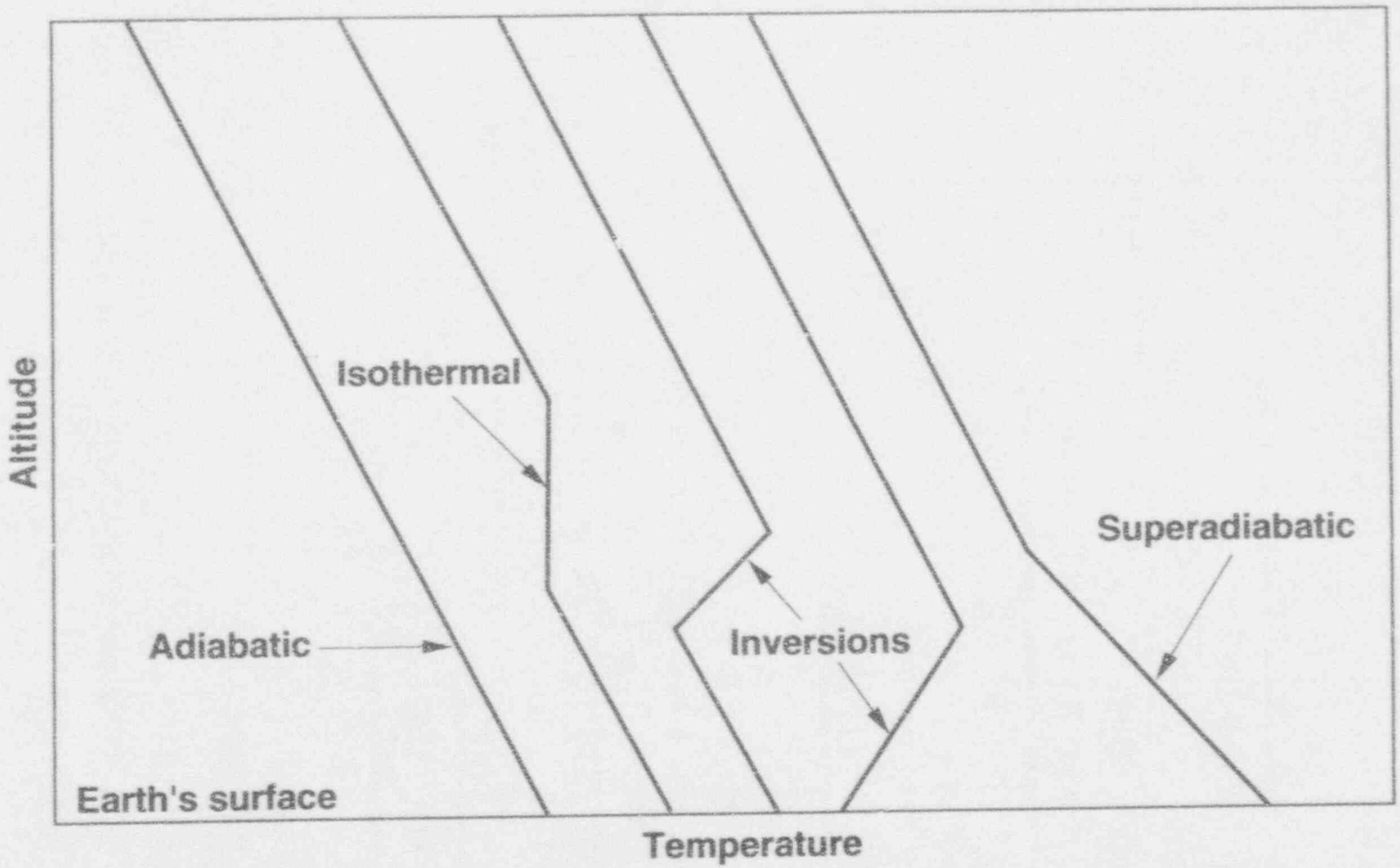


Figure 5.2-2 Examples of low-level temperature distribution in the atmosphere

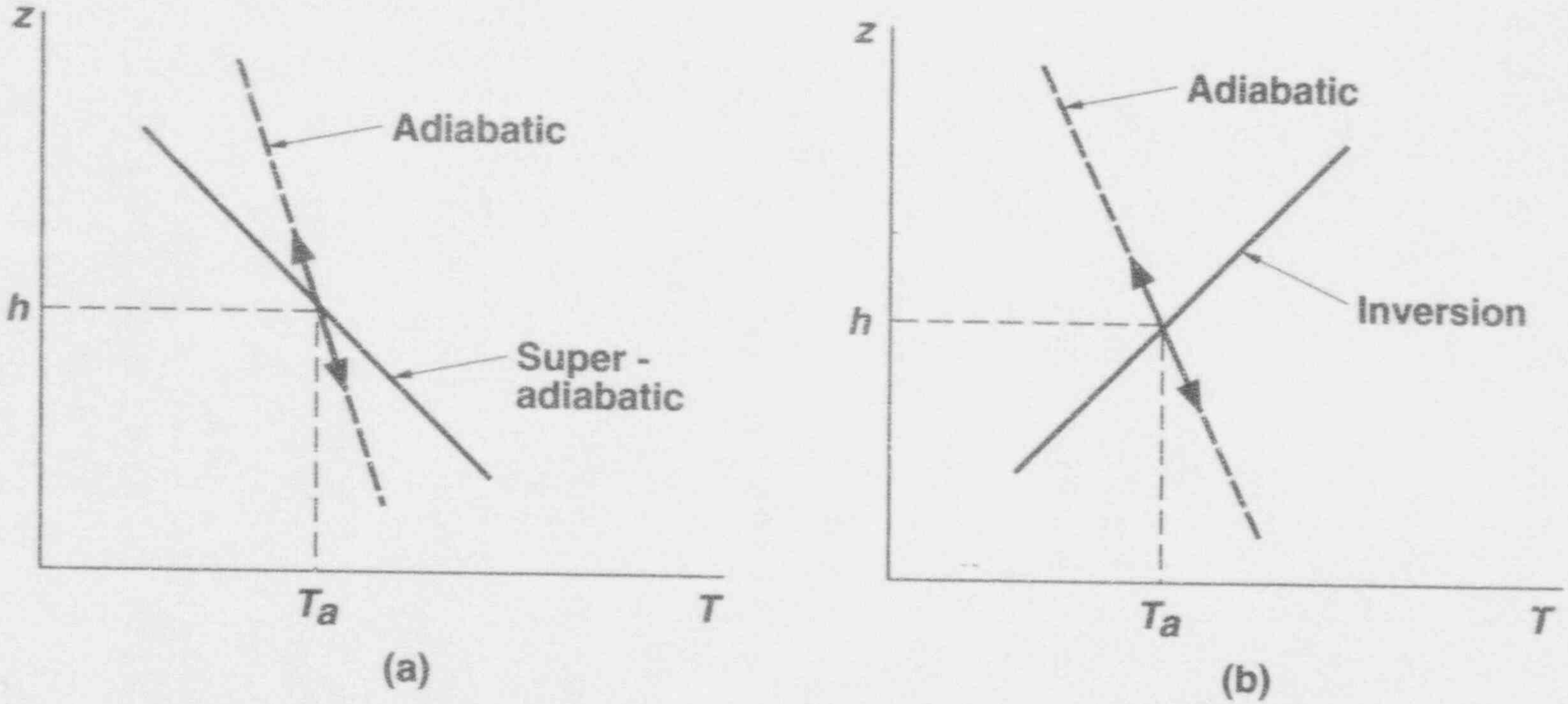


Figure 5.2-3 Movement of a parcel of air in (a) a superadiabatic profile and (b) an inversion profile

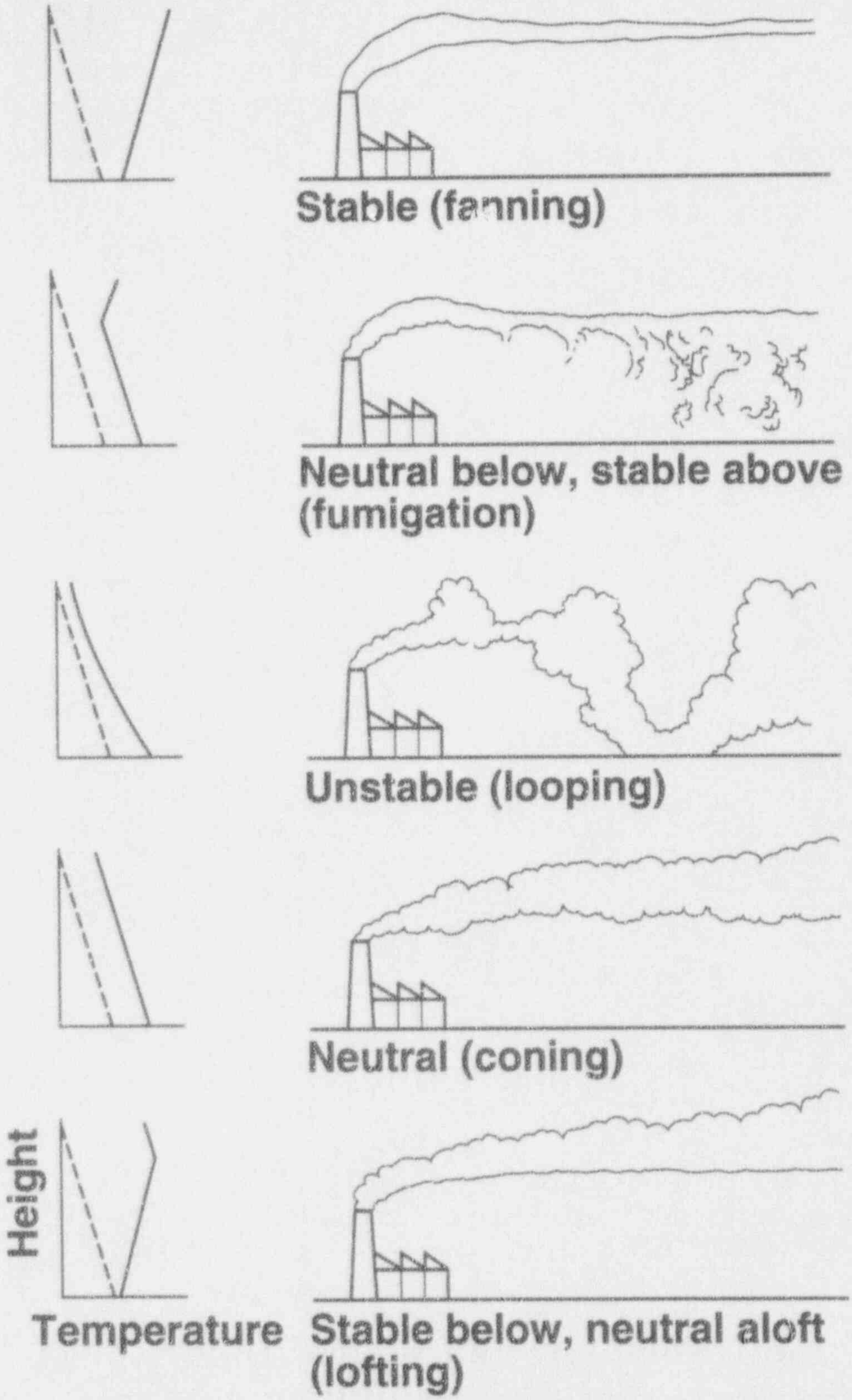


Figure 5.2-4 Various types of smoke plume patterns

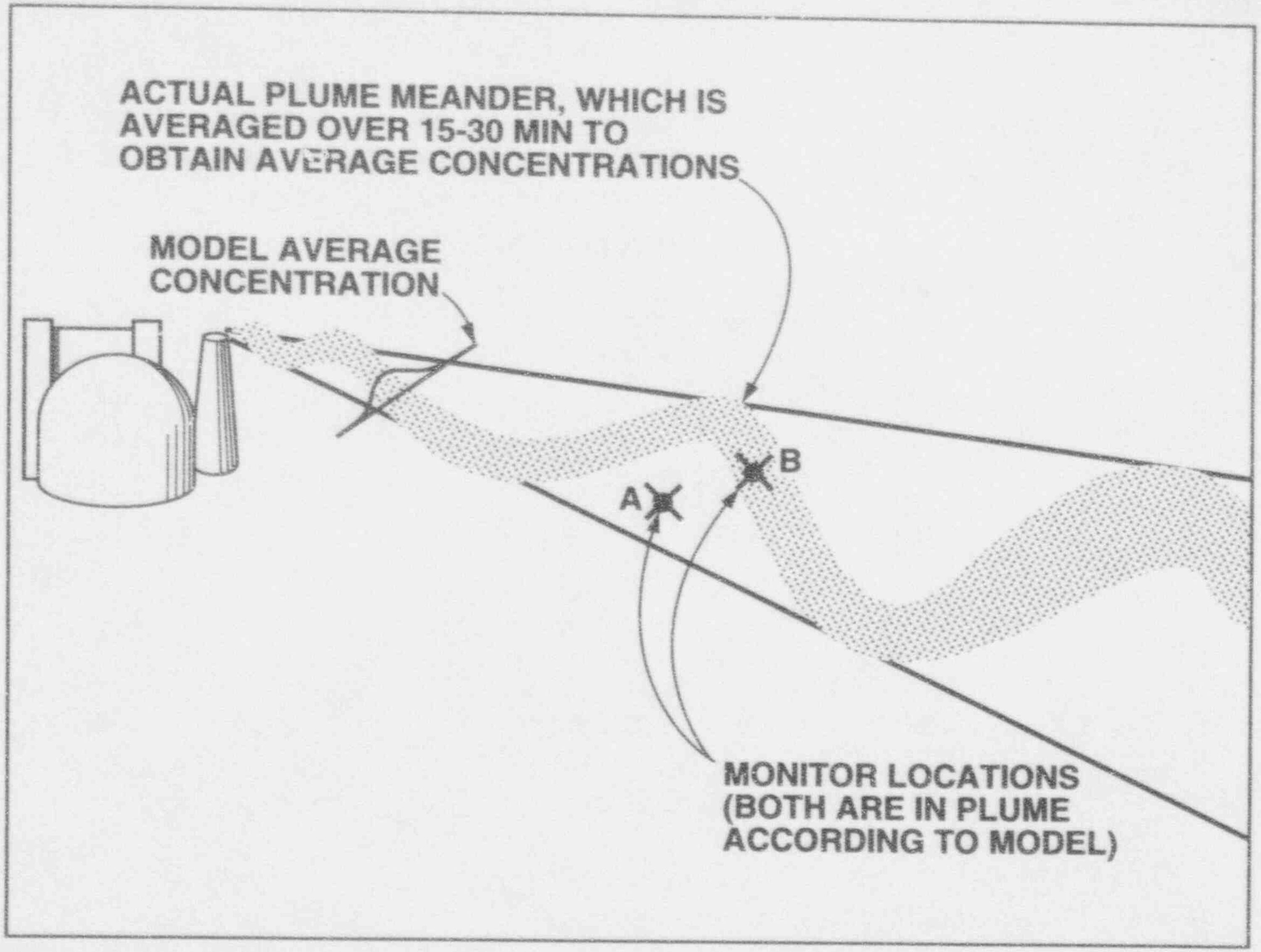


Figure 5.2-5 Relationship between actual plume and model projections

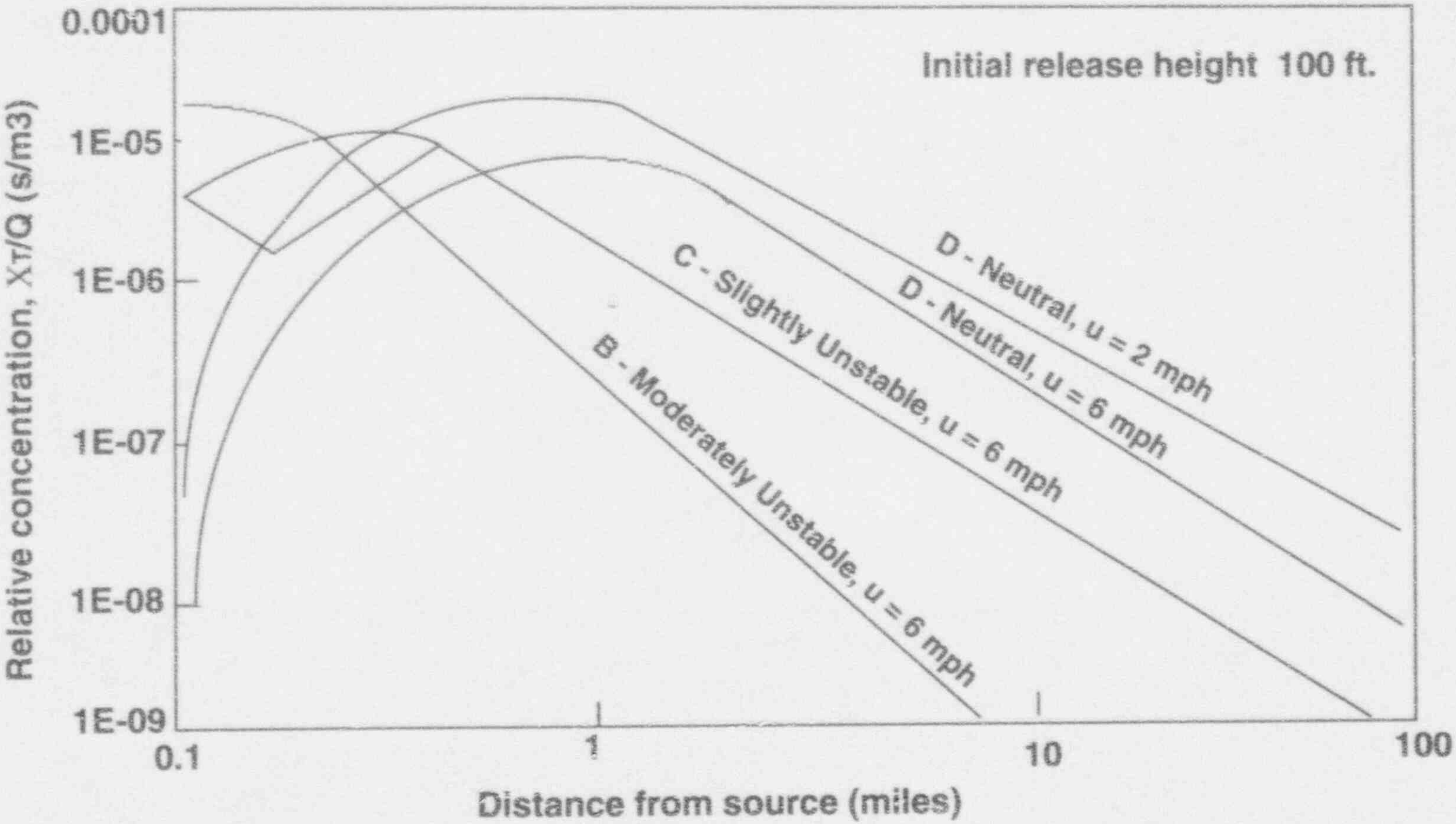


Figure 5.2-6 The quantity Xт/Q at ground level, for effluents emitted at a height of 30 m, as a function of distance from the source

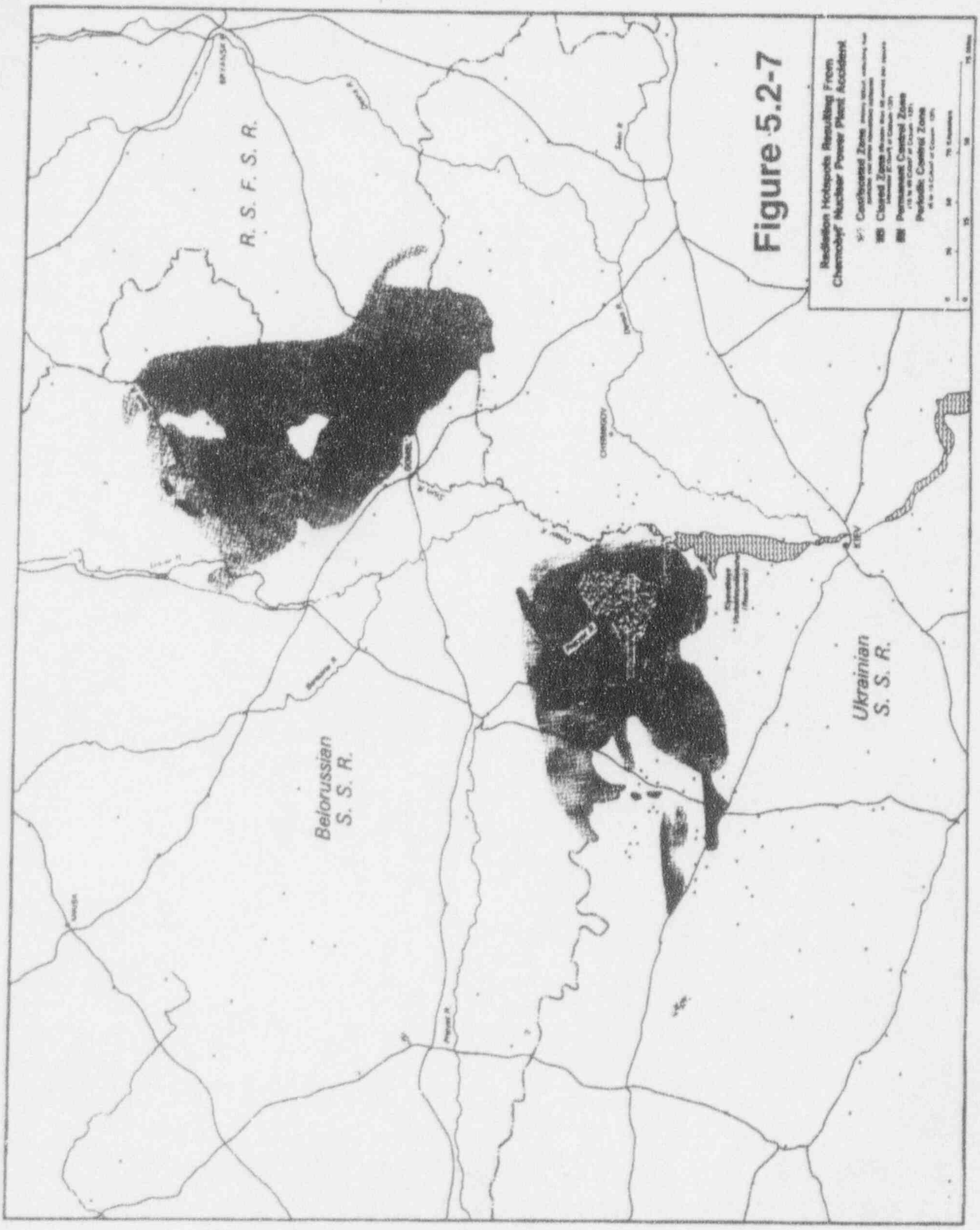

R. S. F. S. R.
Belorussian S. S. R.
Ukrainian S. S. R.
Radiation Hotspots Resulting From Chernobyl' Nuclear Power Plant Accident
Confiscated Zone
Closed Zone
Permanent Control Zone
Periodic Control Zone

Figure 5.2-7

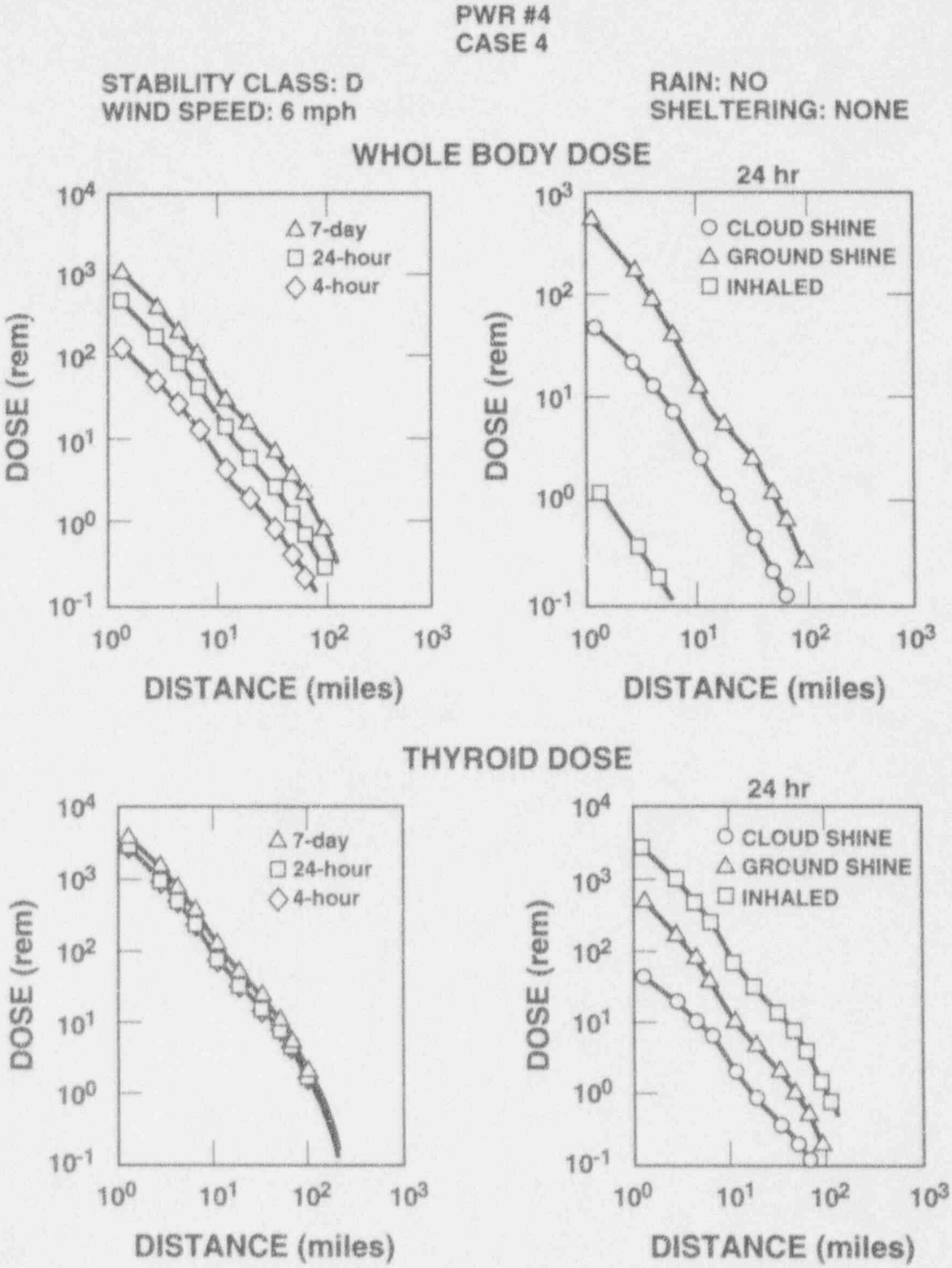


Figure 5.2-8 Example from NUREG-1062, dose calculations for severe LWR accident scenarios

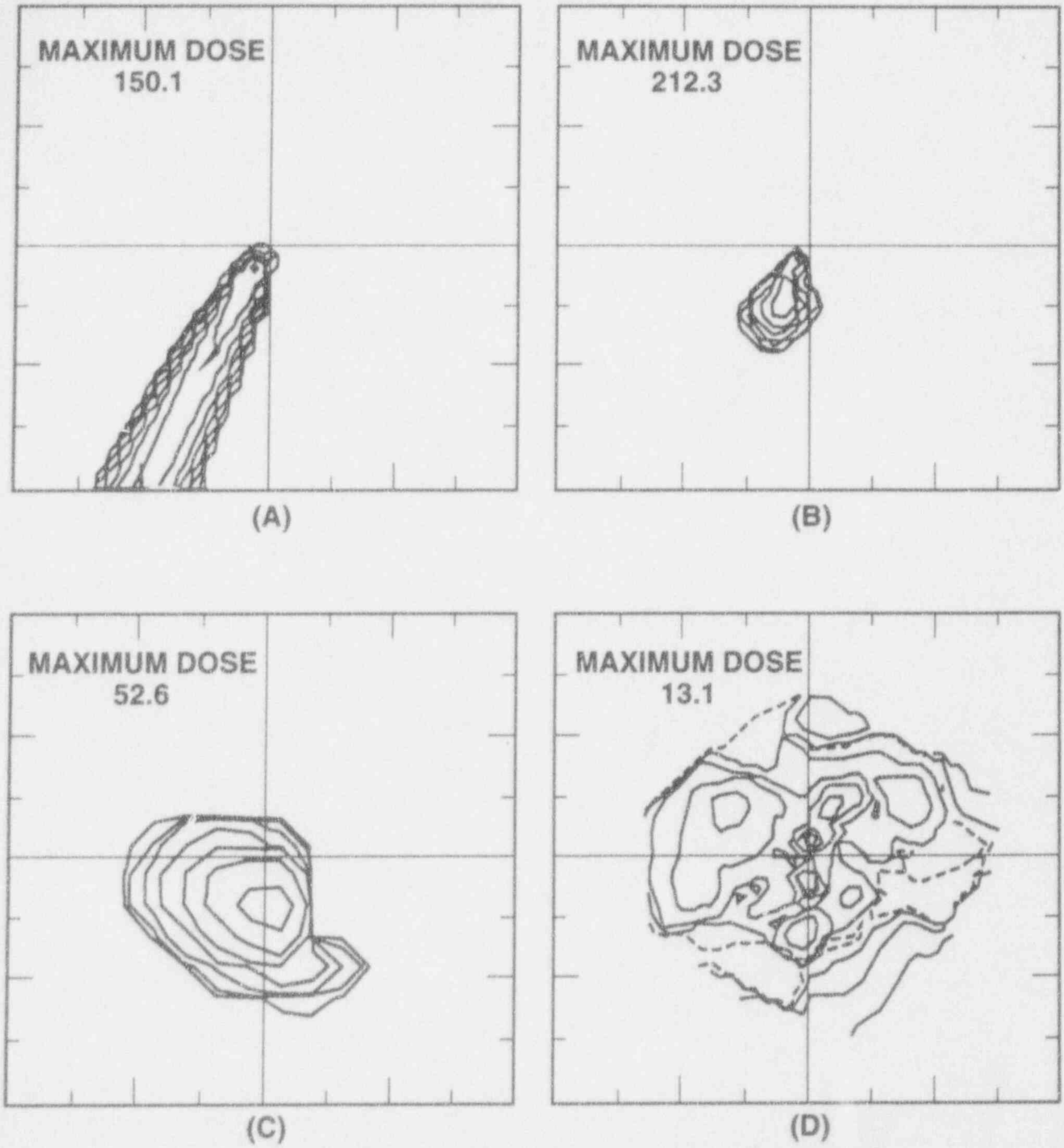
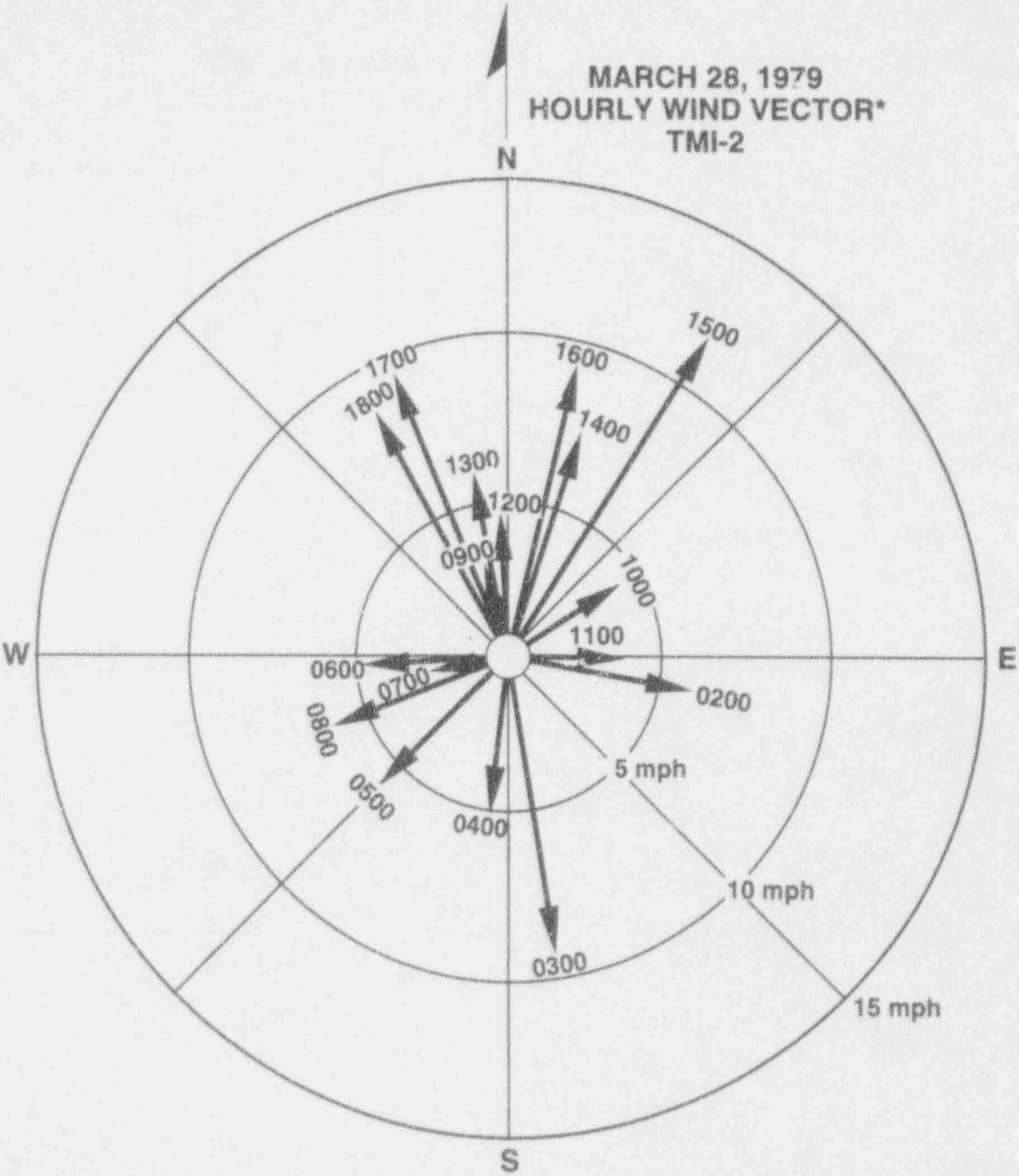


Figure 5.2-9 One-hour surface doses predicted by (A) Gaussian plume model, (B) puff-trajectory model, (C) complex numerical model, and (D) doses actually observed



*Arrows indicate direction toward which the on-site wind was blowing at the local time indicated. Circles represent varying wind speeds.

Figure 5.2-10 Hourly wind vector at Three Mile Island on March 28, 1979

References for Section 5.2

1. D. H. Slade, Editor, *Meteorology and Atomic Energy--1968.* Washington, DC: U.S. Atomic Energy Commission, 1968.

2. U.S. Nuclear Regulatory Commission Regulatory Guide 1.23, 1980.

3. T. S. Margulies and J. A. Martin, Jr., *Dose Calculations for Severe LWR Accidents*, NUREG-1062, U.S. Nuclear Regulatory Commission, Division of Risk Analysis and Operations, Office of Nuclear Regulatory Research, Washington D.C., May 1984.

4. J. A. Martin, et al, *Pilot Program: NRC Severe Reactor Accident Incident Response Training Manual, Public Protective Actions -- Predetermined Criteria and Initial Actions,* NUREG-1210, Volume 4, 1987.

5.3 Emergency Preparedness

Preparations for potential nuclear power plant emergencies are extensive. The discussion in this section is limited to those aspects of preparedness that affect the NRC's role of monitoring protective actions. This includes organizational responsibilities, emergency detection and classification, Emergency Planning Zones, licensee response centers, and the response of state and local organizations.

5.3.1 Learning Objectives

Following completion of this section, the student should be able to:

- indicate the primary responsibilities of the licensee, state and local agencies, and the NRC during a nuclear power plant emergency;
- explain what the plume exposure Emergency Planning Zone is;
- explain what the ingestion pathway Emergency Planning Zone is;
- explain what Emergency Action Levels (EALs) are;
- list the four classes of emergencies in order of increasing severity and indicate which require official notification and which require off-site protective actions;
- describe the functions of the Technical Support Center (TSC) and the Emergency Operations Facility (EOF) during a nuclear power plant emergency;
- describe the role and shortcomings of evacuation time estimates;

5.3.2 Regulatory Basis

Licensees have developed plans and procedures for emergency response in accordance with the requirements and guidelines presented in the following documents:

1. Title 10, Code of Federal Regulations (CFR) Pt. 50.47 and Appendix E, which contain the basic requirements for emergency preparedness;
2. NUREG-0654 [Regulatory Guide (R.G.) 1.101, rev. 2],[1] which contains the criteria to be used in developing and assessing an emergency plan;
3. NUREG-0396,[2] NUREG-1131,[3] and Information Notice 83-28,[4] which discuss the foundation for the current emergency preparedness concepts;
4. NUREG-0737, Supplement 1,[5] which clarifies the requirements for the emergency organization and emergency centers; and
5. NUREG-1210 and RTM-92,[6,7] which update the guidance in NUREG-0654 and IN 83-28 based on results of severe accident research and experience gained in emergency preparedness exercises.

The licensee emergency plans and procedures are available at U.S. Nuclear Regulatory Commission (NRC) Headquarters (HQ) and at the regional offices for each operating reactor.

5.3.3 Roles in an Emergency

5.3.3.1 Role of Licensee

In the event of an emergency, the primary responsibilities of the licensee are to protect the core, to prevent or limit off-site consequences, and to notify predesignated state and local officials promptly (within 15 minutes) of the emergency declaration.

The licensee's first priority is to protect the core by maintaining the following critical safety functions:

1. making the core subcritical and keeping it there,

2. keeping the water flowing through the core,

3. keeping the core covered with water,

4. providing makeup for water boiled off, and

5. removing decay heat from the core to an outside heat sink.

The licensee must also take action to prevent or limit off-site consequences by

1. maintaining reactor containment and the Engineered Safety Feature (ESF) systems,

2. controlling radionuclide releases, and

3. recommending appropriate protective actions to off-site officials.

Licensees have developed Emergency Operating Procedures for use by the control room staff in responding to emergency conditions. These Emergency Operating Procedures are discussed in Section 5.3.4.1.

In parallel with attempts to correct the problem, the licensee must notify off-site officials of emergency declaration promptly (within 15 min). The licensee recommends initial protective actions to off-site officials because the licensee is the only one who would have a true and an early understanding of core and containment conditions. Furthermore, if an actual off-site radionuclide release occurs, the licensee is responsible for monitoring that release to ensure that actions recommended off site are appropriate (i.e., that initial protective action recommendations/decisions continue to be valid based on current, actual monitoring data). Section 5.4 discusses role and efficacy of specific protective action concepts.

5.3.3.2 Role of State and Local Agencies

State and local agencies are charged with protecting the public from the off-site consequences that might result from a power plant accident. These organizations have the ultimate responsibility for notifying the public to take protective actions in the event of a severe accident. State and local officials base their decisions on the recommendations of the licensee. The licensee cannot order an evacuation of areas surrounding the plant; the licensee can only make such a recommendation to the appropriate off-site officials. Those officials must make the decision to notify the public to implement any protective actions. The response of state and local organizations is discussed in Section 5.3.7.

5.3.3.3 Role of the NRC

The NRC role is one of monitoring the licensee's actions and providing assistance to the licensee. It is important that the NRC response personnel understand that extensive preplanning has been completed to assist in early decision making. When prompt protective action is dictated by plant conditions in a serious accident, it is not appropriate for the licensee or the responsible state or local agency to seek NRC concurrence prior to initiating the action. The NRC should intervene only if there is a serious lack of appropriate action.

5.3.4 Emergency Detection and Classification

5.3.4.1 Emergency Operating Procedures

Prior to the accident at Three Mile Island, plant emergency operating procedures were "event-oriented." They described the steps which the operator should take given the occurrence of certain preselected, pre-analyzed events. These procedures were typically limited to transient events or loss-of-coolant events followed by successful operation of all safety systems designed to respond to these events.

Since the Three Mile Island accident, considerable effort has been devoted to the development of "symptom-based" procedures to replace (or at least significantly augment) the event-specific procedures. The basic premise underlying these symptom-based procedures is that there is a limited set of critical safety functions (CSFs), which, if successfully performed by either automatic plant response or manual action, result in a "safe" condition for the plant. The basic goal of the plant safety systems and the ultimate goal of operator actions is to ensure the performance of these critical safety functions. Symptom-based operating procedures relate critical safety function performance to specific plant/control room instruments.

The attractiveness of the "critical safety functions" concept evolves from the implication that the operator need only monitor a relatively few pieces of information to ascertain the safety of the plant. While there are a limited number of critical functions (or parameters) which indicate the performance of these functions, there are virtually an unlimited number of events (with a wide variety of symptoms) that can affect the performance of these functions. The operator can carry out his duties by focusing on these critical functions without regard to the specific events that have occurred.

It is important to note that, in general, the Emergency Operating Procedures address actions that lead up to core damage but do not include actions to be taken after core damage. Therefore, the operators may not have procedures to help them once the core has been damaged. However, as a result of shortcomings identified in the Three Mile Island accident, licensees have installed additional instrumentation to detect inadequate core cooling, developed core condition assessment procedures, and conducted training on core condition assessment. These assessments are based on the relationship of various plant instruments (e.g., containment monitor, water level, or thermocouple readings). These relationships must be used with caution, but they do provide gross indicators of the extent of core damage.

5.3.4.2 Emergency Action Levels

Licensees have established Emergency Action Levels based on control room instrument readings (e.g., 1000 R/hr containment monitor reading or 2000°F thermocouple) that indicate the scope of an emergency. NRC guidance requires that Emergency Action Levels be established for a full range of events from situations that indicate just a potential problem to actual core damage (General Emergency).

Emergency Action Levels are extremely important. They are trigger levels for the declaration of emergencies and the initiation of predetermined activities that lead to immediate, early actions (e.g., activation of organization, notifications, and protective actions).

Each licensee's emergency action plan contains a list of Emergency Action Levels which are used by the operators in assessing the level of response needed. Most licensees have established their Emergency Action Levels for each of the 60 example initiating conditions provided in NUREG-0654. In many cases, this results in a very long list of diagnostic control room parameters, as can be seen from the sample shown in Table 5.3-1. Some licensees have streamlined this approach by using flow charts and other visual aids. A newer symptomatic EAL classification scheme has been developed by NUMARC and is being adopted by some licensees. In the NUMARC methodology, generic recognition categories replace individual analyses of multiple NUREG-0654 initiating conditions.

Table 5.3-2 shows several examples of the timing of some boiling water reactor (BWR) core damage accidents; these examples illustrate that core damage could occur within a few minutes or many hours. These are only examples to show what might be typical of the timing during an event and to demonstrate how the ability to take early action based on the exceeding of Emergency Action Levels could provide sufficient time to implement protective actions.

5.3.4.3 Emergency Classification System

Four classes of emergencies (Unusual Event, Alert, Site Area Emergency, and General Emergency) have been established by NRC regulations. The class of emergency that is declared is based on conditions that trigger the Emergency Action Levels (EALs). Typically, licensees have established for each emergency class specific Emergency Plan Implementation Procedures (EPIPs) that are to be implemented by the control room staff. The importance of correct classification cannot be overly emphasized. The event classification initiates all appropriate actions for that class. Both over- and under-reaction could have serious adverse consequences. The classification procedures (i.e., Emergency Action Levels) for specific nuclear power plants are included in the emergency plans, which are located in the Region Incident Response Centers (IRCs) and the Headquarters Operations Center.

Each class requires specific initial actions. The classes and the appropriate initial actions are discussed in more detail in the following subsections.

5.3.4.3.1 Unusual Event

The rationale for establishing notification of an "Unusual Event" as an emergency class is to provide early and prompt notification of minor events that could possibly lead to more serious conditions. The purpose of off-site notification is to

1. ensure that the first step in any response later found to be necessary has been carried out.

2. bring the operating staff to a state of readiness.

3. provide systematic handling of unusual events information and decision making, and

4. control rumors.

5.3.4.3.2 Alert

Events are in progress or have occurred that involve an actual or potentially substantial degradation of the level of safety at the plant. Any radiological releases are expected to be limited so that resulting exposures would be small fractions of the U.S. Environmental Protection Agency (EPA) Protective Action Guides.

The purpose of an alert is to

1. ensure that the on-site Technical Support Center is activated so that licensee emergency personnel are readily available to respond,

2. provide off-site authorities with information on the current status of the event, and

3. provide assistance to the control room staff.

5.3.4.3.3 Site Area Emergency

Events are in progress or have occurred that involve actual or likely major failures of plant functions needed for protection of the public. Radiological releases, if any, are not expected to result in doses exceeding Environmental Protection Agency Protective Action Guide levels, except possibly near the site boundary.

The purpose of the Site Area Emergency declaration is to

1. ensure that all emergency response centers are manned,

2. ensure that radiological monitoring teams are dispatched,

3. ensure that personnel required to aid in the evacuation of near-site areas are at duty stations should the situation become more serious,

4. provide consultation with off-site authorities,

5. provide updates for the public through off-site authorities, and

6. ensure that nonessential personnel are evacuated.

5.3.4.3.4 General Emergency

Events are in progress or have occurred that involve actual or imminent substantial core degradation or melting. Risks of exceeding Environmental Protection Agency Protection Action Guide exposure levels in more than the immediate area are considerably elevated. This is a very special case. A General Emergency indicates that plant conditions are well beyond design and early protective actions are warranted.

The purpose of the General Emergency declaration is to

1. initiate predetermined protective action notification to the public and

2. bring the full available resources of government and industry to bear on the situation.

5.3.4.3.5 Class Summaries and NUMARC Recognition Categories

Summary descriptions of the four emergency classes are provided in Table 5.3-3. A summary of emergency classification actions for the three major classes is presented in Table 5.3-4. The number of emergencies typically reported to the NRC in a year is 200 unusual events, 10 alerts, and 1 or 2 site area emergencies. No general emergencies have been declared since TMI-2.

Table 5.3-5 displays the relationship between the four emergency classes and the NUMARC recognition classes. By matching the observed plant condition with the recognition category descriptions on the left, the applicable emergency class can be determined. If the recognition category is "Fission Product Barriers Failure or Challenge," plant specific measurable values indicating loss or potential loss of the cladding, reactor coolant system, and containment barriers are developed by the licensee.

5.3.4.4 Protective Action Recommendations

As discussed earlier, within 15 min of identifying a situation requiring urgent action (General Emergency), the licensee must recommend protective actions to off-site officials. For situations requiring urgent actions, recommended protective actions should have been predetermined based on discussions between the licensee and off-site officials considering plant and local conditions. The implementation and efficacy of specific public protective action recommendations during severe accidents are discussed in Section 5.4. It is important to note that applications of protective actions are site-specific. For example, one plan may call for initial evacuation out to 5 miles, while another calls for initial evacuation out to 3 miles, but the basic concept of prompt evacuation of the area near the plant for a severe core damage accident is met.

No predetermined actions are established for site area and lesser events. The specific actions for these lesser events would be based on projected plant conditions, off-site projections, and monitoring conducted at the time.

5.3.5 Emergency Response Centers

5.3.5.1 Control Room

Authority to take action in the event of an emergency must reside in the plant control room until the Technical Support Center (see 5.3.5.2) or the Emergency Operations Facility (see 5.3.5.4) is activated. This includes the authority to declare emergencies, to notify offsite officials within 15 minutes of general emergency declaration, and to provide any appropriate protective action recommendations. The NRC must be notified after the appropriate state and local officials are notified and no later than 1 hr after declaring the emergency.

Upon declaration of an emergency, most sites designate an on-site Emergency Director, who is in charge of the plant's total response. During night and week-end hours, this typically is the Shift Supervisor. Once the appropriate augmentation staff arrive following declaration of an emergency, this responsibility (and title) normally transfers to the Technical Support Center and then to the Emergency Operations Facility.

5.3.5.2 Technical Support Center

There were indications from the events at Three Mile Island that numerous personnel in the control room acted to congest and confuse the reactor operators' control room activities. Review of this accident also shows that there existed a lack of reliable technical data and other records on which to base accident recovery decisions. As a result, today licensees are required to establish Technical Support Centers whose staff have access to plant technical information and who are responsible for engineering support of reactor operations during an accident. Personnel in the Technical Support Center must be able both to assist the control room when needed and to diagnose and mitigate an event. Until the Emergency Operations Facility is activated, the Technical Support Center will also perform the functions of the Emergency Operations Facility. The Technical Support Center is located close to the control room inside a protected and shielded area to allow fast access for face-to-face discussions with control room personnel.

5.3.5.3 Operations Support Center

The establishment of an Operations Support Center (OSC) was introduced to help relieve the influx of shift/operational support personnel in the control room. The function of the Operations Support Center is to provide a place to which shift personnel report to receive further instructions from the operations staff. The Operations Support Center can be a locker room with capability for reliable communications with supervisory and decision-making personnel.

5.3.5.4 Emergency Operations Facility

Personnel with primary responsibility for the licensee's communications with the outside world during a severe accident are located in the Emergency Operations Facility once it is activated. The Emergency Operations Facility is an off-site facility, which is usually near the site with hardening/shielding or a backup facility if necessary. Figure 5.3-2 depicts the relative locations of the licensee emergency response centers.

The Emergency Operations Facility is generally where protective action recommendations would be formulated and where the Emergency Director would be located. Space is also be provided for state and local agencies. The Emergency Operations Facility enables effective coordination of onsite actions with those off site, and provides a central location from which to direct all offsite actions by the licensee (e.g., monitoring, sampling, and dose assessment).

5.3.5.5 Flow of Authority and Responsibility

The responsibility and authority for licensee actions during a severe nuclear power plant accident start in the control room and then flow out as people arrive to man the Technical Support Center and the Emergency Operations Facility. The licensee will typically start transferring functions/responsibilities/authorities out of the control room as soon as possible so that control room personnel can concentrate on bringing the situation under control. To staff the Technical Support Center would typically require about 30 minutes. About one hour would be required to staff the Emergency Operations Facility. NRC staff initially attempting to contact licensee personnel must be aware of how long the accident has been under way to determine where their contacts should be made. The Emergency Network System (ENS) and Health Physics Network (HPN) lines can be used to determine where the appropriate licensee representative is located.

5.3.6 Emergency Planning Zones

Plume and ingestion Emergency Planning Zones have been established around each nuclear reactor plant site. These Emergency Planning Zones were established so that the public can be notified to implement appropriate protective actions in an efficient and a timely manner in the event of a real emergency.

5.3.6.1 Plume Exposure EPZ

The plume exposure Emergency Planning Zone is that area requiring possible immediate action to reduce risk to the public in the event of an accident. It is an area approximately 10 miles in radius around the power plant. This size is based primarily on the following considerations.

- Projected doses from the traditional design basis accidents would not exceed Environmental Protection Agency Protective Action Guide (PAG) levels outside the zone.

- Projected doses from most core melt sequences would not exceed Protective Action Guide upper levels outside the zone.

- For the worst-case core-melt sequences, immediate life-threatening doses would generally not occur outside the zone. (For most hypothesized severe accidents, life-threatening doses are not predicted beyond 2 to 3 miles from the plant.)

- Detailed planning within 10 miles provides a substantial base for expansion of response efforts in the event that this proves necessary.

It is unlikely that any immediate protective actions would be required beyond the plume exposure pathway Emergency Planning Zone. The zone is sufficiently large that protective actions within it provide for substantial reduction in early health effects (injuries or deaths) in the event of a worst-case core melt accident.

The boundaries of the plume Emergency Planning Zone take into account local features such as roads, rivers, lakes, peninsula, etc. that may extend the zone beyond 10 miles. The boundaries are selected to assure the existence of adequate evacuation routes as illustrated in Figures 5.3-3 and 5.3-4.

Extensive provisions are made for action within the emergency planning zone. These include

1. provisions for prompt decision making on protective actions for the public by all responsible parties;

2. development of evacuation plans;

3. provisions for informing the public of emergency plans and procedures (i.e., a public education program);

4. provisions for promptly (within 15 min of the time that state and local officials are notified) alerting and informing the public of the actions to be taken (e.g., siren system and radio messages);

5. provisions for maintaining 24-hr communication between the licensee and state and local officials;

6. provisions for radiological monitoring in the event of an off-site radioactivity release; and

7. provisions for activating and maintaining emergency operations centers.

5.3.6.2 Ingestion Pathway EPZ

The ingestion pathway Emergency Planning Zone is the area in which plans exist for protecting the public from the consumption of food contaminated with radioactive material and for which there is considerable time (hours to days) for action to reduce risks. Thus, the level of preparation is much less in this Emergency Planning Zone than it is in the plume exposure pathway Emergency Planning Zone. Also, the preparations that are made for this Emergency Planning Zone are typically effected at the state level rather than at the local level.

In this Emergency Planning Zone, the concern is for the interdiction of foodstuffs rather than the avoidance of exposure to the plume itself. Protective actions within this zone would generally include the restriction of grazing animals to stored feed and restrictions on crop consumption and water usage. The area of this Emergency Planning Zone generally encompasses a 50-mile radius around the plant site. The size of the ingestion exposure Emergency Planning Zone (about 50 miles in radius, which also includes the 10-mile radius plume exposure Emergency Planning Zone) was selected for the following reasons:

- The downwind range within which contamination will generally not exceed the Protective Action Guides is limited to about 50 miles from a power plant because of wind shifts during the release and travel periods.

- There may be conversion of atmospheric iodine (i.e., iodine suspended in the atmosphere for long time periods) to chemical forms that do not readily enter the ingestion pathway.

- Much of any particulate material in a radioactive plume would be deposited on the ground within about 50 miles of the facility.

- The likelihood of exceeding ingestion pathway Protective Action Guide levels at 50 miles is comparable to the likelihood of exceeding plume exposure pathway Protective Action Guide levels at 10 miles.

Except for the most severe accidents, immediate action is not critical for food and agricultural produce because of the additional time involved when compared to the time frame associated with the plume exposure Emergency Planning Zone. Preplanned actions for the immersion pathway Emergency Planning Zone ordinarily will be implemented by local agencies at the direction of state agencies.

5.3.7 Response of State and Local Organizations

5.3.7.1 Emergency Response Plans

States and local agencies have formulated written emergency response plans in response to U.S. Nuclear Regulatory Commission (NRC) and Federal Emergency Management Agency (FEMA) requirements. These documents (1) describe the procedures that state and local officials will follow in the event of a nuclear power plant emergency and (2) list the responsibilities of each state and local agency involved. In most states, the decision to notify the public to implement protective actions is made by local not state authorities.

5.3.7.2 Public Notification

The licensee must notify off-site state and local organizations responsible for implementing protective actions within 15 min of the declaration of an emergency. This permits off-site officials to make prompt protective action decisions, to provide an alerting signal (e.g., a siren), and to follow the signal by a message via the local radio station as to what actions the public should take. State and local officials have predetermined the criteria that they will use to make protective action decisions. These criteria should have been coordinated with the recommendations made to local agencies by the licensee.

In most cases, the specific protective action criteria for severe core damage accidents have been developed after consideration of plant and local conditions. For example, the areas planned to be evacuated may be confined to a valley around the site, or the specific evacuation sector boundaries may be determined by local roads. This delineation is done so that the local population can understand the evacuation instructions.

As discussed in sections 5.2.6 and 5.4.3, current NRC guidance calls for prompt off-site protective actions on detection of actual or imminent core damage (before dose assessment). Earlier guidance caused many state and local agencies to rely primarily on projected dose assessments. The currently envisioned role for dose assessment during an emergency is discussed in Section 5.2.7.

A flow chart showing the typical steps from detection of an event in the power plant control room (CR) to notification of the public is shown in Figure 5.3-5. Note that the off-site officials generally make decisions based on licensee recommendations, which are, in turn, based on criteria discussed and agreed to in advance. However, only off-site authorities know what off-site conditions actually exist at the time the event is occurring (e.g., ice storm, blocked highway, bridge out, etc.) that might alter implementation of the licensee's recommendation.

5.3.7.3 Evacuation Time Estimates

Licensees are required to develop evacuation time estimates for the plume-exposure Emergency Planning Zone (10-mile radius). These estimates are based on various models and must be used with caution. These models have not been validated against evacuations and are subject to large uncertainties.

Often, the evacuation time estimates are dominated by assumptions of how long it will take to notify people and for them to get ready to leave. Sometimes it is assumed that it will take an hour or more for pre-evacuation preparation. Actual experience has shown, however, that, if people are told and motivated to "go now," most will follow instructions, and most will evacuate very fast. Except for special cases where there is a large population near the site (e.g., Zion and Indian Point) or where there is some special population (e.g., hospital patients), the area near the site should be able to be evacuated in 1 hr or less. Because of the NRC's siting criteria, there is a limited population (<300 people) within 2 miles of most sites. In these cases, the capacity of the local roads will be great enough so as not to delay an evacuation.

5.3.7.4 Dose Projections and Field Monitoring

Dose projection models used by off-site officials are generally similar to those used by the licensee and have the same limitations as other dose models. The only source of release estimates (source term) is from the licensee. Therefore, while off-site officials can confirm (check) licensee transport calculations, they must rely on the licensee's release (source term) estimates. Because of the complex processes involved in a core melt scenario, the source term (release) estimate would be highly uncertain early in an event. The degree of off-site monitoring capabilities varies markedly from excellent to marginal, depending on the state's emphasis on developing an independent capability. In some situations, off-site officials rely on the licensee or the responding federal agencies (e.g., U.S. Department of Energy, Environmental Protection Agency, and NRC) for monitoring information.

5.3.7.5 Location of Authority and Responsibility

During the initial phase of the event, the specific location of the local off-site officials with the authority and responsibility to take action varies. The communications system between the licensee and off-site officials should accommodate this need. This is very site-and/or state-specific. In some cases, there are duty officers and 24-hr manned centers, and in others there are local police stations. Once the local emergency organization has been activated, it will establish a local Operations Center. It should be noted that at some sites there are several (2 to 20) local governments within the plume Emergency Planning Zone and that each might have a center.

At the state level, there are typically two levels of activity of interest: (1) an organization that is responsible for conducting technical assessments (e.g., dose assessment) of the situation and (2) decision makers (e.g. governor). These functions may be performed at two separate locations (centers). The NRC must coordinate its contact with off-site officials to avoid considerable confusion resulting from carrying out discussions with both groups. The licensee or state emergency plans should be consulted to determine the specific emergency organization's locations.

5.3.8 Major Points

The major points covered in this section are summarized as follows.

- In the event of an emergency, the primary responsibilities of the licensee are to maintain critical safety functions, to notify off-site officials, and, when appropriate, to recommend off-site protective actions.
- State and local agencies are responsible for protecting the public from off-site consequences that might result from a power plant accident. These agencies are responsible for notifying the public to take protective actions.
- During a nuclear power plant emergency, the role of the NRC is to monitor the licensee's actions and to provide assistance to the licensee. The NRC should intervene only if there is a serious lack of appropriate action.
- The plume exposure Emergency Planning Zone is an area approximately 10 miles in radius around a nuclear power plant for which extensive preplanning of actions to protect the public is conducted. The actual shape and area of the Emergency Planning Zone are site specific.
- The four classes of emergency in order of increasing severity are unusual events, alerts, site emergencies, and general emergencies. All require the licensee to notify designated state and local agencies.
- A general emergency indicates actual or imminent core damage with the potential for causing off-site doses substantially in excess of protective action guide levels.
- When a severe core damage accident is detected or projected, the licensee should recommend and state/local agencies should implement predetermined off-site protective actions.
- Licensees have established Emergency Action Levels, which are sets of observable control room instrument readings that indicate the scope of plant damage, in particular, the adequacy of core cooling or the extent of core damage.
- The Technical Support Center is a protected area near the control room that is staffed during an emergency with licensee personnel who provide engineering support of reactor operations.
- The Emergency Operations Facility is an off-site facility, which houses the licensee's Emergency Director, enables effective coordination of on-site and off-site actions, and provides a central location from which to direct all off-site actions by the licensee (e.g., monitoring, sampling, and dose assessment).
- The licensee authority and responsibility for taking actions on site (e.g., notifying and making recommendations to off-site officials) will initially be in the control room, but as other personnel arrive,

authority and responsibility for certain actions will move to the Technical Support Center (accident assessment) and Emergency Operations Facility (dose projection and off-site coordination).

- Evacuation time estimates should be used with great caution. Often they apply to the full Emergency Planning Zone rather than to the nearby low-population zone.

Table 5.3-1 Sample initiating condition and examples of accompanying Emergency Action Levels (EALs)

Initiating condition No. 1	Emergency Action Levels
Known loss of coolant accident (LOCA) greater than makeup pump capacity	Low reactor water level (-134 in.) on level/pressure recorder 1B21-R623B panel 1H12-P601
	or
	High drywell pressure (+1.8 lb) on pressure indicators CM010 and/or CM021, panel 1PM06J **with** Water level below (and failure to return to) top of active fuel as indicated on fuel zone level indicator 1B21-R6210, panel 1H13-P601 (-150in. +50 in. range with "0" corresponding to top of active fuel), following a time delay of 3 min

Table 5.3-2. Example of timing for BWR general emergency sequences

	Timing of event (hr)			
	TW[a]	TQUV[b]	AE[c]	S_2J[d]
Unusual event	0.017			
Alert	0.33			0.17
Site Area Emergency	1			0.5
General Emergency (protective actions recommended)	1 to 3	0.17	0.17	3+
Core damage	18	1	0.17	29
Containment failure[e]				
Leak	16	3	0.25	
Major	21	5	3	20

[a]Reactor shutdown followed by loss of decay heat removal.
[b]Reactor shutdown followed by loss of ability to provide coolant water.
[c]Large loss of coolant and failure of system to replace water.
[d]Small loss of coolant and loss of long - term heat removal.
[e]Assuming isolation.

Table 5.3-3. Emergency class descriptions

Class[a]	Core status	Radiation
Unusual Event	No threat to irradiated fuel	No release above technical specification (or annual limits)
Alert	Actual (or potential for) substantial degradation of safety	Release is small fraction of EPA PAGs beyond the site boundary
Site Area Emergency	Major failures of functions needed for public protection	Release is less than EPA PAGs beyond the site boundary
General Emergency	Actual or imminent core degradation	Dose may exceed EPA PAGs

[a]Classifications are based on plant instrument levels (i.e., Emergency Action Levels).

Table 5.3-4. Emergency class response

Class[a]	Plant action	Local and state agency action
Unusual event	Provide notification	Be aware
Alert	Mobilize plant resources; Man centers (help for control room)	Stand by[a]
	Activate Technical Support Center (TSC)	
Site Area Emergency	Full mobilization; Nonessential site personnel evacuate	Mobilize; Man emergency centers and dispatch Monitoring Team
	Activate TSC, Operations Support Center, and Emergency Operations Facility	Inform public-activate warning system
	Dispatch Monitoring Team	Take protective actions in accordance with PAGs or on an *ad hoc* basis
	Provide dose assessments	
General Emergency	Full mobilization; Recommend predetermined protective actions (within 15 min) after declaring emergency	Recommend predetermined protective actions to the public based on plant conditions
		Precautionary evacuation (2 to 5 miles)

[a]The NRC will typically begin staffing its response centers at the Alert level and may be expected to go to "standby" or "initial activation."

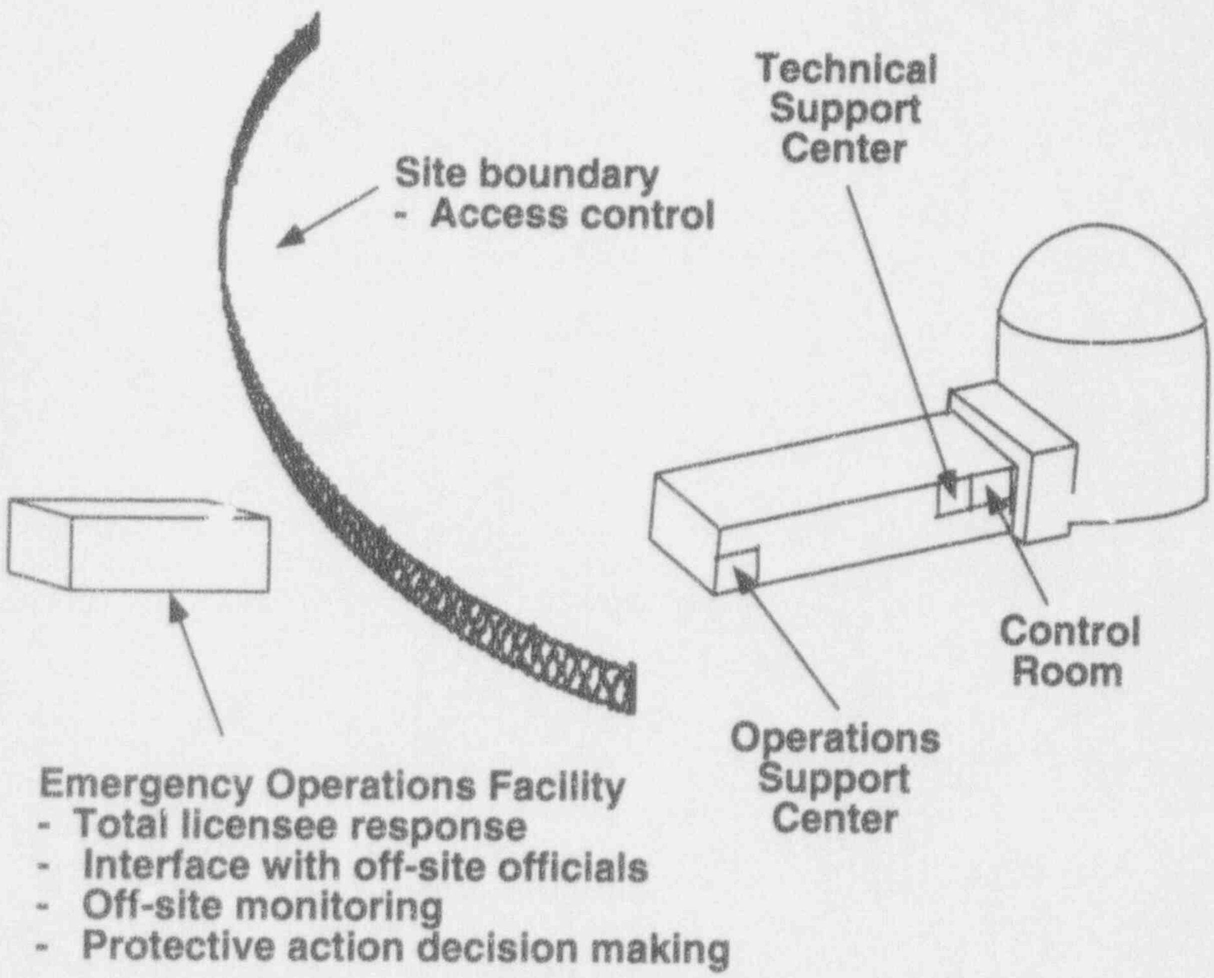


Figure 5.3-1 Relative locations of licensee emergency response centers

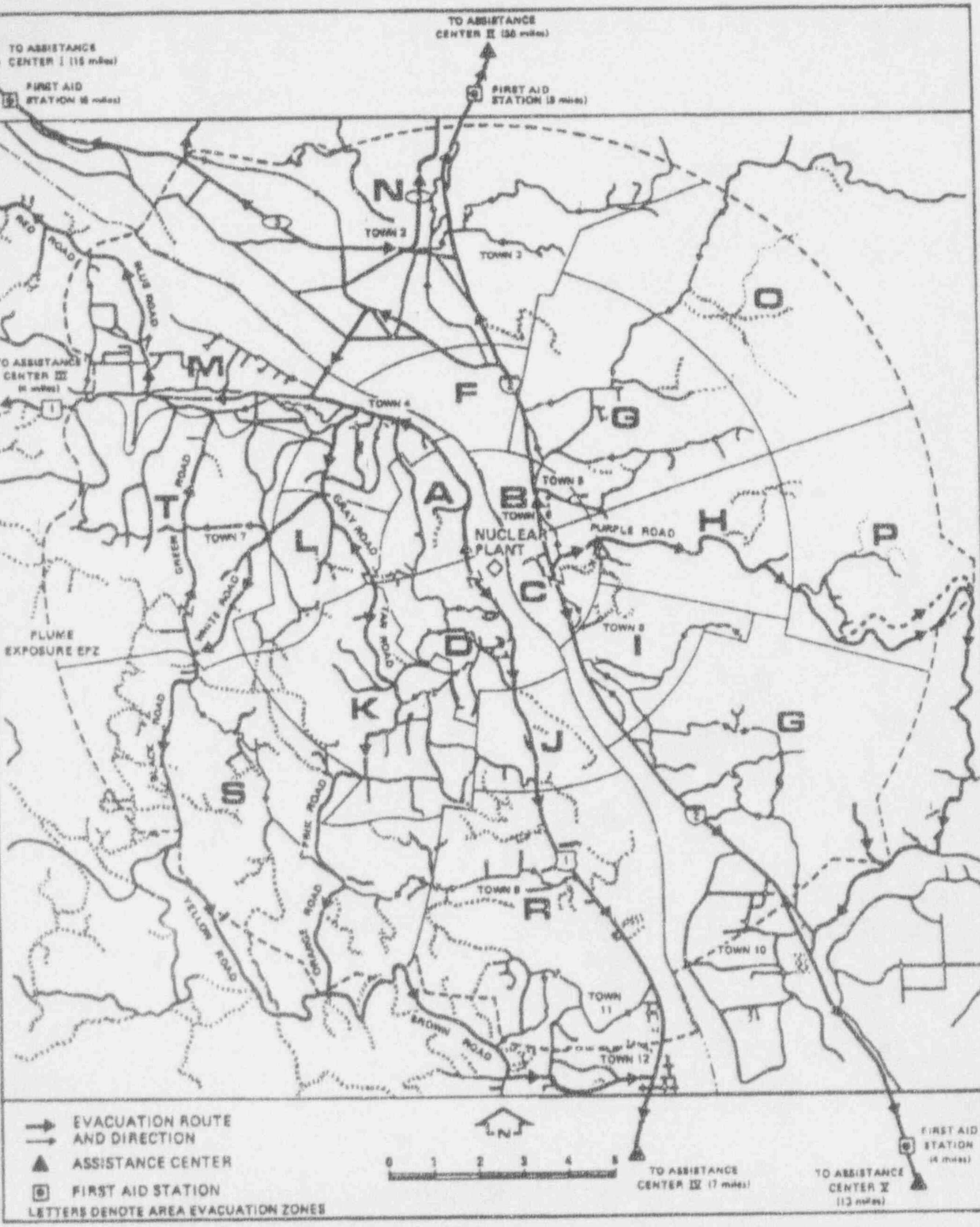


Figure 5.3-2 Example of a plume emergency planning zone with boundaries and evacuation routes determined by roads

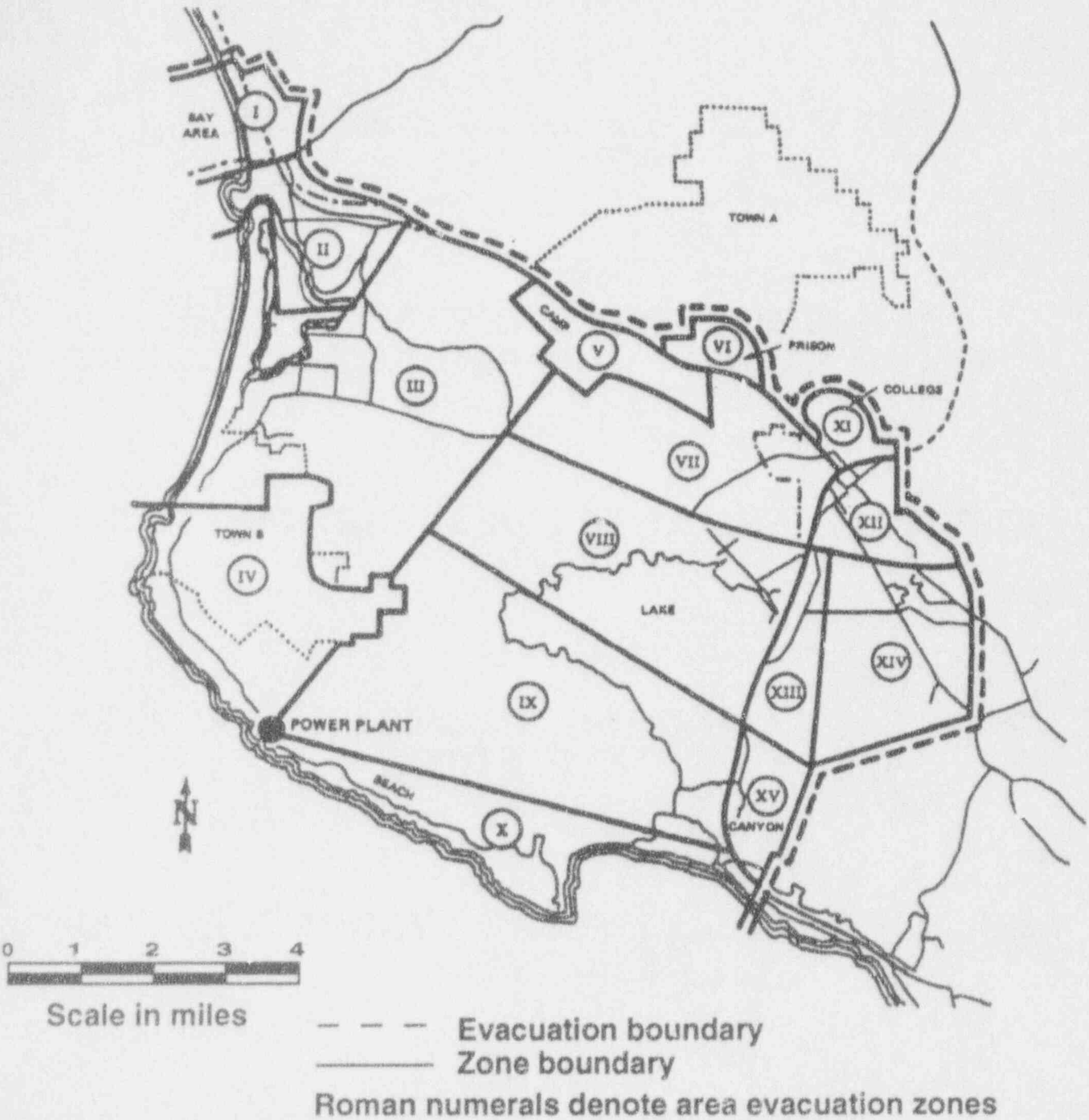


Figure 5.3-3 Example of a plume emergency planning zone (boundaries are determined by natural features)

EVENT DETECTED BY CONTROL ROOM STAFF

EVENT IS CLASSIFIED, AND EMERGENCY IS DECLARED

OFF-SITE OFFICIALS NOTIFIED ABOUT RECOMMENDATIONS OF PROTECTIVE ACTION

OFF-SITE OFFICIALS DECIDE ON ACTIONS TO BE TAKEN

SIRENS SOUND, AND THE PUBLIC TUNES TO LOCAL RADIO STATION

RADIO MESSAGE ADVISES TO EVACUATE AS SOON AS POSSIBLE

INDIVIDUALS LEAVE HOMES

Figure 5.3-4 Flow chart showing steps from detection of an event in the control room to public evacuation

References for Section 5.3

1. U.S. Nuclear Regulatory Commission and Federal Emergency Management Agency, *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants*, NUREG-0654, FEMA-REP-1, Rev. 1, November 1980.

2. H. E. Collins, B. K. Grimes, and F. Galpin, *Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants*, NUREG-0396/EPA 520/1-78-016, 1978.

3. D. C. Aldrich, P. McGrath, and N. C. Rasmussen, *Examination of Offsite Radiological Emergency Protective Measures for Nuclear Reactor Accidents Involving Core Melt*, NUREG/CR-1131, SAND78-0454, 1978.

4. U.S. Nuclear Regulatory Commission Information Notice (IN) 83-28, *Criteria for Protective Action Recommendations for General Emergencies*, May 1983.

5. U.S. Nuclear Regulatory Commission *Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability*, NUREG-0737, Supp. 1, No. 1, Washington, D.C., January 1983.

6. T. J. McKenna, et al, *Pilot Program: NRC Severe Reactor Accident Incident Response Training Manual*, NUREG-1210, Volumes 1-5, December, 1990.

7. U.S. Nuclear Regulatory Commission, *RTM-92, Response Technical Manual*, NUREG/BR-0150, Revision 2, October 1992.

5.4 Protective Actions

5.4.1 Learning Objectives

After completing this section, the student should able to

1. describe the NRC guidance regarding evacuation, sheltering, and post-release monitoring and relocation for severe accidents,

2. describe the role and efficacy of other protective actions,

3. explain why evacuation recommendations should not be delayed for fear of panic, and

4. describe NRC's role in the early implementation of protective actions.

5.4.2 Potential Protective Actions

Once a decision has been made that protective action is warranted, the type of protective action to be taken must be selected. It is convenient to identify three time phases, early, intermediate, and late; within each, different considerations apply to most protective actions. Although these phases cannot be represented by precise periods and may overlap, they provide a useful framework for the considerations involved in emergency response planning.

The early phase (also referred to as the emergency phase) is the period at the beginning of a reactor accident when immediate decisions for effective use of protective actions are required based primarily on indications of the core status and the prognosis for worsening conditions. Protective actions based on the PAGs may be preceded by precautionary actions during the early phase. This phase may last from hours to days.

The intermediate phase, is the period beginning after the radiological releases have been brought under control and reliable environmental measurements are available for use as a basis for decisions on additional protective actions. It extends until these additional protective actions are terminated. This phase may overlap the early and late phase and last from weeks to many months.

The late phase (also referred to as the recovery phase) is the period beginning when recovery actions to reduce radiation levels in the environment to acceptable levels for unrestricted use are commenced, and ending when all recovery actions have been completed. This period may extend from months to years.

The protective actions available to avoid or reduce radiation dose can be categorized as a function of exposure pathway and incident phase, as shown in Table 5.4-1. Evacuation and sheltering are the principal protective actions for use during the early phase to protect the public from exposure to direct radiation and inhalation from an airborne plume. It may also be appropriate to initiate protective action for the milk supply during this period, and, in cases where emergency response plans include procedures for issuing stable iodine to reduce thyroid dose, this may be an appropriate protective action for the early phase.

Some protective actions are not addressed by assignment of a PAG. For example, the control of access to areas is a protective action whose introduction is coupled to a decision to implement one of the other early or intermediate phase protective actions and does not have a separate PAG. And, although the use of simple, ad hoc respiratory protection may be applicable for supplementary protection in some circumstances, this protective action is primarily for use by emergency workers.

It is necessary to distinguish between evacuation and relocation with regard to incident phases. Evacuation is the urgent removal of people from an area to avoid or reduce high-level, short-term exposure, usually from the plume or deposited activity. Relocation, on the other hand, is the removal or continued exclusion of people (households) from contaminated areas to avoid chronic radiation exposure. Conditions may develop in which some groups who have been evacuated in an emergency may be allowed to return based on the relocation PAGs, while others may be converted to relocation status.

Relocation and decontamination are the principal actions taken to protect the public from whole body external exposure due to deposited material and from inhalation of any resuspended radioactive particulate materials during the intermediate and late phases. Decisions will be made during the intermediate phase concerning whether areas from which the public has been relocated will be decontaminated and reoccupied, or condemned and the occupants permanently relocated. Another protective action during the intermediate phase encompasses restrictions on the use of contaminated food and water. This protective action may overlap the early and late phases.

As indicated in Section 5.3, the initial, early protective actions to be recommended to the public under a given set of emergency conditions should be determined in advance (predetermined) if at all possible. However, adjustments to preplanned actions may be required if specific local conditions warrant. Four potential emergency actions are discussed in the following subsections: (1) evacuation, (2) sheltering, (3) improvised respiratory protection, and (4) use of potassium iodide (KI) as a thyroid blocking agent for radioiodine. Protective actions for the intermediate and late phases are discussed in subsection 5.4.2.5.

5.4.2.1 Evacuation

As illustrated in Section 5.4.4, for the most severe accidents, evacuation near the plant (within 2 to 3 miles) may be the only action that prevents early health effects. Early evacuation of the area near the plant has several benefits in terms of public safety:

1. Cloud shine dose from all or at least part of the plume can be avoided (if the evacuation begins before or shortly after the release).

2. Dose from contaminated ground and other surfaces can be avoided.

3. Inhalation of contaminated air can be avoided.

4. The highest-risk areas would be cleared early.

In contrast, sheltering only reduces exposures (and only moderately in a typical farmhouse); it does not avoid them. Consequently, emergency planners must continue to be concerned about people in shelters.

At certain times, evacuation may not be practical. For example, if an ice storm is in progress, if major transportation arteries are blocked, or if a major population center is involved, ordering an evacuation may result in entrapment of persons outside, where they may be more vulnerable than in their original locations. Predetermined evacuation recommendations should, however, be canceled only if entrapment conditions are going to delay evacuation for many hours. If early evacuation is simply not possible, emergency personnel should monitor for ground contamination following a release, if any, and motivate people to leave any highly contaminated areas (i.e., hot spots). It would, most likely, not be necessary for people to move very far from such heavily contaminated areas to significantly reduce their exposures.

A concern exists that, once a release from a severe reactor accident starts, an evacuation should not be recommended because the evacuees may run into or be overtaken by the plume. However, as mentioned in Section 5.2.3, plume concentrations decrease exponentially with distance from the source. As a result, large reductions in doses to individuals are achieved by evacuation. Conversely, sheltering in most homes can reduce a person's dose by no more than a factor of 2. Also, evacuation precludes the possibility of long term exposure to hot spots.

Studies consistently indicate that evacuation during plume passage does not increase risk over sheltering. Conversely, delaying evacuation can considerably increase risk. These conclusions are supported by the NUREG-1150 results for a large source term resulting from early containment failure at Zion as depicted in Figure 5.4-1, which compares probabilities of exceeding 50 rem acute red bone marrow dose given a major release for six different protective action scenarios. Clearly, scenario 4 (evacuation before release) provides the greatest risk reduction. Protective action scenarios 5 (evacuation at time of release) and 6 (evacuation 1 hour after release) both result in lower probabilities of exceeding the 50 rem bone marrow dose than scenario 2 (basement sheltering) which is better shelter than exists at many sites.

In summary, it is almost always better for people to move out of areas near the plant (2 to 3 miles) if at all possible, even if the release of radioactivity has already started. The main exception, as noted previously, is under severe entrapment conditions (e.g., a snow or ice storm) because a car is not as good a shelter as a house. Entrapment problems are expected to be rare at most reactor sites in the United States, especially rare in conjunction with a General Emergency. Fewer than 300 people live within the first 2 to 3 miles of most nuclear power plants in the United States. Within this distance there are few facilities such as hospitals that would require special attention in the event of an evacuation. At a few reactor sites, where these conditions are not met, the emergency planner (and responder) must recognize that evacuation would be more difficult. Emergency plans must be prepared and decisions made accordingly. It should be stressed that (1) for all sites, early evacuation of nearby areas would be most beneficial and (2) for the most severe accidents, early evacuation would be the only protective action available to achieve basic radiation protection objectives near the plant.

5.4.2.2 Sheltering

Early sheltering is an appropriate protective action measure

1. for areas where the risk of exceeding the doses required for early health effects is relatively low,

2. for lesser events (e.g., Site Area Emergencies) where a major release is not expected,

3. if outside entrapment problems are likely to occur should an evacuation be attempted,

Numerous studies indicate that, beyond 2 to 3 miles of the plant, sheltering followed by post-release monitoring and relocation from "hot spots" would be as effective as evacuation for most severe accident scenarios. This might not be the case under certain meteorological conditions, in particular, if the radioactive plume passes through rainfall or if severe inversion conditions trap and confine the plume near the ground. Such conditions cannot be predicted with any useful degree of accuracy, and off-site radiological monitoring after the release must be relied upon to determine when evacuation at distances greater than 2 to 3 miles from the plant is warranted.

Table 5.4-2 provides factors that can be used to indicate the relative amount by which exposures may be reduced for various pathways as a result of sheltering. These sheltering factors should be used for comparison purposes only, not for predictive purposes. They can be used to determine the type of structure to recommend if a choice of structures is available. For cloud and ground shine, small farmhouses provide very little protection; but, if a farmhouse has a basement, protection can be improved. Large concrete structures can provide a great deal of protection.

Enclosed structures can offer protection from the inhalation pathway. The degree of inhalation protection provided depends on the "openness" or ventilation rate of the shelter and on how long the plume remains outside. Small dwellings with closed windows and doors ventilate at a rate of about one air turnover per hour. For a one hour puff, a protection factor of about three (two-thirds reduction in dose commitment) can be achieved in such a dwelling. For longer releases (plumes), the inhalation protection factor would be lower (assuming that the wind does not shift). For perspective, virtually all potential life-threatening releases resulting from severe core damage accidents would be 0- to 2-hr puffs. Less-severe (in quantity) releases could last much longer.

5.4.2.3 Improvised Respiratory Protection

Improvised respiratory protection, such as placing a towel over the mouth and nose, reduces only the inhalation exposure, not the exposure to cloud shine or the exposure to contaminated ground and other surfaces. Since, for most severe accidents, inhalation dose would not be particularly important, improvised respiratory protection is a secondary protective action (i.e., it may be recommended in conjunction with evacuation or sheltering). Implementation of improvised respiratory protection should never delay implementation of other protective actions such as sheltering or evacuation.

Table 5.4-3 shows the results of experiments conducted using different types of improvised respiratory protection.[1] Military personnel used various household items for protection and measured their efficiency in removing particles. Some results were remarkable; for example, a bath towel had an efficiency of 74% to 85%. More recent experiments show that an efficiency of 90% can be achieved by using a surgeon's or painter's mask.

The use of a loose-fitting towel over the nose and mouth should reduce the inhalation exposure from small particulates by a factor of about 2 to 5. Babies can be lightly wrapped in blankets, such as they are for protection from wind and cold. Use of a tight-fitting heavy towel is expected to reduce particulate inhalation by about a factor of 10. Note, however, that exposure received through inhalation of gases is not reduced by either of these techniques. Basically, improvised respiratory protection could be used as a secondary protective action to provide some relatively unknown, nontrivial level of additional protection.

5.4.2.4 Use of Potassium Iodide (KI)

The Food and Drug Administration has recommended that potassium iodide tablets be administered for projected thyroid doses greater than 25 rem.[1] Ingestion of potassium iodide (KI) tablets reduces the dose to the thyroid caused by the intake of radioiodine. It must be understood, however, that use of the thyroid-blocking agent potassium iodide (KI) is not an adequate substitute for prompt evacuation or sheltering by the general population near a plant in response to a severe accident. The primary risk to the population from a severe reactor accident is bone marrow dose, not the dose to the thyroid from radioiodine.

To be effective, potassium iodide must be taken just before or shortly after exposure to radioiodine (within 1 to 2 hr). Thus, to be potentially effective, it must be readily available.[2] Taking the recommended dosage of potassium iodide (130 mg) just before or at the time of exposure could block more than 90% of radioactive iodine uptake by the thyroid as indicated in Figure 5.4-2. If taken approximately 3 to 4 hr after acute exposure, only about 20% blocking would occur in some persons. Note that a small percentage of people could react adversely to potassium iodide, but the risk of a severe reaction is very small.

The NRC and the Federal Emergency Management Agency (FEMA) recommend predistribution of potassium iodide to predesignated emergency workers, site personnel, and institutionalized individuals who might find it difficult to evacuate during an emergency. FEMA has stated the federal position that predistribution of potassium iodide to the general public should not be required for a state or local emergency plan to be acceptable.[3] The federal position on the use of potassium iodide is currently undergoing review.

5.4.2.5 Other Protective Actions

Other protective actions such as decontamination of evacuees, milk contamination control, and reservoir (water) protection may also be part of the emergency response; however, very early implementation of these actions (within 0 to 4 hr of the release) would not be crucial to their effectiveness. They would, however, be important in reducing the number of latent health effects.

Long-term protective actions are used to reduce the number of latent health effects. For radiation protection purposes, it is assumed that, no matter how low the dose, some percentage of the population will eventually suffer from cancer because of the radiation exposure. As indicated in Section 5.1, consequence models predict that many of the radiation-induced cancers would occur due to doses received by people tens to hundreds of miles from the plant. This is the result of a great number of people receiving a very low dose. Thus, as a practical matter, emergency-phase protective actions available to reduce these effects are very few. In the early time frame of a response, sheltering to long distances, where convenient, might be advised--much as for an air pollution alert.

After a severe reactor accident that occurs during the growing season, crops and pasture within the 50 mile ingestion pathway EPZ might need to be decontaminated, disposed of, or temporarily quarantined to permit radioactive decay. Surveys of pastures, milk, fruits, and leafy vegetables would need to be conducted very soon after the accident. Dairy and meat animals would have to be fed uncontaminated stored forage or moved from contaminated to uncontaminated pastures. Contaminated crops would have be prevented from reaching market (entering the food distribution system), and residents in the 50 mile EPZ would have to be carefully warned not to eat contaminated food they had privately grown.

5.4.2.6 Direction of Initial Protective Action Coverage

In what direction should initial protective actions be taken? Past practice has been to plan to initiate protective action only in a "downwind" direction. This would greatly limit the population affected. The problem is that it would be difficult if not impossible in the early time frame to predict the magnitude and timing of a major release and where "downwind" would be at the time of a release. For example, frequent wind shifts occurred during the Three Mile Island accident as discussed in Section

5.2.6. Emergency plans that call for awaiting a major release provide little, if any, risk reduction potential for the public. Therefore, the initial, early, precautionary evacuation near the plant should be effected in all directions.

5.4.3 Guidance on Protective Actions

Technical guidance on determining protective actions for severe reactor accidents has evolved from numerous severe accident studies including NUREG-1150.[4] The current NRC guidance is illustrated Figure 5.4-3 and discussed in the following subsections.

5.4.3.1 Timing of Initial Actions

To be most effective, initial protective actions (evacuation or sheltering) must be taken before or shortly after the start of a major release to the atmosphere.

As discussed in Section 5.1, core damage is required for a severe release, and control room indicators of core damage should be numerous. However, once core damage exists, the timing and size of a release cannot be projected. A major release would be very intense with most of the radioactive material being released within 0.5 to 2 hr of containment failure. It would be virtually impossible to predict the occurrence or time of containment failure in most severe accident sequences. Protective actions must be taken early where at all possible to be effective in avoiding early health effects. Relying on predictions of containment failure or waiting for indications of containment failure could delay an evacuation during the period when it would be the most effective action for avoiding offsite health effects.

The best way to ensure that protective actions are started before a major release is to initiate the actions as soon as core damage is detected. If the decision to take action awaits a dose projection (if possible) or field monitoring results, the population close to the plant could be exposed to a large puff release. This is one of the primary reasons for establishing emergency action levels that result in detection of core damage, declaration of a General Emergency, and recommendation of protective actions.

5.4.3.2 Initial Evacuation and Sheltering

If a severe core damage accident occurs, people should immediately evacuate areas near the plant (within a 2- to 3-mile radius) and remain in shelter elsewhere for the immediate future.

As discussed in Section 5.2, risk decreases rapidly up to a distance of about 2 to 3 miles and decreases more slowly thereafter. Thus, in a core melt accident, early evacuation of the first 2 to 3 miles would markedly reduce individual risks (i.e., the payoffs would be greatest within this distance). Second, the population within this distance is small (at many sites, a few hundred people), and there are normally few impediments to immediate evacuation of the area. Indeed, this area encompasses the low-population zone around most reactor sites. Third, the individual risk of early deaths or injuries for the most severe accident is, in most cases, confined to this area. Immediate evacuation of people near the plant could well prove to be precautionary because most severe accidents (like the Three Mile Island accident) would not be expected to lead to a major release. On the other hand, core damage accidents are expected to be extremely rare, so that precautionary evacuations would also be rare; and the results of not taking immediate protective actions could be tragic.

5.4.3.3 Evacuation from Hot Spots

Doses from ground contamination may become very important within a few hours of a major release, requiring prompt radiological monitoring and relocation of people near hot spots.

After implementing initial protective actions near the plant, dose projections and field monitoring should be performed. Dose projections would be used to determine if protective actions should be expanded according to the Environmental Protection Agency protective action guides. As is also discussed in Section 5.2, great uncertainties are associated with dose projection. Therefore, dose projections should be very suspect. As soon as possible after a release, field monitoring data should be the preferred basis for expanding initial protective actions.

In the event of an actual major release, anyone found in shelter in an area of high ground-level contamination (e.g., >1 R/hr) would be asked to leave-whether or not an emergency plan calls for it. The predetermined level of 1 R/hr conforms to the Environmental Protection Agency protective action guide of 1 to 5 rems projected whole-body dose. As noted earlier, evacuation at lower dose rates could be recommended on an ad hoc basis; but for a very severe accident, the 1-R/hr level may be suitable as an initial predetermined "trip" level.

5.4.3.4 Environmental Protection Agency Guidance

The conclusions presented in the two preceding subsections, which call for evacuation near the plant and monitoring after a major release, are consistent with the objective of reducing doses that would otherwise exceed Environmental Protection Agency protective action guide levels. It is important to note that the initial actions are also taken to meet the a more important objective of protecting against the possibility of early health effects near the plant.

Table 5.4-4 summarizes Environmental Protection Agency protective action guides. (See also Section 5.1.6.2.) Table 5.4-4a presents the 1980 PAGs, while the newer PAGs, which replace projected whole body dose with committed effective dose equivalent (CEDE), are presented in Table 5.4.3b. Note that for a projected dose greater than or equal to 1 rem whole body (CEDE) or 5 rem thyroid, evacuation is recommended. If evacuation is not immediately possible or if sheltering would provide better protection (unlikely for severe reactor accidents) sheltering should be initiated. Below a projected dose of 1 rem whole body (CEDE) or 5 rem thyroid, no planned (i.e., predetermined) protective action would be warranted. However, ad hoc decisions are provided for on a case-by-case basis (see footnotes to Table 5.4-4a.

The Food and Drug Administration has established protective action guides for food and agricultural pathways. These are listed in Table 5.4-4c.

5.4.3.5 Protective Action Flow Chart

The NRC has incorporated the guidance discussed in this section into response procedures and training manuals for the NRC staff, the latest edition of which is Response Technical Manual (RTM)-92.[5] Figure 5.4-4 is the protective action flow chart from RTM-92, which depicts the current NRC guidance for determining initial protective action to be recommended to off-site officials in the event of a severe accident.

5.4.4 Benefits Of Protective Actions

To examine the effectiveness of protective actions for a very severe accident, a calculation was made assuming the large PWR-1 source term from the Reactor Safety Study.[6] It was further assumed that people within 1, 2, or 3 miles of a site would leave at a speed of 10 miles/hr, starting 0.5 hr after the beginning of the release (a somewhat pessimistic time delay). People outside these early evacuation radii were presumed to seek shelter in basements of homes. People in shelters within 10 miles were relocated after 4 hr of exposure to ground contamination (in addition to the puff); people farther than 10 miles were relocated after 8 hr of exposure to ground contamination (also in addition to the puff).

These relocation times were used as estimates of the time that might be required for monitoring teams to locate hot spots and warn and motivate the people and for people to leave. The calculations were performed for a typical 800-MW(e) reactor at a site in the northeastern United States.[7] Actual population distributions were used. The results are indicative of the potential benefits of the predetermined protective action scheme.

As discussed in Section 5.2.4, doses decrease rapidly within the first few miles of a potential atmospheric release point. Results of the previously described calculations bear out this observation, as displayed in Figure 5.4-5. This figure displays the conditional risk of an early fatality for early (0.5 hr after start of the release) evacuation radii of 1, 2, and 3 miles and 24 hr of normal activity (no protective actions). The specific dose/risk projections from this type of calculation are not very meaningful, but when used to compare various options, they are useful. In this case, they show a reduction of a factor of 10,000 in the possibility of early fatalities when there is early evacuation of the area near the plant. The risk of an early fatality is greatly reduced by using the 3-mile evacuation radius. Although zero fatalities were calculated for the 3-mile early evacuation case, this in no way represents a prediction for the noted assumptions. Nevertheless, the potential benefits of the recommended 2- to 3-mile early evacuation, shelter, and relocation scheme are evident from this example.

The example also indicates the importance of monitoring to locate ground contamination and relocating the sheltered population away from hot spots quickly. In this case the people were assumed to evacuate if the ground contamination is 1 R/hr (about 100,000 times the normal background dose rate).

The basic conclusion is that, even for a very large release, virtually all early fatalities can be prevented if a) the areas near the plant (2 to 3 miles) are evacuated before or shortly after the release and b) prompt monitoring is conducted to locate ground contamination that requires expeditious relocation of people sheltered elsewhere.

5.4.5 Implementation

5.4.5.1 Entrapment Scenarios

Scenarios can be hypothesized in which predetermined protective actions would not be the best (or even feasible) responses. For example, entrapment could result from a major earthquake that blocked normal evacuation routes. Under such conditions, local officials must use common sense in providing the best shelter and/or evacuation possible. Expedient shelter of some sort is always available. However, coincidences of core melt and major impediments to immediate evacuation of small areas by most people should be extremely rare.

5.4.5.2 Evacuation Risks

Objections have been raised to evacuation because of fears of panic or injuries during the evacuation. Evacuations of up to a few thousand people from areas up to about several square miles are not uncommon. Examples of evacuations of record are presented in Table 5.4-5. Evacuations of significant size occur about every week to ten days in the United States. (Keep a mental note every time you hear of an evacuation.)

The historical fatality risk is about 1/500,000 per person during evacuations. This evacuation risk is considerably less than the estimated 1/10 to 1/100 risk of a fatality given a core melt accident typically reported in probabilistic risk assessments. Although the comparison says nothing definitive about the risk for any particular core melt accident, it does indicate strongly that, on the average, it would be far less risky for a person to evacuate than to remain within 2 to 3 miles of a nuclear power plant experiencing a severe core damage accident. Conversely, on a predetermined basis, an evacuation should not be recommended unless a core-melt accident is actually under way.

It must also be remembered that few people live close to most nuclear power reactors. Figure 5.4-6[8] illustrates the number of people within 1 and 5 miles of 111 nuclear power plant sites (actual or proposed in 1979). Evidently, evacuations of everyone within a circular area of radius somewhere between 1 and 5 miles of these sites would be below the 10,000-person figure. At most sites, in fact, fewer than 300 people live within 2 miles of the site.

5.4.5.3 Public Behavior During Emergencies

No nuclear accidents with severe off-site consequences have occurred in the United States. Other types of events have occurred that may indicate how people would respond to a nuclear accident. Objections to citing public behavior during nonnuclear emergencies for purposes of radiological emergency planning can and have been expressed.

Although the data base is limited, several nuclear-related incidents involving public response have occurred and can be compared to the nonnuclear experience. Some of these incidents (excluding weapons-related incidents) are presented in Table 5.4-6. The Environmental Protection Agency found no reason to expect that people will react differently to a nuclear accident than they would to a flood, fire, or similar emergency.[9]

The accident that appears to be of the greatest relevance is Three Mile Island (TMI). The accident at TMI's Unit 2 occurred at 7:00 a.m. on March 28, 1979. By 8:00 a.m., the national television networks were broadcasting the news. A small percentage of the local population left the area during the first two days. On the third day (Friday), the governor of Pennsylvania recommended the evacuation of children and pregnant women. By the end of the weekend, about half of the population within 20 miles had left the area. Throughout this time, the people were subjected to intense stress and (to them) conflicting opinions and advice. Despite these conditions, the evacuations that occurred were orderly.

Some observers have stated that the evacuations represented panic. Conversely, it could be argued that the public's behavior was perfectly understandable considering the intense pressures to which they were subjected (e.g., various authorities expressed diametrically opposed positions, and some authorities even reversed their own positions during the course of the accident). In fact, if the current protective action guidance had been in place at the time of the accident, evacuation of the area near the plant would have been recommended.

Although fear and trauma are common in emergency situations, widespread panic (irrational behavior caused by stress) is uncommon to nonexistent. In fact, disaster victims often react with initiative, sometimes insisting on acting on their own against the expressed advice of public authorities. (Authorities might call this panic.) Furthermore, contrary to general assumptions, local organizations have generally proven themselves able to cope with emergencies rather than to be overwhelmed by them. Most disasters have not led to widespread antisocial behavior such as looting, nor do disasters destroy the morale of the communities involved. In many cases, the result of a disaster, over time, is an increase in the collective morale of the community.

During an evacuation, it can be expected that a small part of the population will not follow recommendations (will not evacuate) and that another group will evacuate on their own. However, most people will react calmly and normally to authoritative directions during an emergency. In media accounts of evacuations, reporters typically note with surprise that, instead of panicking, people helped each other.

In essence, the keys to a successful protective action strategy are early warning, clear instructions, and strong motivation provided by an authority figure such as a local newscaster, police chief, mayor, or governor.

Some fear and trauma should be expected in response to an evacuation order, but fears by authorities of widespread panic should not be an impediment to ordering an evacuation if grave cause exists.

5.4.5.4 NRC's Role in Implementation

In cooperation with local officials, most licensees have developed site-specific criteria for recommending protective actions to the public. Normally the NRC would not be part of the early predetermined protective action decision process. Licensees are required to report those events to off-site officials within 15 min and then immediately to the NRC (within 1 hr). It is expected to take an additional hour after notification for the NRC response organizations to be activated and prepared to comment on protective action recommendations. Calling the NRC to confirm a preplanned protective action would only delay protective action implementation.

The NRC staff does have some influence over early response actions by virtue of its emergency planning appraisals and its role as the Lead Federal Agency in the event of an accident at a commercial U.S. reactor. In this role, the NRC is responsible for

1. coordinating Federal protective action positions and presenting them to the states (with the Federal Emergency Management Agency, FEMA, if time permits);

2. coordinating the Federal technical response with the Federal non-technical response;

3. providing information on the emergency conditions onsite; and

4. being the source of information on potential or real offsite radiological conditions.

When time permits, the NRC should rely on the expertise of Environmental Protection Agency (EPA), U.S. Department of Agriculture (USDA), and Health and Human Services (HHS) when interpreting their guidance. The NRC is responsible for promptly releasing plant and radiological data to State and other Federal agencies with protective action responsibilities.

5.4.6 Major Points

The major points covered in this section are summarized in the following paragraphs.

- To be most effective, protective actions must be taken before or shortly after the start of a major release to the environment.

- If a severe core damage accident occurs, people should immediately evacuate areas near the plant (within a 2- to 3-mile radius) and remain in shelter elsewhere for the immediate future.

- Doses from ground contamination may become very important within a few hours of a major release, requiring prompt radiological monitoring and relocation of people near hot spots.

- Sheltering is preferred if entrapment problems are likely to occur in an evacuation. Sheltering is also appropriate for lesser events (e.g., a Site Area Emergency).

- Improvised respiratory protection, can be quite effective, but only in reducing inhalation doses. Improvised respiratory protection should not be allowed to delay sheltering, evacuation, or relocation.

- Use of the thyroid-blocking agent KI is not an adequate substitute for prompt evacuation or sheltering by the general population near a plant in response to a severe accident.

- Evacuations of up to a few thousand people from areas of several square mile are not uncommon.

- On average, it would be far less risky for a person to evacuate than to remain within 2- to 3- miles of a nuclear power plant experiencing a severe accident.

- Most people will react calmly and normally during an emergency evacuation. A decision to evacuate should not be delayed for fear of panic.

- The NRC may have little influence over the implementation of early protective actions, except by virtue of emergency planning appraisals.

Table 5.4-1 Exposure pathways, nuclear incident phases, and protective actions

Potential Exposure Pathways	Incident Phases	Potential Protective Actions
1. External radiation from facility	Early	Sheltering Evacuation Control of access
2. External radiation from plume	Early	Sheltering Evacuation Control of access
3. Inhalation of activity in plume	Early	Sheltering Use of potassium iodide Evacuation Ad hoc respiratory protection Control of access
4. Contamination of skin and clothes	Early, Intermediate	Sheltering Evacuation Decontamination of persons
5. External radiation from ground deposition	Early, Intermediate, Late	Evacuation Relocation Decontamination of land and property
6. Ingestion of contaminated food and water	Intermediate, Late	Food and water controls
7. Inhalation of resuspended activity	Intermediate, Late	Relocation Decontamination of land and property

Note: The use of stored animal feed and uncontaminated water to limit the uptake of radionuclides by domestic animals in the food chain can be applicable in any of the phases.

Table 5.4-2. Factors by which radionuclide exposure may be reduced by sheltering for different types of shelters and pathways of exposure

Type of shelter	Cloud shine	Ground shine	Inhalation
Small, frame building			
Without basement	1	2	2[a]
With basement	3	5-10	3[a]
Multiple-story, concrete structure	5	10	5

[a]Puff release only.

Table 5.4-3. Respiratory protection provided by common household and personal items against aerosols of 1- to 5-μm particle size[a]

Item	Number of thicknesses	Geometric mean efficiency (%)
Handkerchief, man's cotton	16	94.2
Toilet paper	3	91.4
Handkerchief, man's cotton	8	88.9
Handkerchief, man's cotton	Crumpled	88.1
Bath towel, turkish	2	85.1
Bath towel, turkish	1	73.9
Bed sheet, muslin	1	72.0
Bath towel, turkish (wet)	1	70.2
Shirt, cotton (wet)	1	65.9
Shirt, cotton	2	65.5
Handkerchief, woman's cotton (wet)	4	63.0
Handkerchief, man's cotton (wet)	1	62.6
Dress material, cotton (wet)	1	56.3
Handkerchief, woman's cotton	4	55.5
Slip, rayon	1	50.0
Dress material, cotton	1	47.6
Shirt, cotton	1	34.6
Handkerchief, man's cotton	1	27.5

[a]Resistance obtained when checked immediately after hand wringing. This resistance began to decrease after about 1 min when the material began started to dry.

Table 5.4-4a. Environmental Protection Agency recommended protective actions[a] to reduce whole-body and thyroid dose from exposure to a gaseous plume

Projected Dose (rem) to the Population		Recommended actions[b]	Comments
Whole Body[c] Thyroid	< 1 < 5	No planned protective actions[d] State may issue an advisory to seek shelter and await further instructions. Monitor environmental radiation levels.	Previously recommended protective actions may be considered or terminated.
Whole Body Thyroid	1 to < 5 5 to < 25	Seek shelter as a minimum. Consider evacuation. Evacuate unless constraints make it impractical. Monitor environmental radiation levels. Control access.	If constraints exist, special consideration should be given for evacuation of children and pregnant women.
Whole Body Thyroid	5 and above 25 and above	Conduct mandatory evacuation. Monitor environmental radiation levels and adjust area for mandatory evacuation based on these levels. Control access.	Seeking shelter would be an alternative if evacuation were not immediately possible.

[a]EPA Manual of Protective Action Guides and Protective Actions for Nuclear Incidents, 1980.

[b]These actions are recommended for planning purposes. Protective action decisions at the time of the incident must take existing conditions into consideration.

[c]Effective dose from external sources (cloud and ground) is approximately equal to whole body dose.

[d]At the time of the incident, officials may implement low-impact protective actions in keeping with the principle of maintaining radiation exposures as low as reasonably achievable.

Table 5.4-4b. Environmental Protection Agency recommended protective actions[a] to reduce external gamma dose from plume exposure and committed dose to the thyroid from inhalation.

Projected Dose (rem) to the Population	Recommended actions[b]	Comments
1-5 rem[c]	Evacuation[d] (or sheltering)	Evacuation (or for some situations, sheltering[b]) should normally be initiated at one rem.
25 rem[d]	Administration of stable iodine	Requires approval of state medical officials.

[a]EPA Manual of Protective Action Guides and Protective Actions for Nuclear Incidents, 1991.

[b]Sheltering may be the preferred protective action when it will provide protection equal to or greater than evacuation, based on consideration of factors such as source term characteristics, and temporal or other site-specific conditions.

[c]The sum of the effective dose equivalent resulting from exposure to external sources and the committed effective dose equivalent incurred from all significant inhalation pathways during the early phase. Committed dose equivalents to the thyroid and to the skin may be 5 and 50 times larger respectively.

[d]Committed dose equivalent to the thyroid from radioiodine.

Table 5.4-4c. Food and Drug Administration (FDA) protective action guides (PAGs)

Organ	FDA PAG[b] dose (rem)	Protective Action
Whole body (bone)	0.5-5	At lower projected dose, use of grazing land should be restricted. At higher projected dose, contaminated milk should be impounded.
Thyroid	1.5-15	
Other body organs	0.5-5	

Table 5.4-5. Examples of large-scale evacuations (6 months in 1978)

Date	Number evacuated	Place	Incident
6/30/78	3,000	Destrehan, La.	Rail car gas leak (styrene gas)
6/21/78	600,000	Salonika, Greece	Earthquake
5/15/78	1,000	Nacogdoches, Tex.	Chemical explosion; train wreck
4/26/78	1,500	Bowling Green, Ky.	Tank car containing poisonous gas ruptured
4/8/78	1,500	Brc nson, Neb.	30-car derailment; tank car exploded (phosphorous)
4/6/78	2,000	Pineville, Ky.	Liquid propane tank car leak
4/1/78	2,500	Kinsburg, Ind.	Chemical plant fire; toxic fumes
3/15/78	2,000	Steubenville, Ohio	Chemical plant explosion; toxic chlorine fumes
3/8/78	1,200	Vicksburg, Miss.	Insecticide tank at chemical plant exploded
3/2/78	200	Galax, Va.	1600-gal liquified propane spill
2/27/78	250	Youngstown, Fla.	Ruptured railway car; chlorine gas; wind shift noted
2/27/78	2,000	Waverly, Tenn.	Derailed tank car explosion; volatile propane
1/28/78	500	Damascus, Ark.	Leak from fuel tank (NO_4)
1/17/78	52	Pond Eddy, Pa.	11,000-gal acetaldehyde spill
12/29/77	800	Goldonna, La.	Chemical freight train crash
11/29/77	1,000	Norfolk, Neb.	Tank car carrying propane gas ruptured
11/28/77	771	Battle Creek, Neb.	Propane gas leak from tank car
11/8/77	1,000	Marion, Iowa	Tank car carrying propane gas ruptured
10/15/77	600	St. Marys, Kan.	Toxic fumes; unknown origin
10/13/77	800	Chattanooga, Tenn.	Gas fumes; elementary school
10/8/77	2,000	Midland, Mich.	Poisonous chlorine gas leak from chemical plant
10/4/77	160	Kansas City, Mo.	Elementary school; carbon monoxide leak
9/19/77	2,600	Berryville, Ark.	Fire at a fertilizer warehouse; ammonia and nitric acid
9/5/77	2,000	Watseka, Ill.	Railroad car derailed; ethylene oxide
7/13/77	5,200	Rockwood, Tenn.	Chemical truck wreck
5/17/77	2,000	International Falls, Minn.	Rail car leaked chlorine gas
12/11/76	10,000	Baton Rouge, La.	Chlorine gas leak at chemical plant
5/29/76	500	Centerville, Ill.	Toxic fumes released; two tank cars; chlorosulfonic acid and sulfuric acid
5/16/76	1,000	Glen Ellyn, Ill.	Tank car leaking toxic ammonia fumes
4/13/76	3,800[a]	Dwight, Ill.	Truck leaking liquid bromine

[a]Included evacuation of 209 severely retarded and handicapped children, only nine of whom could walk, and another 92 elderly patients from a different center. Total time consumed by the evacuation was 2 hr, and little confusion was noted. Public officials complained about the lack of resources.

Table 5.4-6. Public response to nuclear-related incidents

Date	Location	Incident	Public reaction
1957	Windscale, England	Accident at a graphite reactor caused the release of 20,000 Ci of radioiodine	Typical, no panic
1977	Ft. St. Vrain, Colo.	Erroneous reports of a release of 20 Ci/sec from a nuclear power reactor	Normal, no panic despite blizzard conditions
19__	Rocky Flats, Colo.	Major fire at a plutonium plant	Normal, no panic or widespread flight
1980	Crystal River, Fla.	20,000 gal of primary water was spilled into the containment	Normal, no panic or widespread flight
1979	Three Mile Island, Pa	Nuclear power plant accident	Half of population within 20 miles evacuated within 5 days
1982	Rochester, N.Y.	Primary coolant released to the atmosphere from R.E. Ginna nuclear power plant	Normal, no panic or widespread flight
1981	Indian Point, N.Y.	Power transformer exploded when lightning struck a nuclear power station	Small-scale evacuation

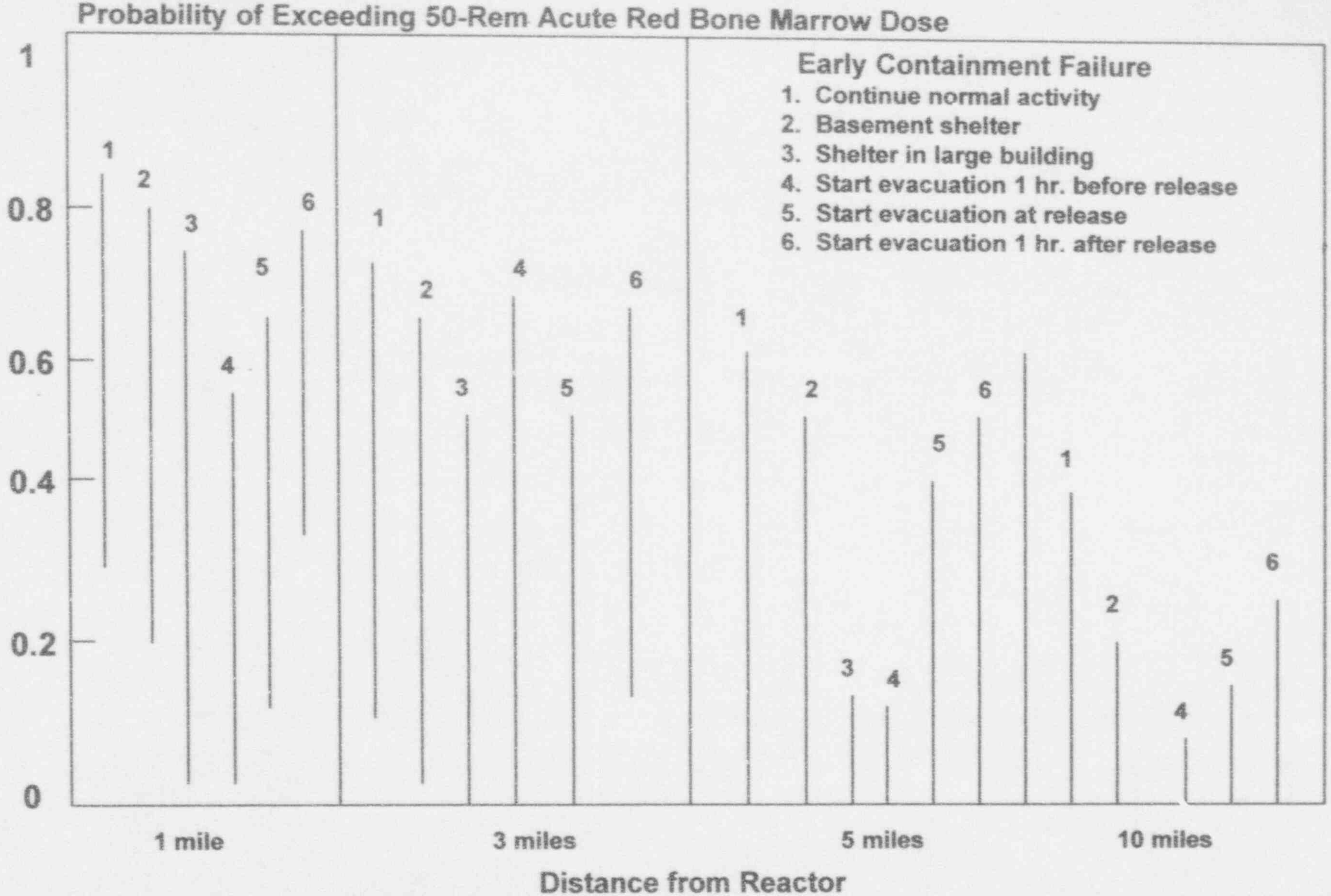


Figure 5.4-1 Relative effectiveness of early protective actions given early containment failure (Source: NUREG-1150, Figure 13.5)

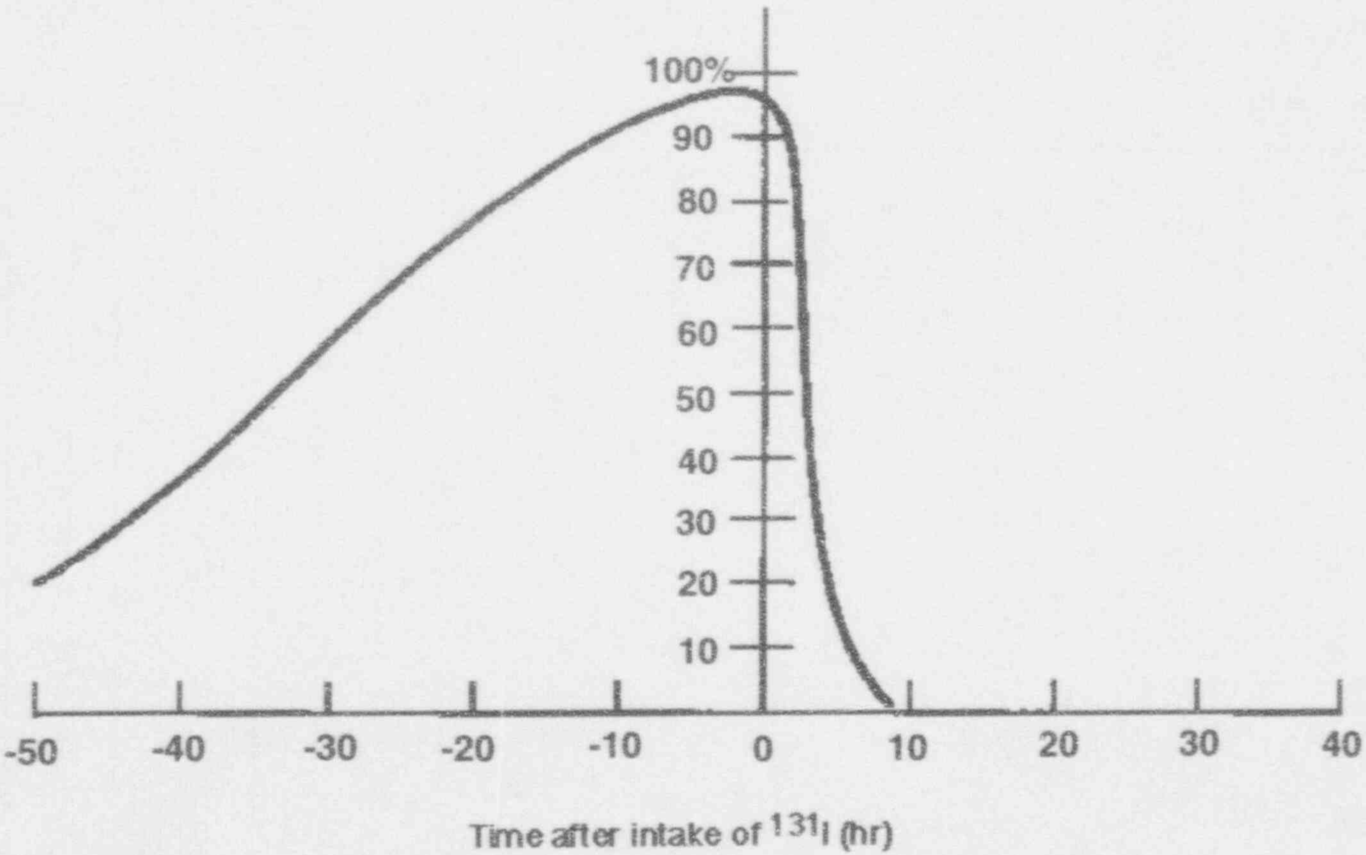


Figure 5.4-2 Percent of thyroid blocking afforded by 100 mg. of stable iodine (130 mg. of potassium iodide) as a function of time of administration before or after a 1-µCi slug intake of ^{131}I

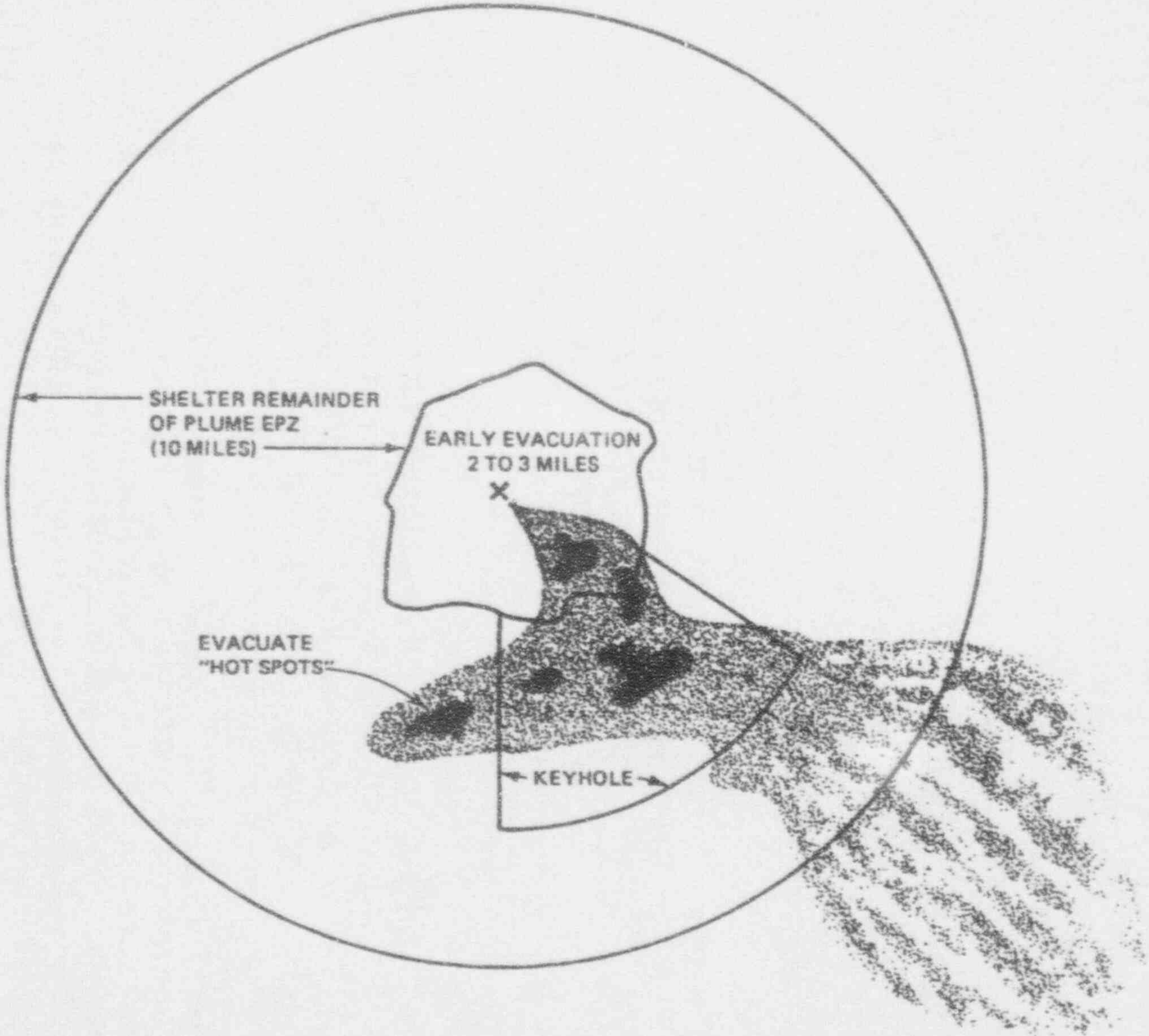
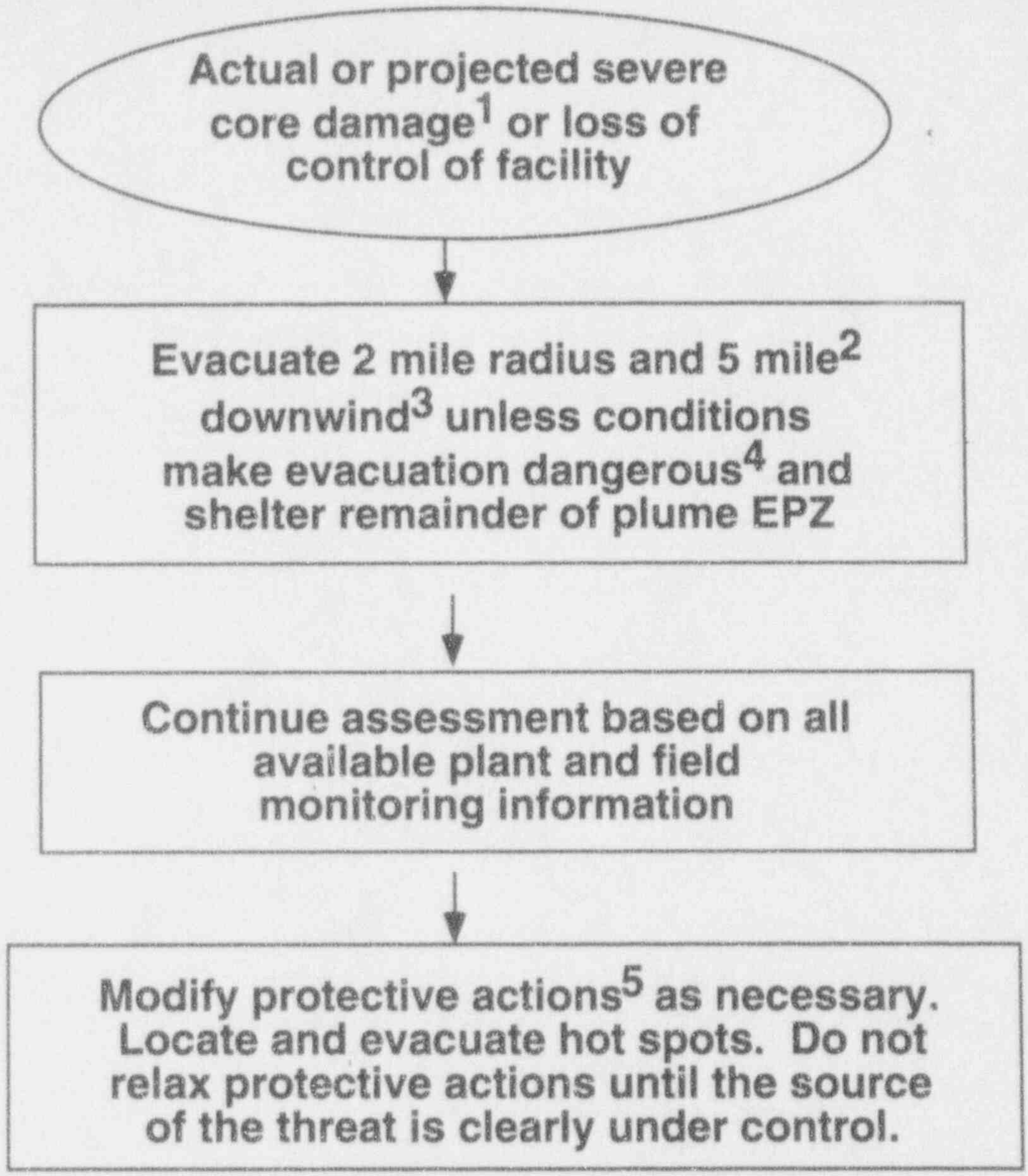


Figure 5.4-3 Early protective actions for core melt accidents



[1] Severe core damage is indicated by (1) loss of critical functions required for core protection (e.g., loss of injection given a LOCA); (2) high core temperatures (PWR) or partially covered core (BWR); (3) very high radiation levels in area or process monitors.

[2] Distances are approximate -- actual distances will be preplanned based on local conditions.

[3] During preparation for evacuation, people should shelter if possible.

[4] Such as very dangerous travel conditions or immobile infirmed population.

[5] Consider EPA PAGs (Table 5.4-3)

Figure 5.4-4 Protective action flow chart for severe core damage or loss of control facility public protective actions

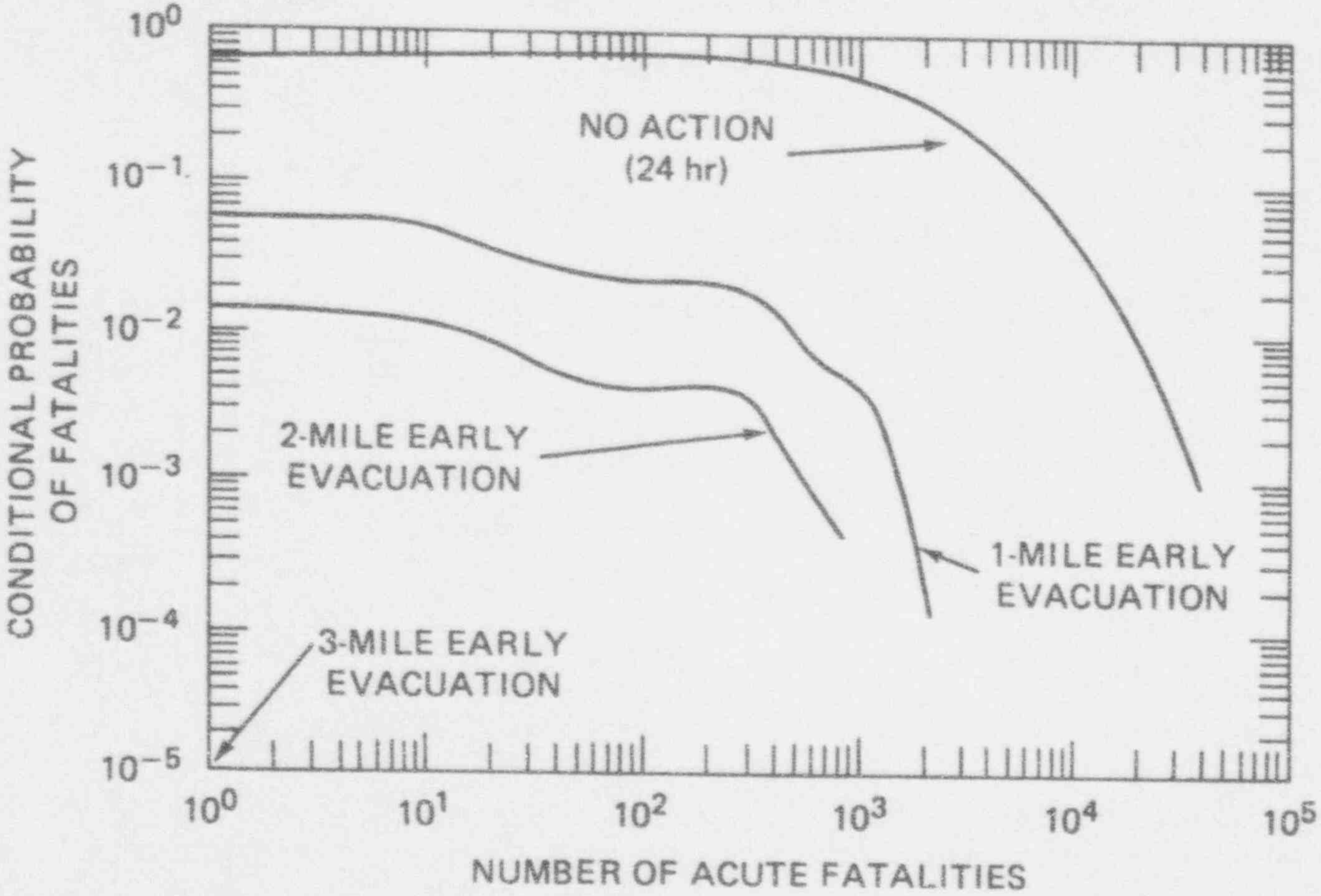


Figure 5.4-5 Conditional probabilities of various numbers of acute fatalities, assuming the Reactor Safety Study PWR 1 source term, early evacuation of small areas, and a slow relocation from highly contaminated areas

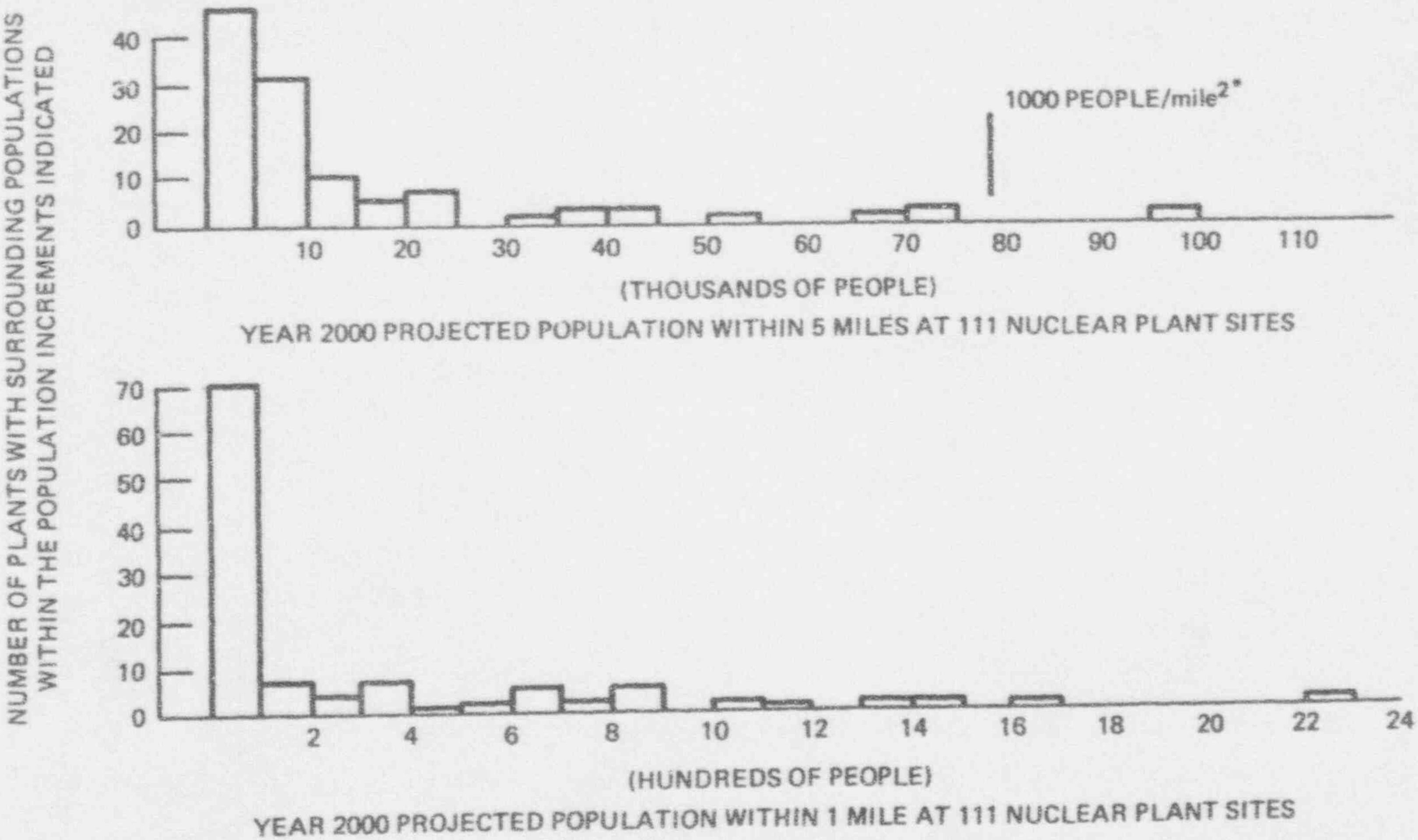


Figure 5.4-6 Number of people within 1 and 5 miles of 111 nuclear power plants, actual or proposed in 1979

References for Section 5.4

1. J. A. Martin, Jr., et el, "Pilot Program: NRC Severe Reactor Accident Incident Response Training Manual, Public Protective Actions -- Predetermined Criteria and Initial Actions," NUREG-1210, Volume 4, 1987.

2. J. A. Martin, "Potassium Iodide: Predistribution or Not? The Real Emergency Preparedness Issue," *Health Physics*, **49(2)**:287-289, August 1985.

3. U.S. Food and Drug Administration, "Radioactive Contamination of Human and Animal Feeds and Potassium Iodide as a Blocking Agent in a Radiation Emergency, *Federal Register*, 43:242, Part VII, December 15, 1978.

4. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

5. U.S. Nuclear Regulatory Commission, *RTM-92 Response Technical Manual*, NUREG/BR-0150, Vol. 1, Rev. 2, October 1992, page I-4.

6. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, WASH-1400, October 1975.

7. C. A. Sakenas, et al, *Pilot Program: NRC Severe Reactor Accident Incident Response Training Manual, Response of Licensee and State and Local Officials*, NUREG-1210, Volume 3, 1987.

8. U.S Nuclear Regulatory Commission, *Demographic Statistics Pertaining to Nuclear Power Reactor Sites*, NUREG-0348, October 1979.

9. J. M. Hans, Jr. and T. C. Sell, *Evacuation Risks--An Evaluation*, Environmental Protection Agency report EPA-520/6-74-002, Office of Radiation Research, National Environmental Research Center, Las Vegas, Nevada, June 1974.

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-6042
SAND93-0971

2. TITLE AND SUBTITLE

Perspectives on Reactor Safety

3. DATE REPORT PUBLISHED

MONTH	YEAR
March	1994

4. FIN OR GRANT NUMBER

L1914

5. AUTHOR(S)

F. E. Haskin/UNM
A. L. Camp/SNL

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.)*

Chemical and Nuclear Engineering Department
209 Farris Engineering Center
University of New Mexico
Albuquerque, NM 87131

Under Contract To:
Sandia National Laboratories
Albuquerque, NM 87185-0747

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 Safety Issue Resolution
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
Washington, D.C. 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

The U.S. Nuclear Regulatory Commission (NRC) maintains a technical training center at Chattanooga, Tennessee to provide appropriate training to both new and experienced NRC employees. This document describes a one-week course in reactor safety concepts. The course consists of five modules: (1) historical perspective; (2) accident sequences; (3) accident progression in the reactor vessel; (4) containment characteristics and design bases; and (5) source terms and offsite consequences. The course text is accompanied by slides and videos during the actual presentation of the course.

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

reactor safety, Technical Training Center

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

Printed on recycled paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

120555139531 1 19A19B19C19D1
US NRC-OADM
DIV FOIA & PUBLICATIONS SVCS
TPS-PDR-NUREG
P-211
WASHINGTON DC 20555