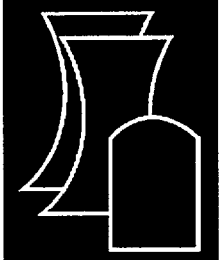
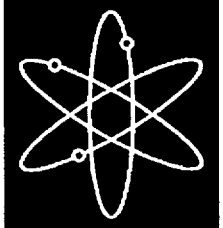
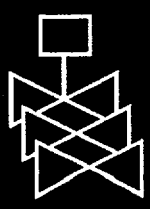
NUREG/CR-6042, Rev. 2
SAND 93-0971







Perspectives on Reactor Safety

ERI Consulting

Sandia National Laboratories

Oak Ridge National Laboratory

U.S. Nuclear Regulatory Commission
Office of Human Resources
Washington, DC 20555-0001

NUREG/CR-6042, Rev. 2, has been reproduced from the best available copy.

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 nuclear safety concepts. The course consists of five modules: (1) the development of safety concepts; (2) severe accident perspectives; (3) accident progression in the reactor vessel; (4) containment characteristics and design basis; 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

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

List of Figures

List of Figures (Cont.)

List of Figures (Cont.)

List of Figures (Cont.)

List of Figures (Cont.)

List of Figures (Cont.)

List of Figures (Cont.)

List of Tables

List of Tables (Cont.)

ACKNOWLEDGMENTS

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, Erick Beckjord, Warren Minners, Jocelyn Mitchell, Tom McKenna, and Jack Lewis.

At Sandia, information and insights were provided by Dana Powers, Jeff LaChance and Donnie Whitehead. Bob Waters and Tim Wheeler provided valuable review comments. Finally, we wish to acknowledge the support of Rebecca Campbell, Emily Preston, Linda Flores, and Annie Valencia 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

1.0 The Development of Safety Concepts, 1946 - 1975

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 arguments 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. To provide a framework for the chapters that follow, a brief history of developments significant to the U.S. regulatory process is presented in Chapters 1 and 2. Trends and events are discussed in roughly the chronological order in which they became significant. Chapter 1 considers the decades preceding the accident at Three Mile Island Unit 2 (TMI-2). Chapter 2 discusses the TMI-2 accident and subsequent events. Several references provide additional information regarding the history of nuclear regulation.[2,3,4,5,6,7,8,9,10]

1.0.2 Learning Objectives for Chapter 1

At the end of this chapter, 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. The 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. Siting Criteria (10 CFR 100)

4. Describe three key conservatisms inherent in traditional design-basis accident analyses.

5. Give examples of accident initiators and multiple failures that would result in beyond-design-basis accidents. Explain why some beyond-design-basis accidents would not be severe accidents

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

7. Describe the level of NRC interest in severe accidents that resulted from the Reactor Safety Study and the Browns Ferry fire.

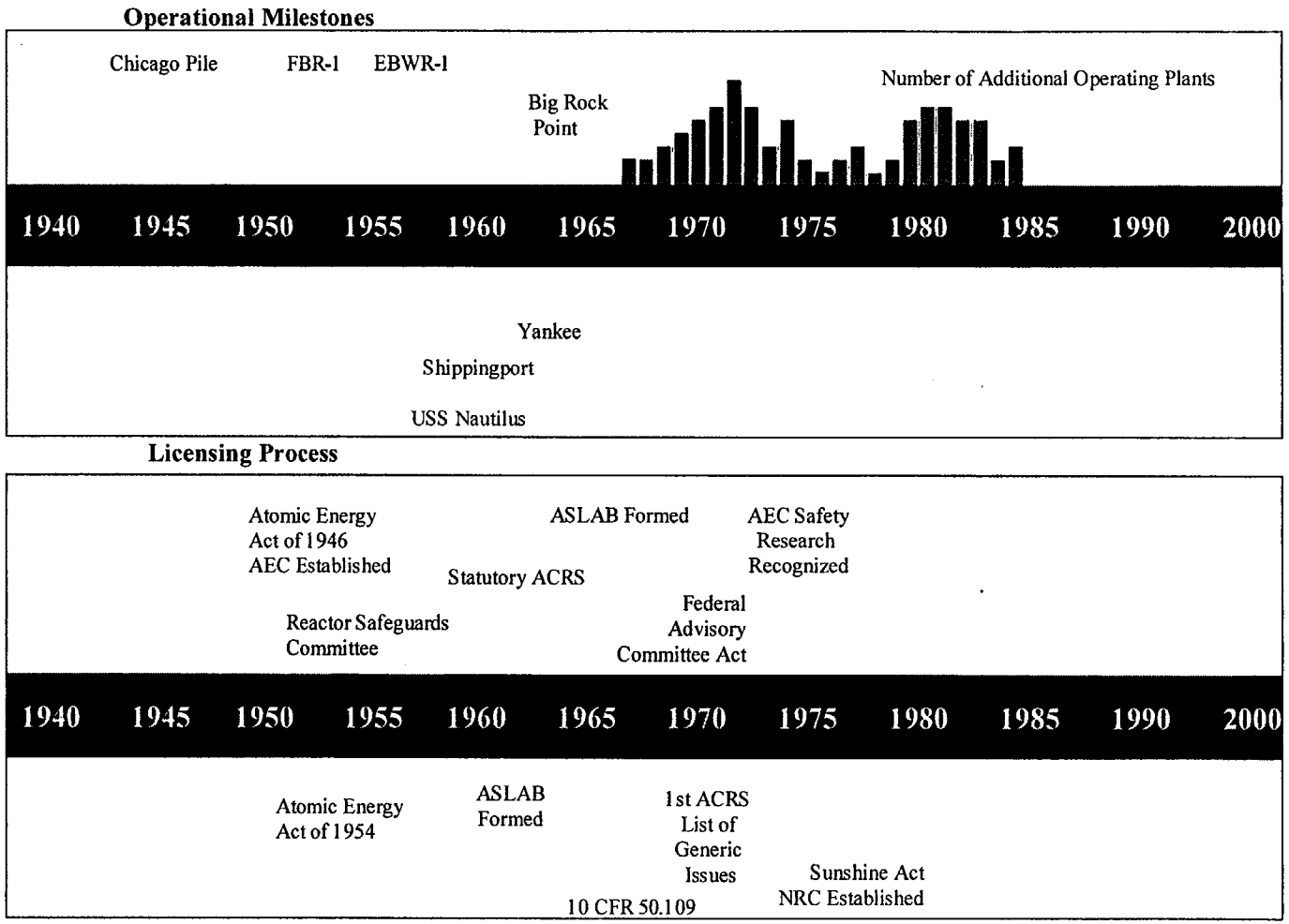
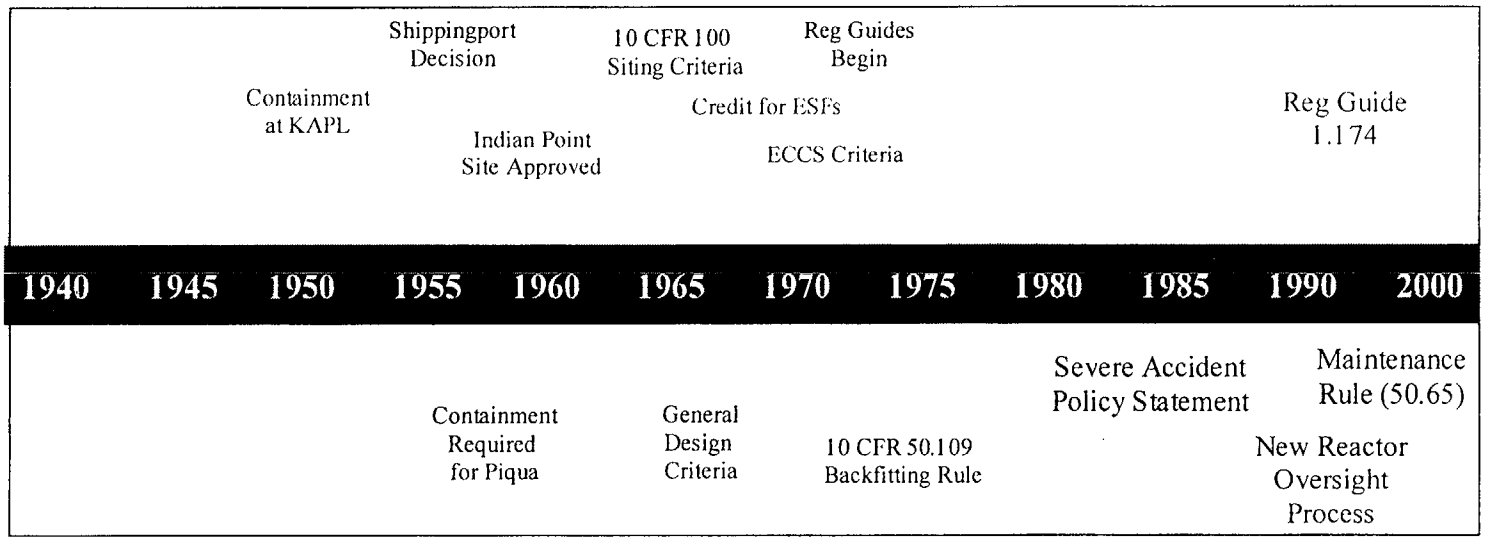


Figure 1.0-1 Timing of major events and activities relevant to commercial power reactor safety from 1940s to present (1 of 3)

Regulatory Decision & Criteria



Siting

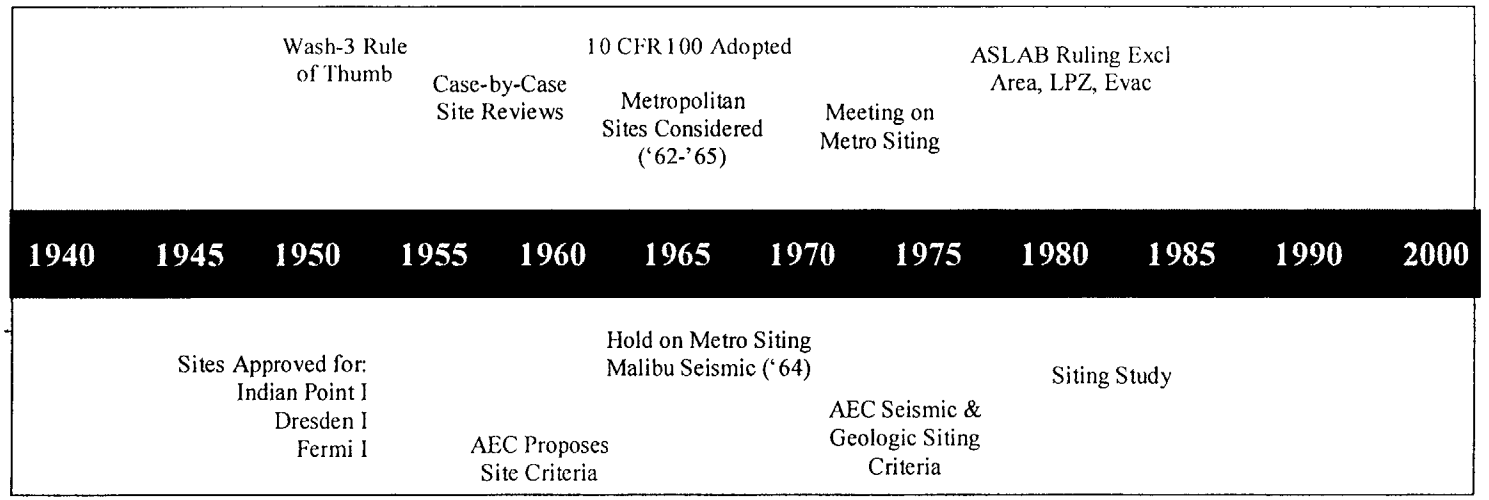


Figure 1.0-1 Timing of major events and activities relevant to commercial power reactor safety from 1940s to present (2 of 3)

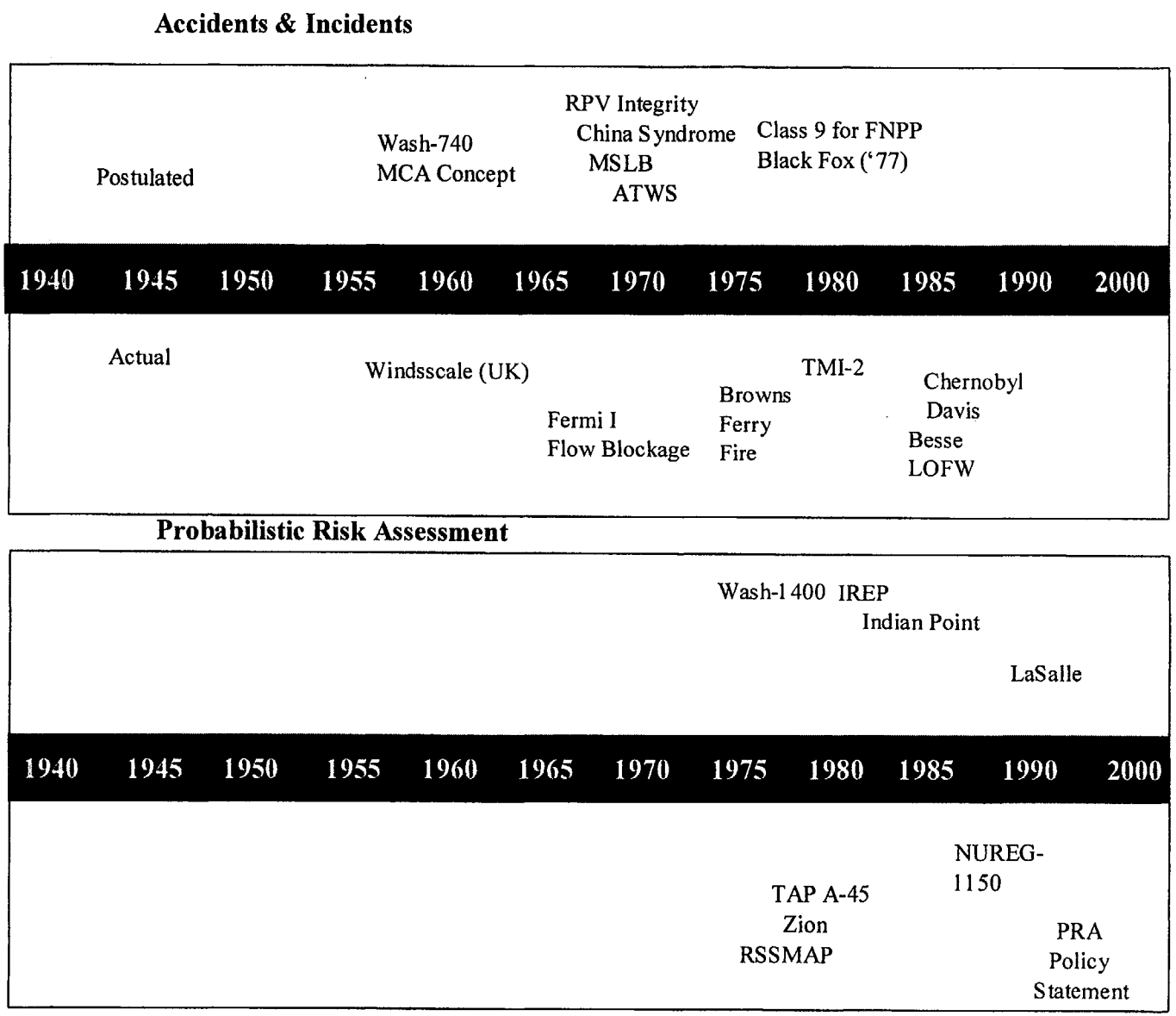


Figure 1.0-1 Timing of major events and activities relevant to commercial power reactor safety from 1940s to present (3 of 3)

References for Section 1.0

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

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, Pennsylvania, 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, Illinois, 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. David Okrent, "Nuclear Reactor Safety: On the History of the Regulatory Process," The University of Wisconsin Press, Madison, Wisconsin, 1981.

7. 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.

8. George T. Mazuzan and Samuel Walker, "Controlling The Atom: The Beginnings of Nuclear Regulation 1946-1962," University of California Press, 1984.

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

10. American Nuclear Society, "Controlled Nuclear Chain Reaction, The First 50 Years," La Grange Park, Illinois, 1992.

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 Remote 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 was related to the reactor thermal power P in kilowatts by the following rule of thumb:

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

or

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

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 30 MWt plant, the rule of thumb gives an exclusion distance of 2.24 miles (3.6 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 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, whereas 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.

The submarine hull provided a containment capability, but to protect the crew, 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 safety 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 shows 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 accident-prevention. Quality control and assurance are emphasized; plant systems and structures are conservatively designed, procured, installed, and inspected; and operators are trained to reduce the likelihood of 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 safety systems 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 containment building is provided to prevent

these radionuclides from escaping the plant. Plants are required to develop accident management programs, which further reduce the likelihood of uncontrolled radionuclide releases during accidents. In spite of these actions, accidental releases are postulated. In siting the reactor, exclusion areas and low population zones (Section 1.2.6) are provided so that potential leakage from the containment can be tolerated without endangering nearby residents. Finally, emergency plans (Sections 2.2.6 and 5.4) 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 of what accident initiators to postulate; what radionuclide releases to postulate; how much credit should be given for removing radionuclides using engineered safety features, 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 sections 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	Thick steel vessels and pipes 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.

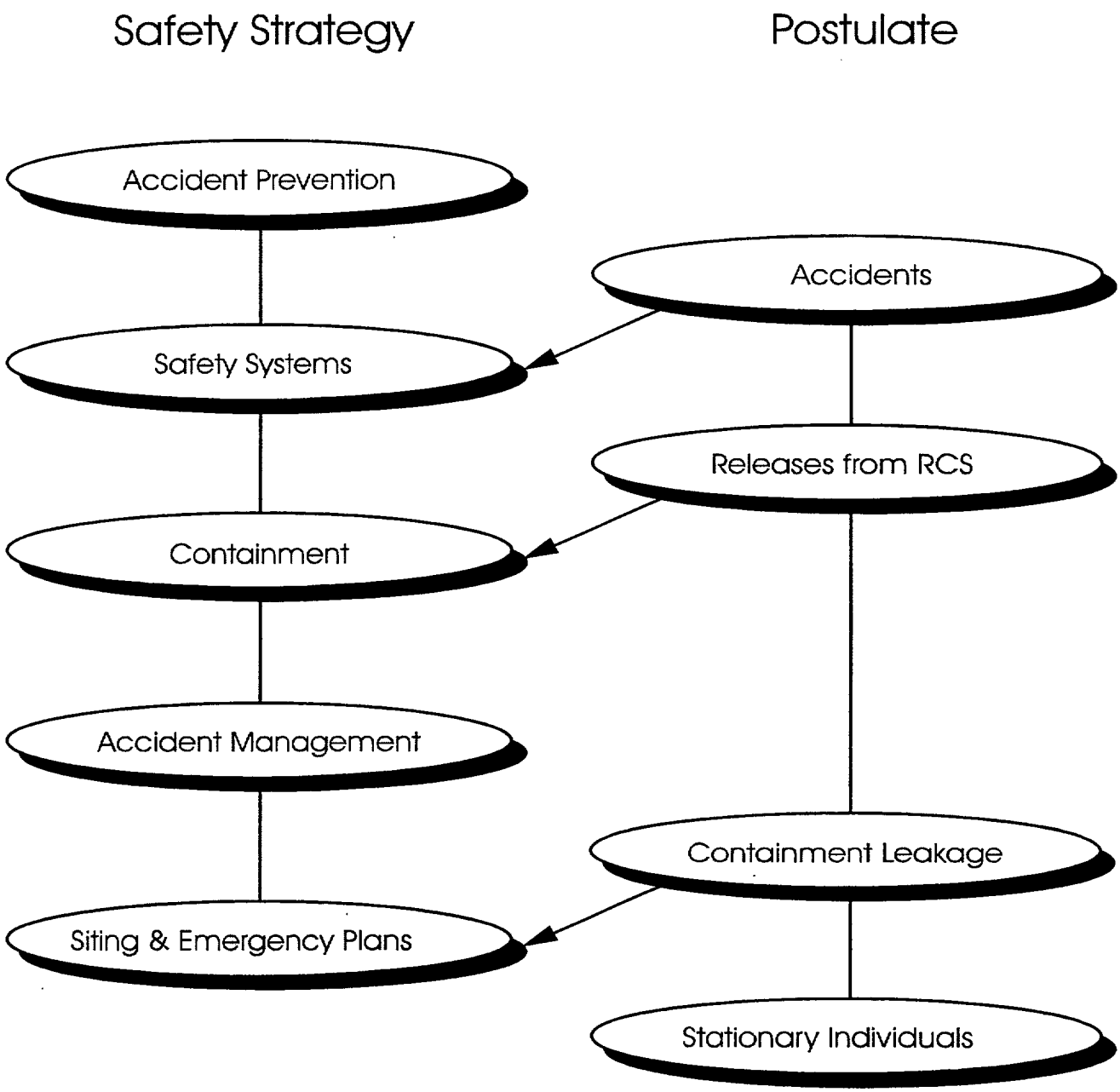


Figure 1.1-1 Defense in depth, safety strategies

References for Section 1.1

1. U.S. Atomic Energy Commission, "Summary Report of Reactor Safeguards Committee," WASH-3, 1950.

2. C. P. Russel, "Reactor Safeguards," p. 19, MacMillan, New York, 1962.

3. Richard G. Hewlett and Francis Duncan, "Nuclear Navy 1946-1962," p. 176, University of Chicago Press, Chicago, Illinois, 1974

1.2 1954-1965 Early Commercial Reactors, Emphasis on Containment

1.2.1 Atomic Energy Act of 1954

In the early 1950s, 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 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 governments 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 nuclear technology. Within a short time the staff drafted rules on radiation protection, distribution and safeguarding of fissionable materials, and the qualification of reactor operators.

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 raised during the reviews of the PRDC application.

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 a house appropriations subcommittee. The subcommittee 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. On the same day, Murray also went to see the chairman of the Joint Committee on Atomic Energy and informed him of the ACRS safety concerns.

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 report. 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 staff 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 Clinton P. 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 been periodically amended, 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 U.S. 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 U.S. 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, 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 failproof. Such perfection 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) or the design-basis loss of coolant accident (LOCA). As discussed in Section 1.4, there is not a single design-basis accident. Plants are designed to withstand a spectrum of postulated accidents. The term siting-basis accident is adopted herein to refer to a design-basis accident that is limiting with respect to site evaluation because it has greater predicted offsite doses than other design-basis accidents. The siting-basis accident is generally initiated by a major reactor-coolant system pipe break.

Rather prescriptive and generally conservative guidance for calculating offsite doses evolved from 10 CFR 100. For example, 10 CFR 100 refers to Technical Information Document (TID) 14844, which postulates that 100% of the noble gas fission products, 50% of the volatile (halogen) fission products, and 1% of the particulates are immediately released to the containment atmosphere following the pipe break.[8,9,10] The TID-14844 release is based on a postulated core melt accident and the 1962 understanding of fission product behavior. (Section 5.1.6 discusses recent revisions to guidance regarding core melt accident releases.) 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 after 10 CFR 100 was issued. 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). The fact that stainless steel, which was used for cladding until the mid-1960s, is considerably less reactive than Zircaloy probably had some influence. Design-basis accident assumptions and calculations are discussed further in Section 1.4. The evolution of hydrogen and the burn that occurred at Three Mile Island Unit 2 are discussed in Sections 2.3 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 doses received) 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 require that uncontained meltdown accidents be postulated.

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 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.[15] The position of the Advisory Committee on Reactor Safeguards was that credit was appropriate for all of the above listed ESFs except the emergency core cooling system. The 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 to build the two-unit Ravenswood plant essentially in the heart of New York City.[3] Double containment was proposed for each of the Westinghouse nuclear steam supply systems and for the common spent fuel storage facility. Even so, both the AEC staff and the ACRS expressed concerns regarding the feasibility of building containments with sufficiently small leak rates. AEC staff calculations indicated that even if all engineered safeguards operated, leakage would have to be limited about 10^{-4} cubic feet per minute in order to meet 10 CFR 100 siting guidelines. In late 1963, Consolidated Edison withdrew its

application for Ravenswood, claiming cheaper power was available from Labrador, 1100 miles away. Metropolitan siting continued to be seriously considered as late as 1970.[3]

References for Section 1.2

1. Union of Concerned Scientists v. U.S. NRC, *Federal Reporter*, 824, 2d series, 108, Washington, DC, 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, Wisconsin, 1981.

4. U.S. Nuclear Regulatory Commission, "A Short History of Nuclear Regulation 1946-1990," NUREG/BR-1075, January 1993.

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

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

7. George T. Mazuzan and 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. *U.S. Code of Federal Regulations* Title 10, Part 100.3 (a), April 1962.

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

13. *U.S. Code of Federal Regulations*, Title 10, Part 100.11 (1)&(2), April 1962.

14. *U.S. Code of Federal Regulations*, Title 10, 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. The first issue concerned reactor pressure vessel integrity. The second was 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 established a special committee to consider reactor pressure vessels in 1955.[2] In March of 1964, 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] Of course plants built to older codes did not benefit from these changes.

As indicated in Figure 1.3-1, reactor vessels are brittle when cold but, as the temperature of reactor vessel material is raised, the toughness increases, slowly at first but rapidly near the reference temperature for nil ductility transition, RT_{NDT}. 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 the reference nil-ductility transition temperature (RT_{NDT}) with irradiation 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. This 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 greatest neutron flux.

Because of the stringent design and surveillance practices applied to reactor pressure vessels in the 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 (ACRS) issued a November 24, 1965 letter.[4] While acknowledging the low probability of reactor

pressure vessel failure, the ACRS letter 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^{-6} 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 (Section 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. Additional information on pressurized thermal shock is presented in the references.[1,6] The regulatory approach that has evolved is aimed at assuring 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. A loss of coolant accident in a 3,200 MWt reactor was analyzed. No credit was given for engineered safety features. BNL 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 ft. (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 *siting-basis accident*, 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 concern that core meltdown could threaten 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 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 were eventually evaluated, and regulated to reduce the probability of core meltdown. Although the new emphasis on prevention gave rise to a greatly expanded list of accidents, until the TMI-2 accident in 1979, the focus was on demonstrating the adequacy of emergency core cooling for such accidents --not on what to do if core cooling failed.

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.[11]

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 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 system; 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,[11] a fact that would be reasserted in the 1975 Reactor Safety Study (Section 1.5) and confirmed by the 1979 accident at Three Mile Island Unit 2 (Section 2.1). 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, and to provide quantitative understanding of the 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 offsite power lines feeding the Dresden 1 plant, which had no on-site emergency AC power. Subsequently, first one small onsite 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.

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.[12] 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).[13] 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 19, 1971 the AEC published a revised set of general design criteria, which became Appendix A of 10 CFR 50.[14] 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 an emergency core cooling system should not fail as a result of a loss of containment integrity.[15] 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 six 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 cannot be discussed here, the five criteria in Category I are worthy of further discussion. These criteria are particularly important and impact many aspects of reactor safety.

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 provide confidence 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 to 10 CFR 50. 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 AEC proposed a new regulation, Appendix B to 10 CFR 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 contains 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 AEC'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 A and B, the AEC 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."[16] This standard was 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.*

Sections 1.4 and 2.5 describe 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. It 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 Browns Ferry Nuclear Power Plant experienced a major fire, resulting in the loss of numerous safety systems. The Browns Ferry fire is discussed at length in Section 1.6. 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."[17] This information was later published as Regulatory Guide 1.120: Fire Protection Guidelines for Nuclear Power Plants.[18]

In 1980 the NRC formally proposed Appendix R to 10 CFR 50 to state the minimum acceptable level of fire protection for power plants operating prior to January 1, 1979. 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.[19] Further, 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
6. jet impingement
7. dynamic loads on components

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 later sections can produce environments exceeding the qualification limits.

In the early 1980s, the NRC began to recognize that devices installed to protect against the dynamic effects of large pipe breaks can have significant safety drawbacks. Pipe whip restraints and jet impingement barriers make access for inservice inspection more difficult and result in higher operational exposures. If these protective devices are removed for inspection and reinstalled, piping or other components may be damaged in the process.

If the protective devices are reinstalled incorrectly, they may impede piping thermal movement and result in overstress. In addition, pipe snubbers can lockup and impede piping thermal movement. As a result, in 1984, Criterion 4 was revised to allow dynamic effects to be excluded from the design basis 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.[20] 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. After the 1975 Browns Ferry fire damaged safety systems at two units (see Section 1.6), new multi-unit sites were designed with complete separation, providing 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. Probabilistic risk assessment 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.

1.3.5 The National Environmental Policy Act (NEPA)

In December 1969 Congress passed the National Environmental Policy Act, which was signed by President Nixon on January 1, 1970. The Act required federal agencies to consider the environmental impact of their activities. The Act was vague and confusing, and it gave federal agencies broad discretion in deciding how to carry out its mandate.

The AEC initially took a narrow view of its responsibilities under the National Environmental Policy Act 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, the AEC did not want to divert 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 additional licensing delays.

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. The AEC also postponed a review of National Environmental Policy Act issues in licensing cases until March 1971.

Environmentalists charged that the AEC had failed to fulfill the purposes of the National Environmental Policy Act 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. 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.*[21]

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 AEC 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."[22]

In response to requirements of the National

Environmental Protection Act (NEPA), the AEC on December 1, 1971 published 10 CFR 51, Licensing and Environmental Policy and Procedures for Environmental Protection.[23] 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 used by some to refer to accidents that involve substantial core damage.

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,[24] that went into effect until further research on emergency core cooling system could be done. These criteria required additional maintenance and monitoring in addition to changes in the emergency core cooling system of some operating reactors.

At the time, generic issues such as emergency core cooling system 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.[25]

In 1973, before the "final criteria" were issued, a second series of experiments was completed. These tests were called 1½ semiscale because a loop simulating the unbroken loops of a reactor was added to the ½ (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, 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 computational restraints, some of which are:

- A multiplier of 1.2 on the decay heat rate,
- the assumption that the cladding oxidation rate is not limited by the predicted availability of steam,
- 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 20 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. The rule was approved by the NRC in September 1988.[26] 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 and 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 1960s 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.

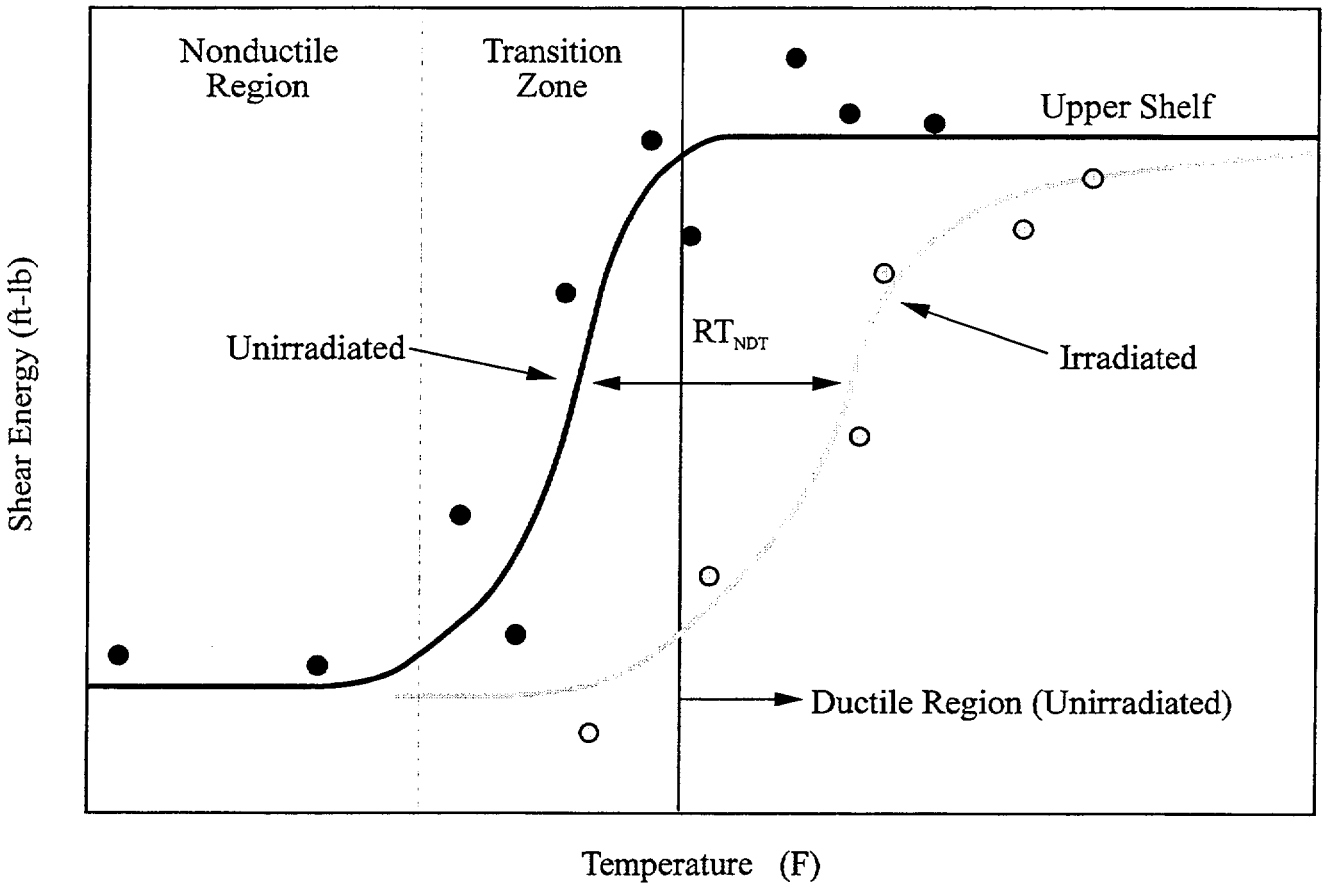


Figure 1.3-1 Shift of nil-ductility transition temperature

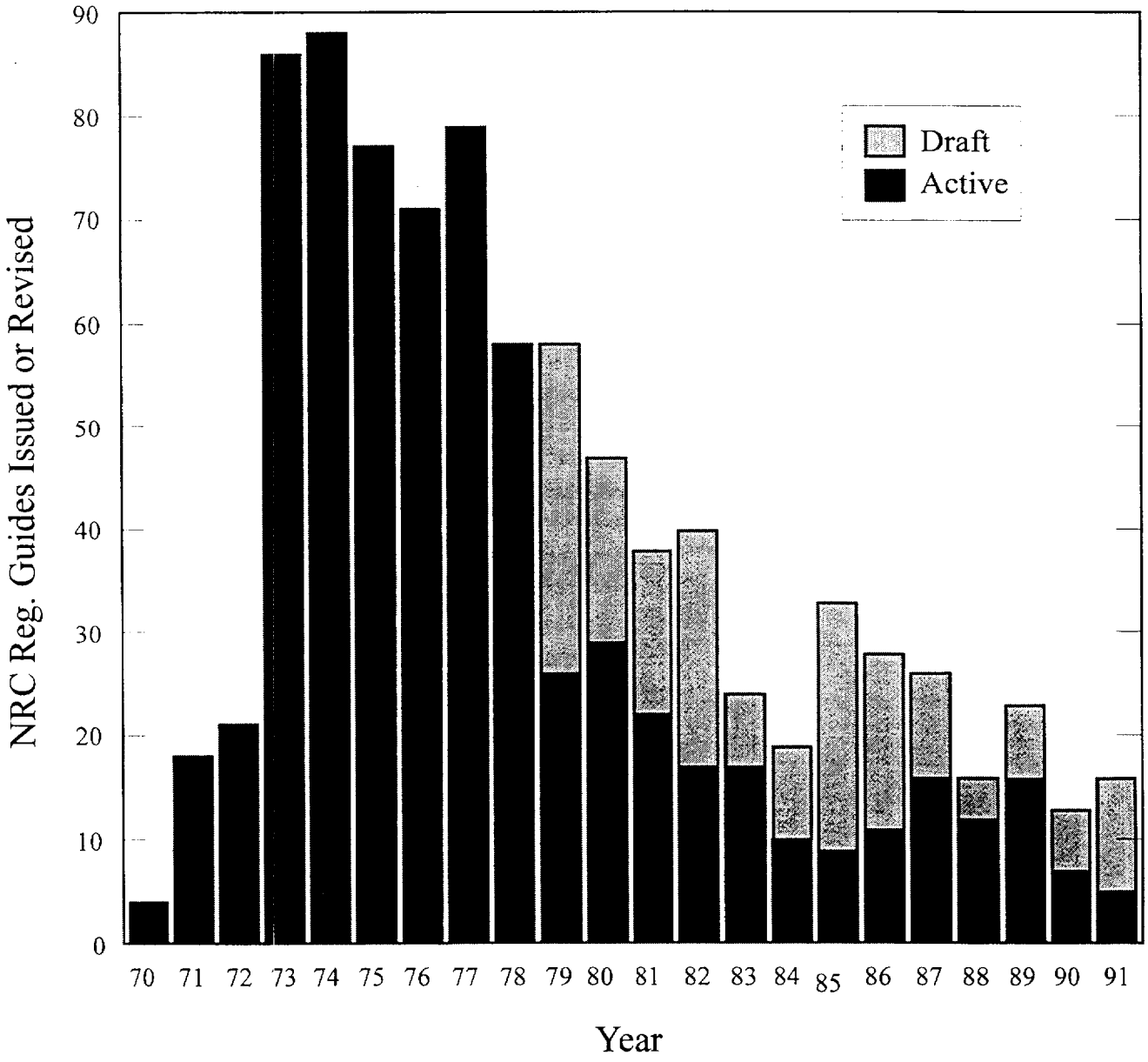


Figure 1.3-2 Number of regulatory guides issued per year

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, p. 37.

2. George T. Mazuzan and Samuel Walker, "Controlling The Atom: The Beginning of Nuclear Regulation 1946-1962," University of California Press, 1984, p. 217.

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

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, pp. 88-89.

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. *U.S. Code of Federal Regulations,* "Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events," Title 10, Part 50.61.

8. Advisory Committee on Reactor Safeguards, *Minutes of June 3, 1966 Subcommittee Meeting*, 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, Wisconsin, 1981, pp. 112-121.

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

11. Eric S. Beckjord, U.S. Nuclear Regulatory Commission Memorandum, February 28, 1992.

12. U.S. Atomic Energy Commission, "Proposed General Design Criteria for Construction Permits for Nuclear Power Plants," *Federal Register*, November 22, 1965.

13. U.S. Atomic Energy Commission, "Proposed General Design Criteria for Nuclear Power Plants," *Federal Register,* July 10, 1967.

14. *U. S. Code of Federal Regulations,* "General Design Criteria for Nuclear Power Plants," Title 10, Part 50, Appendix A, *Federal Register*, February 19, 1971.

15. U.S. Atomic Energy Commission, "Net Positive Suction Head for Emergency Core Cooling Containment Heat Removal," Safety Guide 1.1, November 1970.

16. American National Standards Institute, "Quality Assurance Program Requirements for Nuclear Power Plants," ANSI N45.2.

17. U.S. Nuclear Regulatory Commission, "Guidelines for Fire Protection for Nuclear Power Plants," Auxiliary Power Conversion Systems Branch Technical Position 9.5-1, 1975.

18. U.S. Nuclear Regulatory Commission, "Fire Protection Guidelines for Nuclear Power Plants," Regulatory Guide 1.120, draft for comment, June 1976.

19. *U. S. Code of Federal Regulations,* "Fire Protection Program for Nuclear Power Plants Operating Prior to January 1, 1979," Title 10, Part 50, Appendix R.

20. U.S. Nuclear Regulatory Commission, "Motor-Operated Valve Common Mode Failures During Plant Transients Due to Improper Switch Settings," Inspection Enforcement (IE) Bulletin No. 85-03, 1985.

21. 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 George T. Mazuzan and Roger R. Trask, 1979, p. 68.

22. 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, 1991, p. 34.

23. *U. S. Code of Federal Regulations,* "Licensing and Regulatory Policy and Procedures for Environmental Protection," Title 10, Part 51.

24. George T. Mazuzan and Roger R. Trask, "An Outline History of Nuclear Regulation and Licensing 1946-1979," Historical Office, Office of the Secretary, U.S. Nuclear Regulatory Commission, 1979, p. 71.

25. *U.S. Code of Federal Regulations,* "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled Nuclear Power Reactors," Title 10, Part 51.46.

26. *U. S. Code of Federal Regulations,* "Emergency Core Cooling Systems; Revisions to Acceptance Criteria,"Title 10, Part 50.46.

1.4 Design Basis Perspectives

1.4.1 Safety Analysis Report Requirements

As discussed in Section 1.2.2, the initial applications to build commercial nuclear power plants were received and reviewed by the AEC in 1955 and 1956. Title 10 Part 50, Domestic Licensing of Production and Utilization Facilities, was added to the Code of Federal Regulations in January 1956. From the outset, the preliminary and final safety analysis reports were the main documents reviewed by the AEC (and later the NRC) in deciding whether to grant construction permits and operating licenses.

Requirements regarding the submittal and content of safety analysis reports were first issued as 10 CFR 50 Section 50.34 in December of 1970.[1] Additional guidance was later provided in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants."[2] Table 1.4-1, which is based on this Regulatory Guide, indicates the major topics treated in the safety analysis reports. The NRC reviews safety analysis reports to determine whether plants 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, "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 an applicant's Safety Analysis Report provides information on the geology, seismology, hydrology, and meteorology of the site and vicinity. It also provides information regarding nearby industrial, military, and transportation 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. The seismic design basis is discussed further in subsection 1.4.4.

Table 1.4-2 is a list of potential accident-initiating events (initiators) that applicants are requested to address in Chapter 15 of the Safety Analysis Report. Regulatory Guide 1.70 asks that the potential causes of each of these initiators be identified and that the estimated frequency of occurrence of each 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 1.4-2, the potential exists for the release of radionuclides from successive barriers (fuel, cladding, 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] Conversely, a *design-basis accident (DBA)* is a postulated set of failure events that a facility is designed and built to withstand without exceeding the offsite exposure guidelines of

the NRC's siting regulation (10 CFR 100).

The assumptions used to delineate and analyze DBAs are based on NRC regulations and guidelines that evolved as numerous applications for construction permits and operating licenses were reviewed. Some DBAs are analyzed in detail in the Safety Analysis Report in order to (a) bound the offsite doses for DBAs in each of the eight initiation categories of Table 1.4-2, and (b) demonstrate the adequacy of key engineered safety features, in particular, the emergency core cooling system and containment. Each of the analyzed DBAs invariably postulates at least one significant failure of a component (or operator) to perform an intended safety function. Generally, equipment failures beyond those consistent with loss of electric power and single failure criteria 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 1.4-2) are treated as DBAs. Anticipated transients without scram are discussed separately in Sections 2.4, 2.5 and Appendix 2B.

1.4.2 Siting-Basis Accident

The siting-basis accident is the DBA that results in the greatest calculated offsite doses. For U.S. light water reactors the siting-basis accident is generally a large pipe-break LOCA. Large pipe-break LOCAs are postulated as DBAs in spite of extensive design, construction, testing, inspection, operations, and maintenance measures taken to prevent them. In design-basis LOCAs, a coincident loss of offsite power is postulated and the single-failure criterion is then applied, which usually leads to the assumption that one of the emergency diesel generators fails to start. This implies the loss of one out of two AC-powered trains in various safety systems.

A spectrum of break locations and sizes is considered, including hypothetical severance of the largest pipe in the reactor coolant 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."

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. Some of the steam resulting from this expulsion would pressurize the containment; the rest would be condensed on structures or by engineered safety features. In PWR containments, cold water sprays and/or ice racks are provided to condense steam blowdown. In BWR containments, 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 design-basis 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 1.4-1. 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 an energetic chemical reaction 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 would 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 chapters.

The emergency core cooling system (ECCS) is designed to limit the extent of core damage in postulated design-basis LOCAs. 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.

In determining the acceptability of an ECCS, the NRC reviews design-basis LOCA calculations performed by the applicant, and compares the results to the ECCS acceptance criteria specified in 10 CFR 50.46 (see Section 1.3.6).[5] The quantitative ECCS acceptance criteria (e.g., the cladding temperature shall not exceed 2200°F) do not represent threshold levels. That is, exceeding a quantitative acceptance criterion would not result in an immediate public safety problem. What the success criteria 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 LOCA occurs."[6]

1.4.3 Realism of Design-Basis Accident Analyses

Table 1.4-3 compares realistic assumptions for large-break LOCAs to corresponding assumptions postulated in design-basis analyses. As indicated, the assumptions postulated in design-basis analyses are generally conservative. To illustrate, a typical calculation of peak cladding temperature based on the conservative assumptions of 10 CFR 50 Appendix K is provided in Figure 1.4-2. As indicated in Table 1.4-3, decay heat is conservatively multiplied by a factor of 1.2 in Appendix K calculations. Figure 1.4-2 illustrates that relaxing this conservatism alone can reduce the predicted peak cladding temperature by several hundred degrees.[7]

In September 1988, 10 CFR 50.46 was 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 design-basis LOCAs 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 given that the ECCS acceptance criteria must be met. 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 failed, thereby permitting significant core melting.

One of the most significant barriers to accidental releases of fission products from a nuclear power plant is the containment. The containment is designed to have a very low leakage rate when subjected to the maximum internal pressures predicted for design-basis accidents. The internal pressure following a pipe break inside containment peaks and then begins to decrease rapidly when the rate of energy addition to the containment atmosphere by blowdown falls below the rate of energy removal by internal structures, containment sprays, fan coolers, ice beds, or suppression pools. For accident calculations, however, the containment is conservatively (as if the pressure did not decrease) assumed to leak at a constant rate called the design-basis leak rate for the first 24 hours and at 50% of that rate for the remaining duration of the accident.

DBA 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.

In DBA analyses, radiation doses at the exclusion-area and low-population-zone boundaries are calculated assuming that the accident occurs when meteorological conditions are worse (from the standpoint of 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 1.4-4 presents typical conservative estimates of offsite doses for several DBAs. Even with the very conservative assumptions employed, the calculated doses that a person out-of-doors in the vicinity of the plant might receive for the entire course of a design basis accident are usually well below the 10 CFR Part 100 guidelines.

The radiological consequences that might realistically result from nuclear power plant accidents have been explored in connection with environmental evaluations. Table 1.4-5 presents some realistic dose estimates obtained for typical PWR events and accidents. Note that the realistic exclusion radius dose for a large LOCA in which ECCS acceptance criteria are met is over two orders of magnitude less than the corresponding conservatively calculated dose estimate in Table 1.4-4.[6] Realistically, meeting the ECCS acceptance criteria would prevent the core from melting, and far less than 25% of the radioactive iodine inventory would escape from the fuel to the reactor containment.

In summary, conservative estimates of DBA radiation doses to the public are below 10 CFR Part 100 guidelines, and realistic estimates of DBA doses are much lower. This is not to say that accidents resulting in doses exceeding Part 100 guidelines are impossible; however, such accidents would have to involve initiating events, phenomena, component failures, or operator errors not postulated for DBAs in order to cause

a. ECCS failure leading to core melting and the release of significant quantities of radionuclides from the fuel to containment, and

b. breach or bypass of containment leading to the release of significant quantities of radionuclides to the environment.

To illustrate, some events and phenomena that are not considered in design-basis LOCA analyses include: reactor pressure vessel rupture as an initiator or as a result of pressurized thermal shock (Section 1.3.1); dynamic effects (e.g., pipe whip, jet impingement, and asymmetric loads on reactor vessel internals) exempted with NRC approval as permitted under GDC-4 (Section 1.3.4.2); delayed versus prompt loss of offsite power; multiple failures leading to total loss of AC power; failure of the containment isolation system; and pipe breaks resulting in containment bypass. To assess the likelihood and consequences of such events and phenomena both deterministic and probabilistic analyses may be performed (see Sections 1.5 and 2.5); but such analyses are not required in the licensee's Safety Analysis Report.

1.4.4 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.

The severity of seismic events is usually referenced on one of two scales. Historical observations regarding earthquake magnitudes are categorized according to the *Modified Mercalli Intensity* scale, which indicates damage done on a scale from 1 (not felt) to 12 (nearly total damage) as indicated in Table 1.4-6. The Mercalli categories are also referenced to the maximum acceleration in units of standard gravitational force (g). Measurements of energy releases in earthquake, which generally date from the 1930s, are based on the logarithmic *Richter* scale. A rough comparison of the two scales is provided Table 1.4-6; however, because the amount of damage for a given seismic energy release depends on soil characteristics, the nature of the underlying bedrock, and the type of building construction, an exact correspondence between the Mercalli and Richter scales does not exist.

Postulated earthquake magnitudes for a given site are derived from knowledge of proximity to known active faults and historic earthquake activity. Figure 1.4-3 shows a map of seismic activity for the contiguous United States. The relationship of the four zone designations to the Mercalli intensities is indicated.

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 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. Ultimately this draft evolved into Appendix A to 10 CFR Part 100.[11]

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) establishes the vibratory ground motion 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 is required after the event. If the earthquake exceeds the magnitude of the OBE, the plant must be shut down and can not be restarted until inspections and evaluations confirmed that it would be safe to do so.

The safe shutdown earthquake (SSE) establishes 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 following a SSE are designated Seismic Category I.[12] These features include those 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.*[11]

By a combination of structural analysis and testing, plant structures and equipment important to safety are built to survive the SSE. Seismic analyses of structures, systems, and components are discussed in Safety Analysis Report Sections 3.7 and 3.8, and guidance regarding seismic 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 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 (see Section 1.5) 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.

Appendix A to 10 CFR Part 100 requires that the maximum vibratory ground motion of the OBE be one-half that of the SSE. It further requires suitable dynamic analyses or qualification tests to demonstrate that structures, systems, and components necessary for continued safe operation are capable of withstanding the effects of the OBE. 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. In 1996, Appendix S to 10 CFR 50 was issued. It allows the OBE ground motion for new plant designs to be set in either of two ways:[13]

a. one-third or less of the SSE ground motion, in which case OBE requirements can be satisfied without an explicit response or design analyses being performed, or

b. a value greater than one-third of the SSE ground motion, in which case analysis and design are required.

In either case, the plant must still be shut down for inspection if the OBE is exceeded.

Table 1.4-1 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 1.4-2 Representative initiating events to be analyzed in Section 15.X.X of the Safety Analysis Report

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 1.4-2 Representative initiating events to be analyzed in Section 15.X.X of the Safety Analysis Report (Cont.)

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 partial 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 1.4-2 Representative initiating events to be analyzed in Section 15.X.X of the Safety Analysis Report (Cont.)

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.

8. Anticipated Transients Without SCRAM

8.1 Inadvertent control rod withdrawal.

8.2 Loss of feedwater.

8.3 Loss of AC 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 1.4-3 Partial comparison of realistic assumptions with conservative assumptions for design-basis LOCA calculations

Realistic Assumptions	Conservative Assumptions
Accident Initiation	
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 line.
System/Component Reliability	
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.
Reactor Power	
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. A conservative estimate of decay heat is multiplied by a factor of 1.2.
ECCS and Containment ESFs	
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 1.4-3 Partial comparison of realistic assumptions with conservative assumptions of design-basis LOCA calculations (Cont.)

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 radio-active 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 1.4-4 Conservative offsite doses from design-basis accident analyses*

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

*From WASH-1250

Table 1.4-5 Realistic offsite doses due to releases at a typical PWR*

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 person-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).

Table 1.4-6 Approximate Relationship between Modified Mercalli and Richter Seismic Classifications

Modified Mercali intensity scale	Description of effects[1]	Maximum acceleration (g)	Richter magnitude	Energy release (ergs)
I	Not felt; marginal and long-period effects of large earthquakes evident		M2	10^{14}
II	Felt by persons at rest, on upper floors, or favorably placed			10^{15}
III	Felt indoors; hanging objects swing; vibration like passing of light trucks occurs; duration estimated; might not be recognized as an earthquake	0.003 to 0.007	M3	10^{16}
IV	Hanging objects swing; vibration occurs that is like passing of heavy trucks, or there is a sensation of a jolt like a heavy ball striking the walls; standing motor cars; rock; windows, dishes and doors rattle, glasses clink; crockery clashes, in the upper range of IV, wooden walls and frame creak	0.007 to 0.015	M4	10^{17}
V	Felt outdoors; duration estimated; sleepers waken; liquids become disturbed, some spill; small unstable objects are displaced or upset; doors swing, close, and open shutters and pictures move; pendulum clocks stop, start, and change rate	0.015 to 0.03		10^{18}
VI	Felt by all; many are frightened and run outdoors; persons walk unsteadily, windows, dishes, glassware break; knickknacks, books, etc., fall off shelves; pictures fall off walls; furniture moves or overturns; weak plaster and masonry D crack; small bells ring (church, school); trees, bushes shake	0.03 to 0.09	M5	10^{19}
VII	Difficult to stand; noticed by drivers of motor cars; hanging objects quiver,; furniture breaks; damage occurs to masonry D, including cracks; weak chimneys beak at roof line; plaster, loose bricks, stones, tiles, cornices fall; some cracks appear in masonry C; waves appear on ponds, water turbid with mud; small slides and caveins occur along sand or gravel banks; large bells ring	0.07 to 0.22	M6	10^{20}
VIII	Steering of motor cars affected; damage occurs to masonry C, with partial collapse; some damage occurs to masonry B, but none to masonry A; stucco and some masonry walls fall; twisting, fall of chimneys, factory stacks, monuments, towers, and elevated tanks occur; frame houses move on foundations if not bolted down; loose panel walls are thrown out; changes occur in flow or temperature of springs and wells; cracks appear in wet ground and on steep slopes	0.15 to 0.3		10^{21}
IX	General panic, masonry D is destroyed; masonry C is heavily damaged, sometimes with complete collapse; masonry B is seriously damaged; general damage occurs to foundations; frame structures shift off foundations, if not bolted; frames crack; serious damage occurs to reservoirs; underground pipes break; conspicuous cracks appear in ground, sand and mud ejected in alluviated areas; earthquake fountains and sand craters occur	0.3 to 0.7	M7	10^{22}
X	Most masonry and frame structures are destroyed, with their foundations; some well-built wooden structures and bridges are destroyed; serious damage occurs to dams, dikes, and embankments; large landslides occur; water is thrown on bank of canals, rivers, lakes, etc.; sand and mud shift horizontally on beaches and flat land; rails are bent slightly	0.45 to 1.5	M8	10^{23}
XI	Rails are bent greatly; underground pipelines are completely out of service	0.5 to 3	M9	10^{24}
XII	Damage nearly total; large rock masses are displaced; lines of sight and level are distorted; objects are thrown into air	0.5 to 7		

[1]Masonry A: A good workmanship, mortar, and design; reinforced, especially laterally, and bound together by using steel, concrete, etc; designed to resist lateral forces; Masonry B: Good workmanship and mortar: reinforced, but not designed in detail to resist lateral forces; Masonry C: Ordinary workmanship and mortar; no extreme weaknesses like failing to tie in at corners, but neither reinforced nor designed against horizontal forces; Masonry D: Weak materials, such as adobe; poor mortar; low standards of workmanship; weak horizontally.

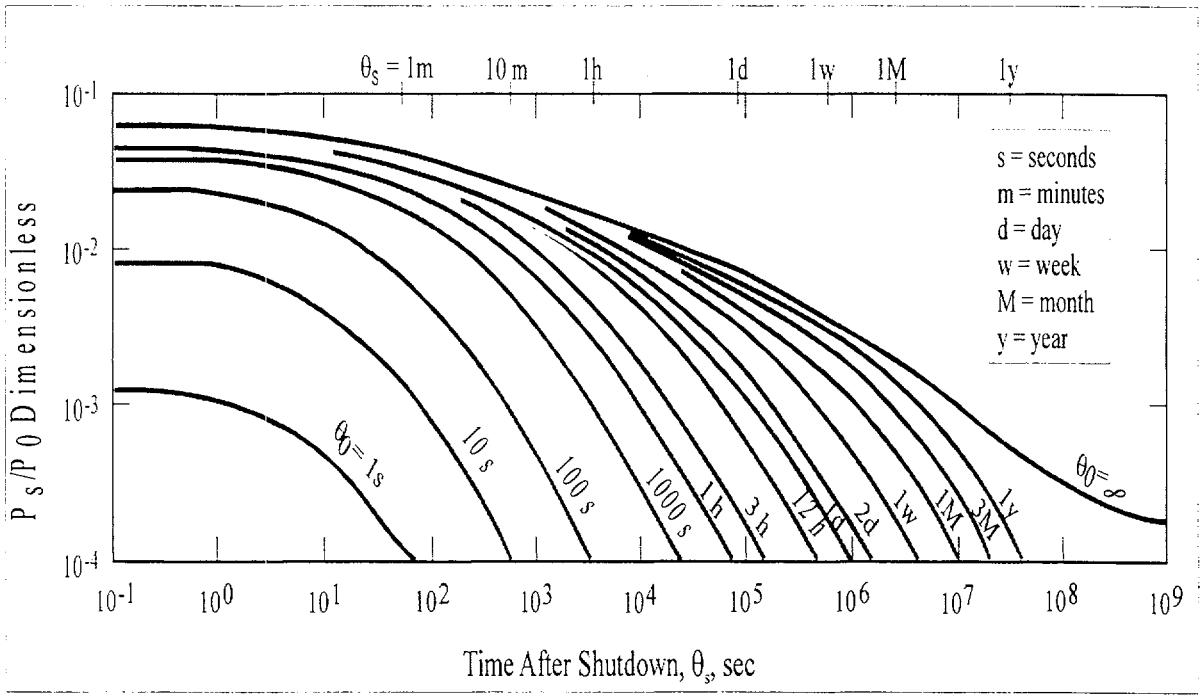


Figure 1.4-1 Ratio of power after to power before shutdown (P_s/P_o) for various operation times before shutdown

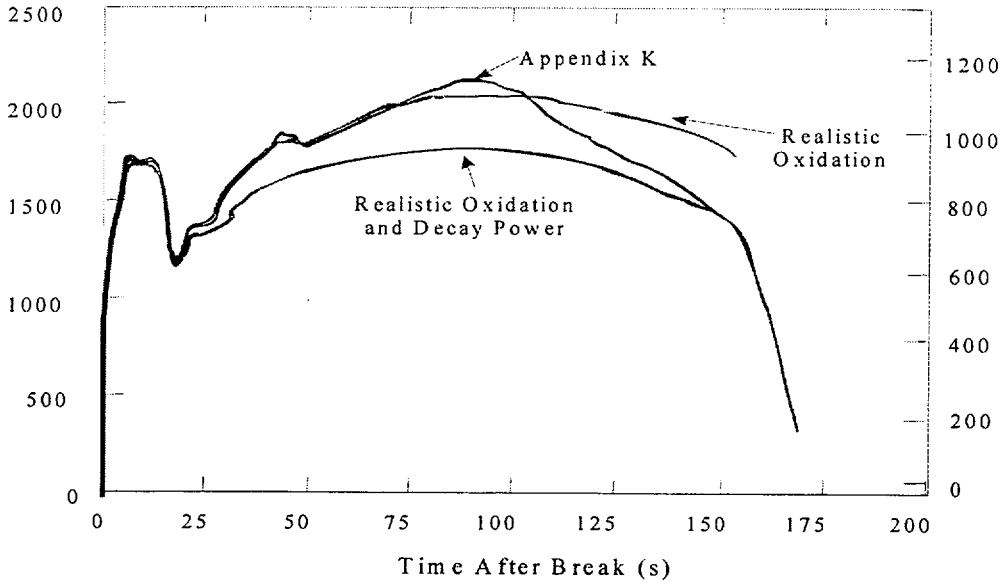
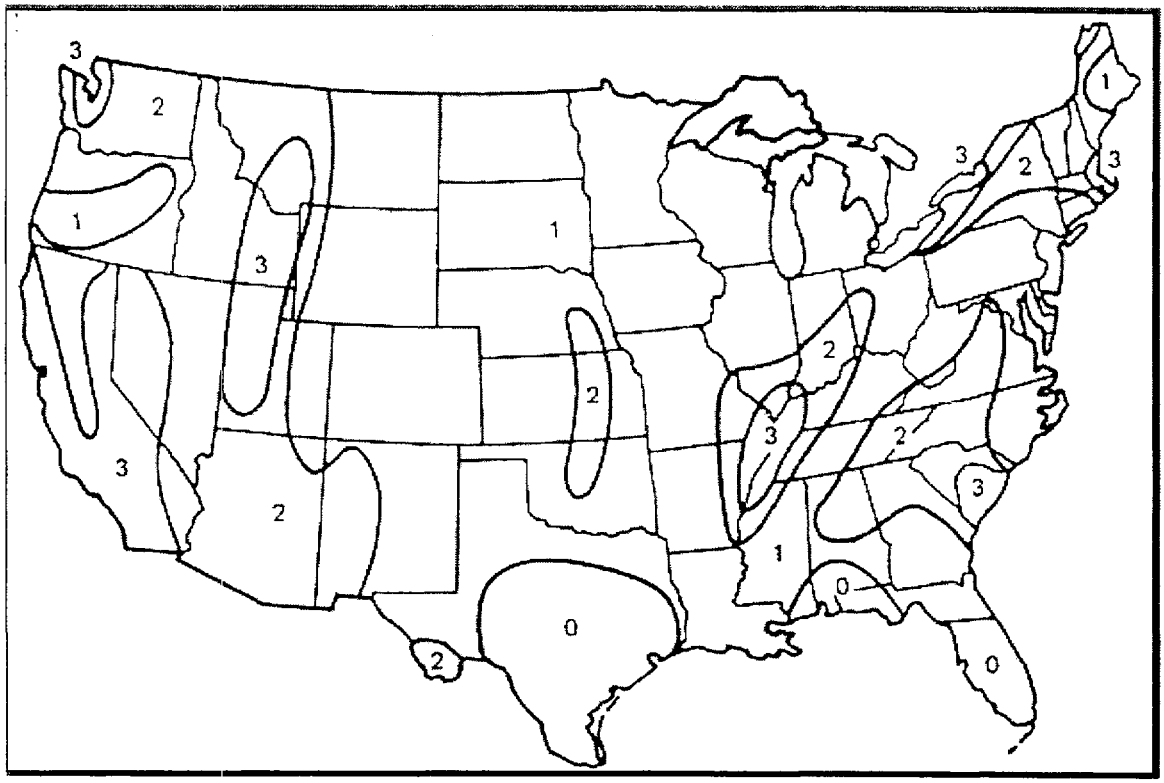


Figure 1.4-2 Effect of selected conservatisms on peak cladding temperature



Zone 0 – No damage
Zone 1 – Minor damage, intensities V and VI of the Modified Mercalli scale
Zone 2 – Moderate damage, intensity VII of the Modified Mercalli scale
Zone 3 – Major damage, intensity VII and higher of the Modified Mercalli scale

Figure 1.4-3 Seismic Risk Map for the contiguous United States

References for Section 1.4

1. *U.S. Code of Federal Regulations,* Title 10, Part 50.34, December 23, 1999.

2. U.S. Nuclear Regulatory Commission Regulatory Guide 1.70, Rev. 3, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants", November 1978.

3. U. S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800, Rev. 2, July 1981.

4. *U. S. Code of Federal Regulations,* Title 10, Part 100.11(a), Footnote 1, September 9, 1999.

5. *U. S. Code of Federal Regulations,* Title 10, Part 50.46 (b), November 3, 1997.

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. *U. S. Code of Federal Regulations,* Title 10, Part 100, Appendix A, January 1, 1990.

12. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.29, "Seismic Design Classification," Rev. 3, September 1978.

13. *U. S. Code of Federal Regulations*, Draft Title 10, Part 50, Appendix S, "Earthquake Engineering Criteria for Nuclear Power Plants," December 1996.

1.5 The Reactor Safety Study

1.5.1 Beyond-Design-Basis Accidents

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] WASH-1250 provided factual information regarding the conservatisms applied in the design of nuclear power plants. It did not, however, address the likelihood or potential consequences of *beyond-design-basis accidents,* which involve more serious initiating events or more failures following initiation than the accidents analyzed in the Safety Analysis Report. Beyond-design-basis accidents include those initiated by reactor pressure vessel rupture, those initiated by seismic events more severe than the safe shutdown earthquake, and those involving multiple component failures or operator errors after initiation, that is, failures beyond those postulated under the single failure criteria.

Figure 1.5-1 illustrates a breakdown of nuclear power plant accidents according to their severity. 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);[3] that is, 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 Section 1.4, 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 Safety Analysis Report for design-basis LOCAs. 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. That is, the accidents with the greatest potential public consequences are uncontained severe accidents.

In this light, several questions had to be addressed in order to respond to Senator Pastore's request for a comprehensive assessment of reactor safety. What accidents could result in significant core damage and containment breach or bypass? How likely are these accidents? What would be their health and economic consequences? These are fundamental questions that WASH-1250

did not address. Such questions are addressed in probabilistic risk assessments, but, 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.[4] In retrospect, this was a highly optimistic estimate, but it typifies the degree to which meltdown accidents were considered "not credible."

1.5.2 The Study

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.

The team attempted to make a realistic estimate of the potential effects of light water reactor accidents on the public health and safety. One BWR, Peach Bottom Unit 2, and one PWR, Surry Unit 1, were analyzed in detail to estimate the likelihood and consequences of potential accidents.

The team adapted methods previously used by the Department of Defense and NASA to predict the effect of failures of small components in large, complex systems. The overall methodology, which is still utilized, is called probabilistic risk assessment (PRA). A tutorial on PRA methods and terminology is included as Appendix 2A.

The team first identified events that could potentially lead to core damage. 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 public health and economic consequences of the identified severe accidents were estimated using computational models that were developed as part of the overall effort.

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 by the NRC in October 1975.[5]

1.5.3 Findings

The Reactor Safety Study indicated that risks to the public from potential U.S. nuclear power plant 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 1.5-2 and 1.5-3 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 1.5-2, 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 (approximately 5×10^{-5} per reactor year for Surry and Peach Bottom), and that light water reactor risks are mainly attributable to core melt accidents. The Reactor Safety Study also demonstrated the wide variety of accident sequences (initiators and ensuing 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).

1.5.4 Impact

The preceding findings have withstood the test of time; however, the Reactor Safety Study received 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.[6] 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.[7]

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.

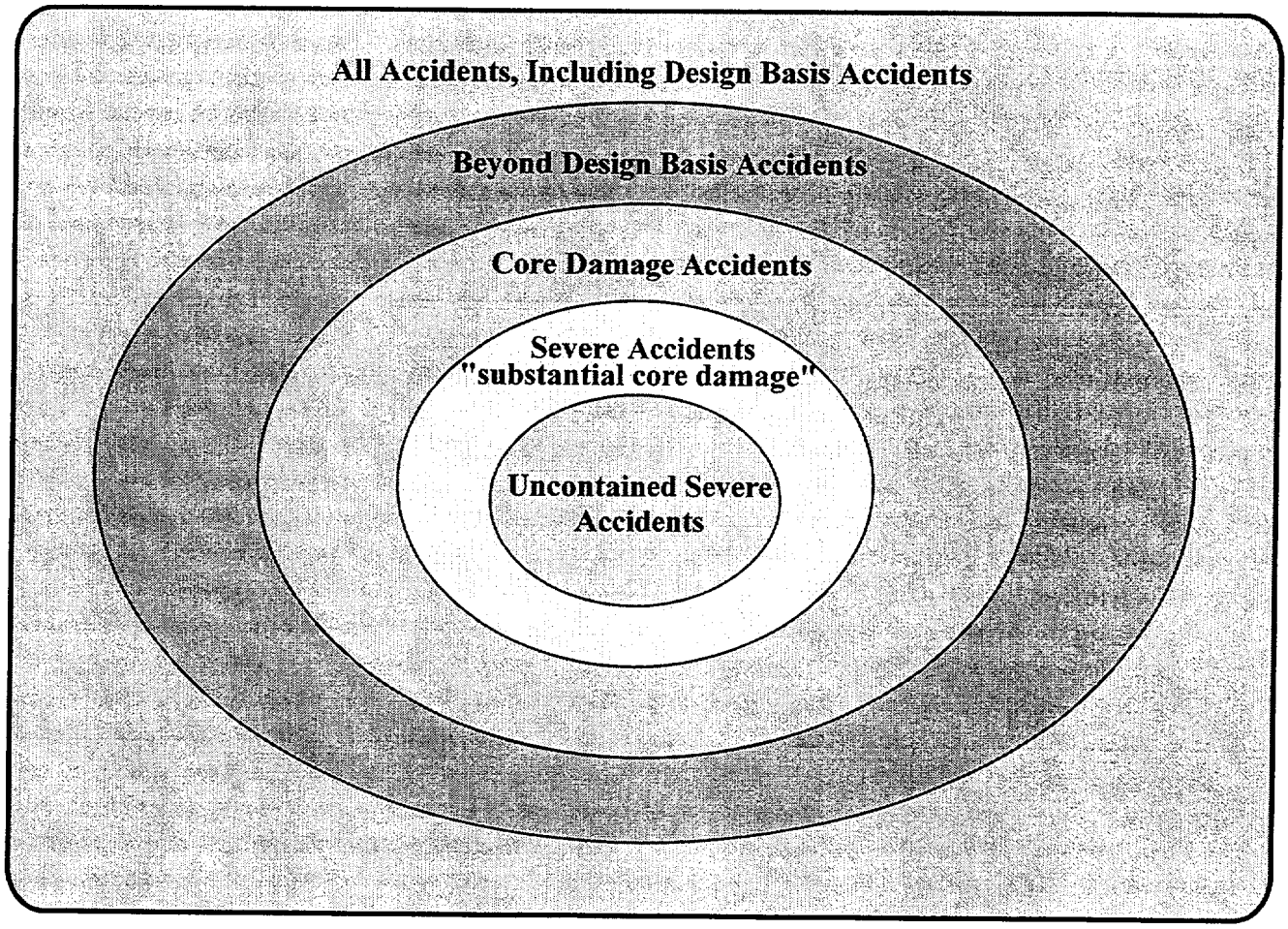


Figure 1.5-1 Breakdown of nuclear power plant accidents by severity

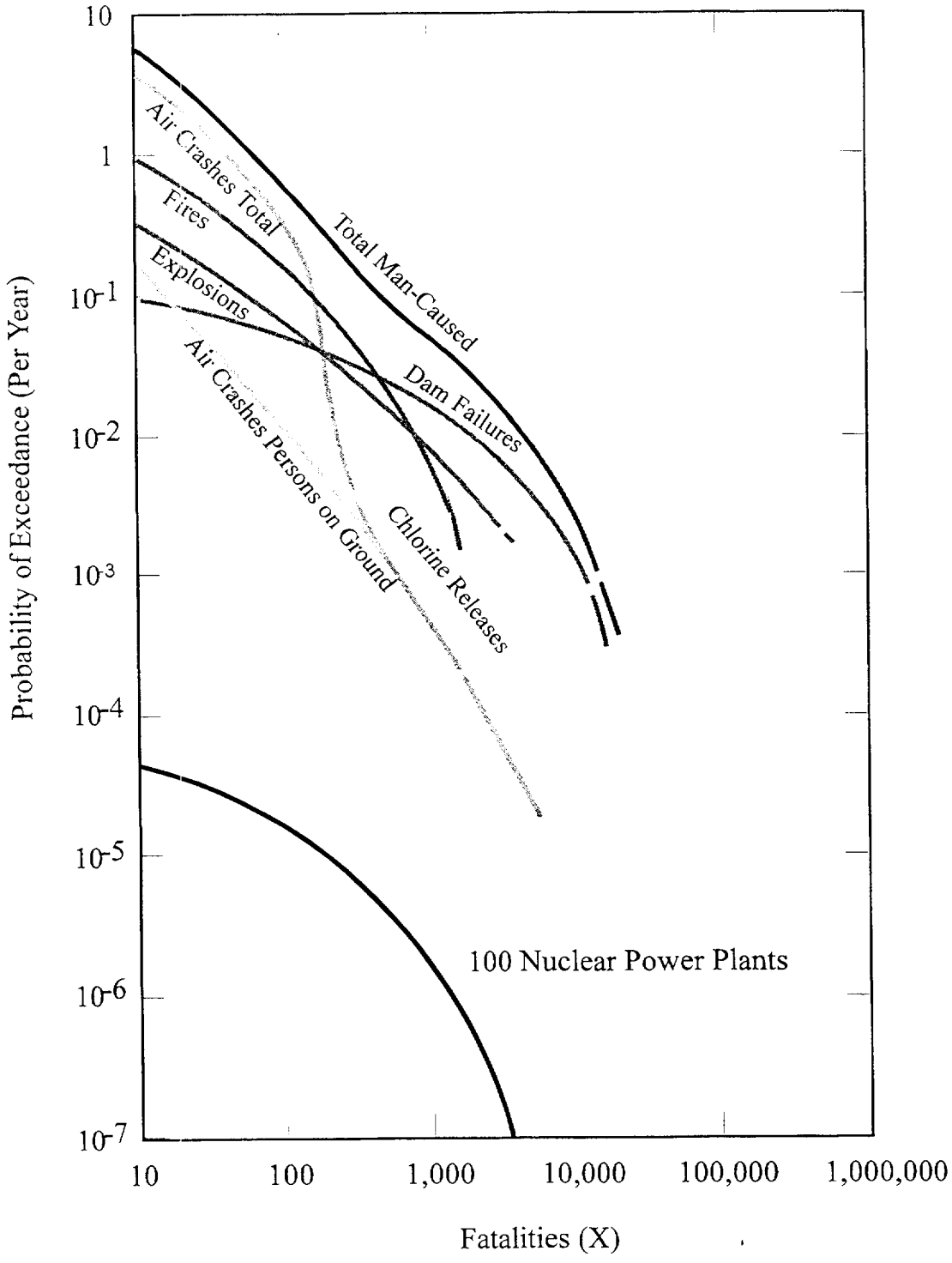


Figure 1.5-2 Frequency of man-caused events involving fatalities

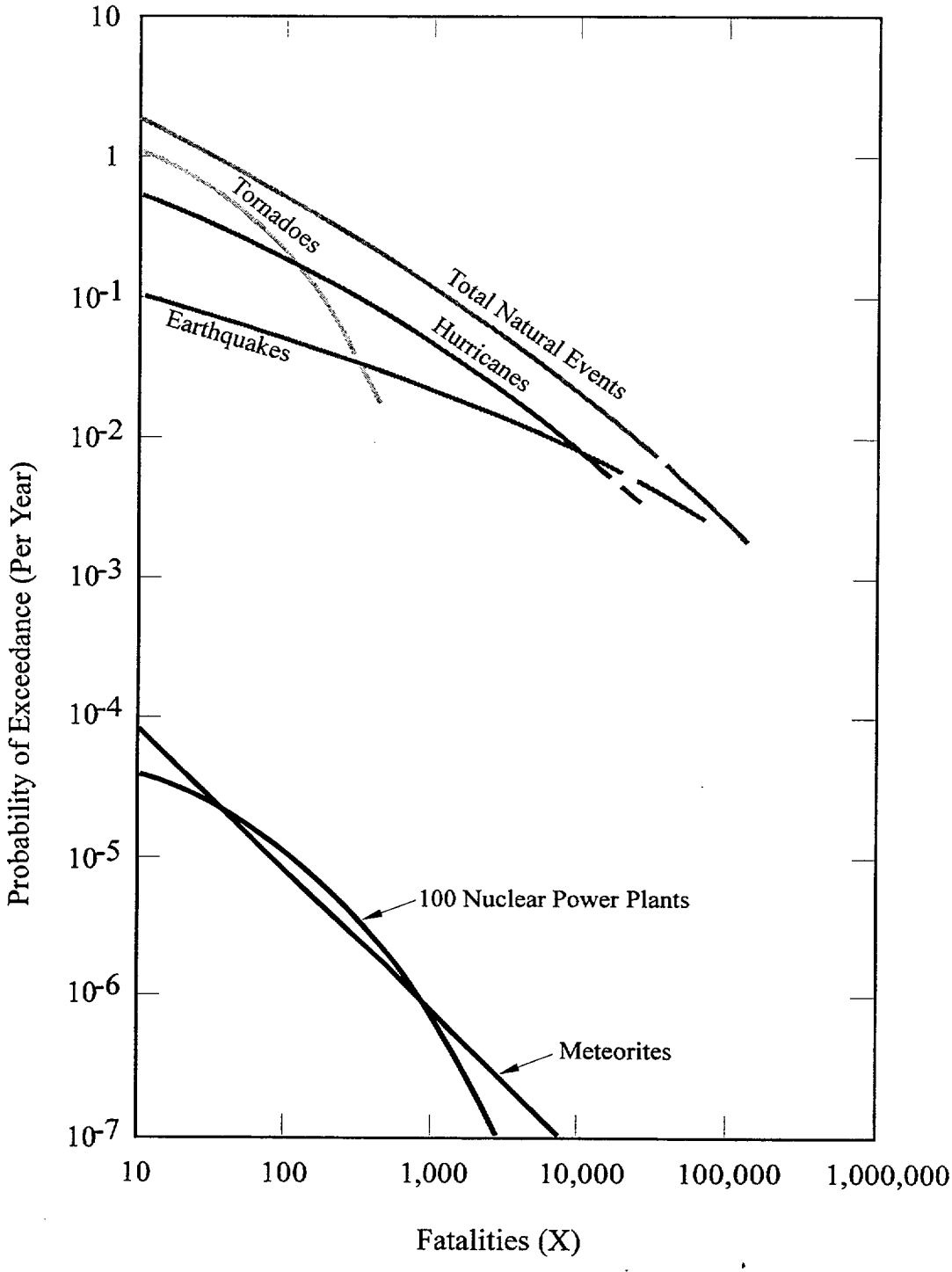


Figure 1.5-3 Frequency of natural events involving fatalities

References for Section 1.5

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

2. *U. S. Code of Federal Regulations*, Title 10, Part 50, Appendix K, January 1, 1991.

3. U. S. Nuclear Regulatory Commission, "NRC Policy on Future Reactor Designs, Decisions on Severe Accident Issues in Nuclear Power Plant Regulation," NUREG-1070, July 1985.

4. U. S. Nuclear Regulatory Commission, Regulatory Staff to Commissioners, November 15, 1971, Policy Paper.

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

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

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

1.6 Browns Ferry Fire

On March 22, 1975 a major fire occurred at the Browns Ferry nuclear power plant, which is located near Decatur, Alabama. The Browns Ferry plant is owned by the Tennessee Valley Authority (TVA). At the time, 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 and 2 were operating at a combined level of 1100 MWe. Unit 3 was still under construction.

The Browns Ferry fire was a close call that very nearly led to core damage. In searching for air leaks in an area containing electrical cables that supplied power to the plant's control room and safety systems, a technician started 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 fire 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 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.

The following subsections discuss the initiation and progression of the Browns Ferry fire and the lessons learned. Much of the material is drawn from an article by R. L. Scott that appeared in *Nuclear Safety* in 1976.[1]

1.6.1 Initiating Events

The fire was initiated by a small (3 in. to 4 in. or 7 to 10 cm) lit candle that was being used to check for air leakage of the reactor containment building (Figure 1.6-1). The flame ignited some polyurethane used to seal leakage paths, and the fire burned for 7 hours before being extinguished (Figure 1.6-2). 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 in.) thick over the foam and over the cables on both sides of the penetration for a distance of 30 cm (12 in.) to form a fire barrier (Figure 1.6-3).

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.

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 in.) wide in a cable-tray penetration through the wall. The hole was approximately 20 in. 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 1.6-4). 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 of 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.

1.6.2 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 (0.8 in. to 1.2 in./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.

1.6.3 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 ft. 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 centrally 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 12:45 p.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 of sending in two or three fire fighters at a time to use dry chemicals on the fire was established. 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.

1.6.4 Fire Damage And Assessment

The fire-damaged areas of the cable-spreading room and the reactor building are shown in Figure 1.6-5. 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.

1.6.5 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 (CRD) 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 in.), 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 would be 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 1.6-6. 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 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.

1.6.6 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 min. 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.

1.6.7 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 bringing 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.

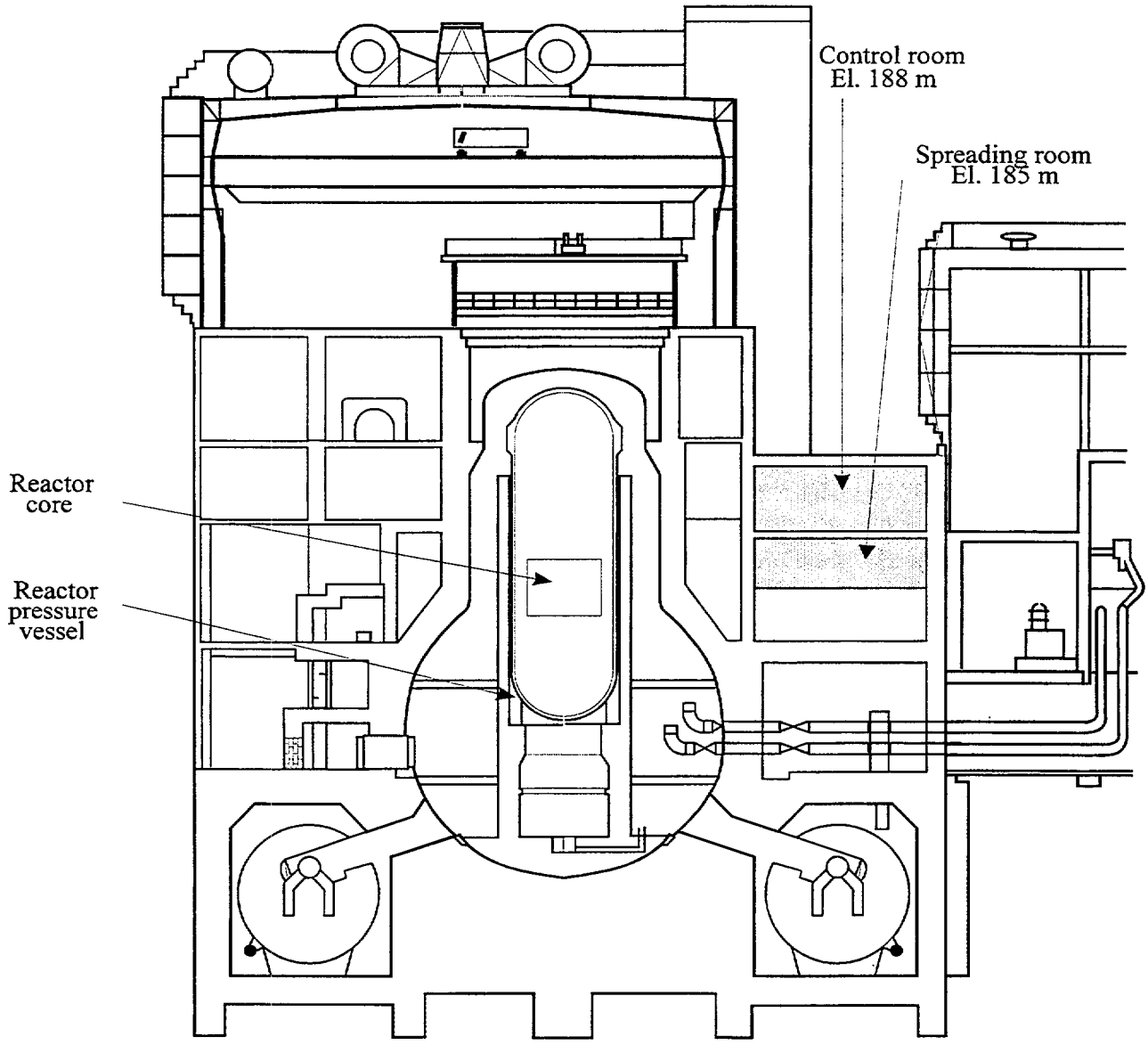


Figure 1.6-1 Vertical cross section of plant showing reactor building control room and spreading room

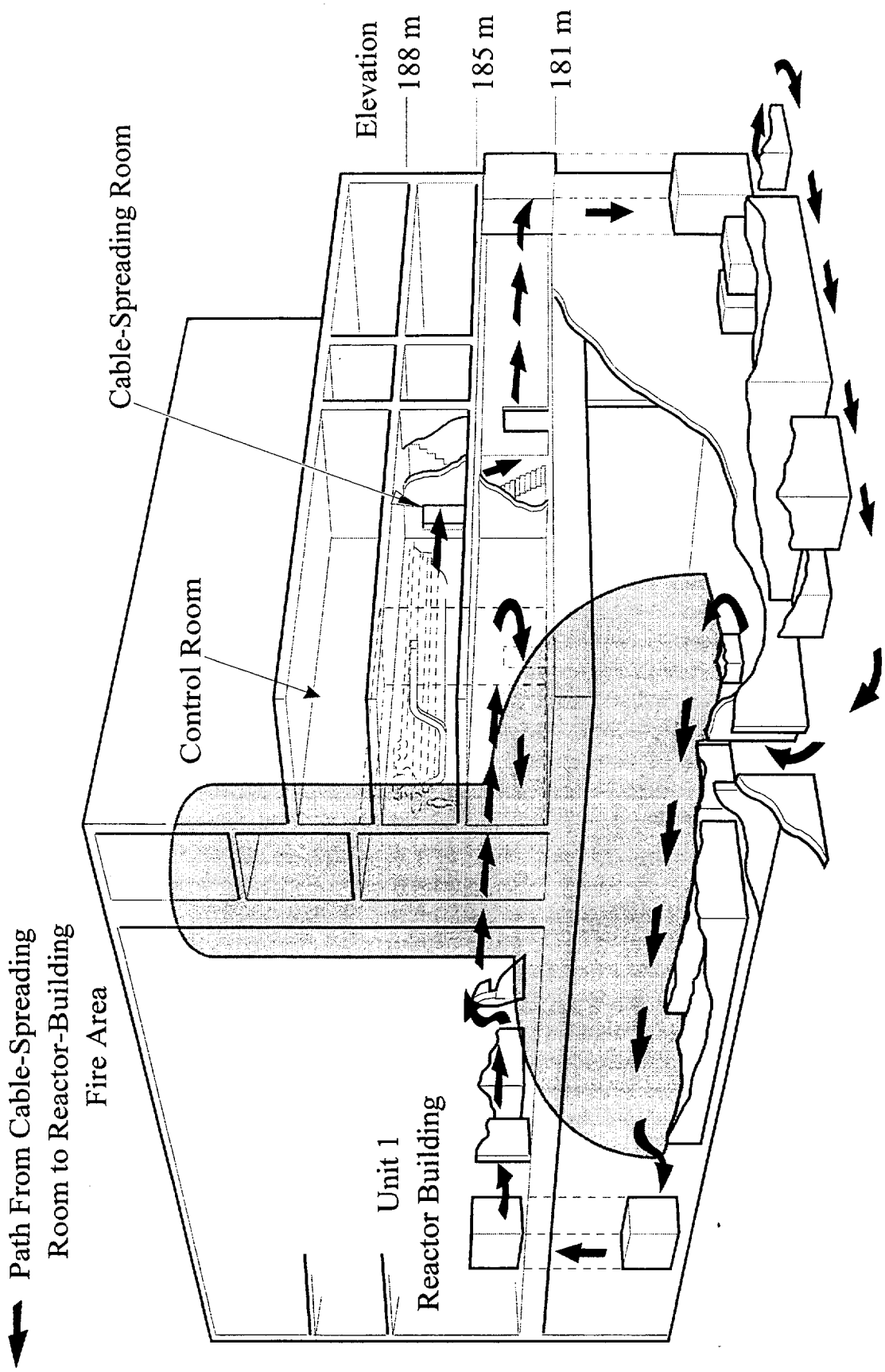
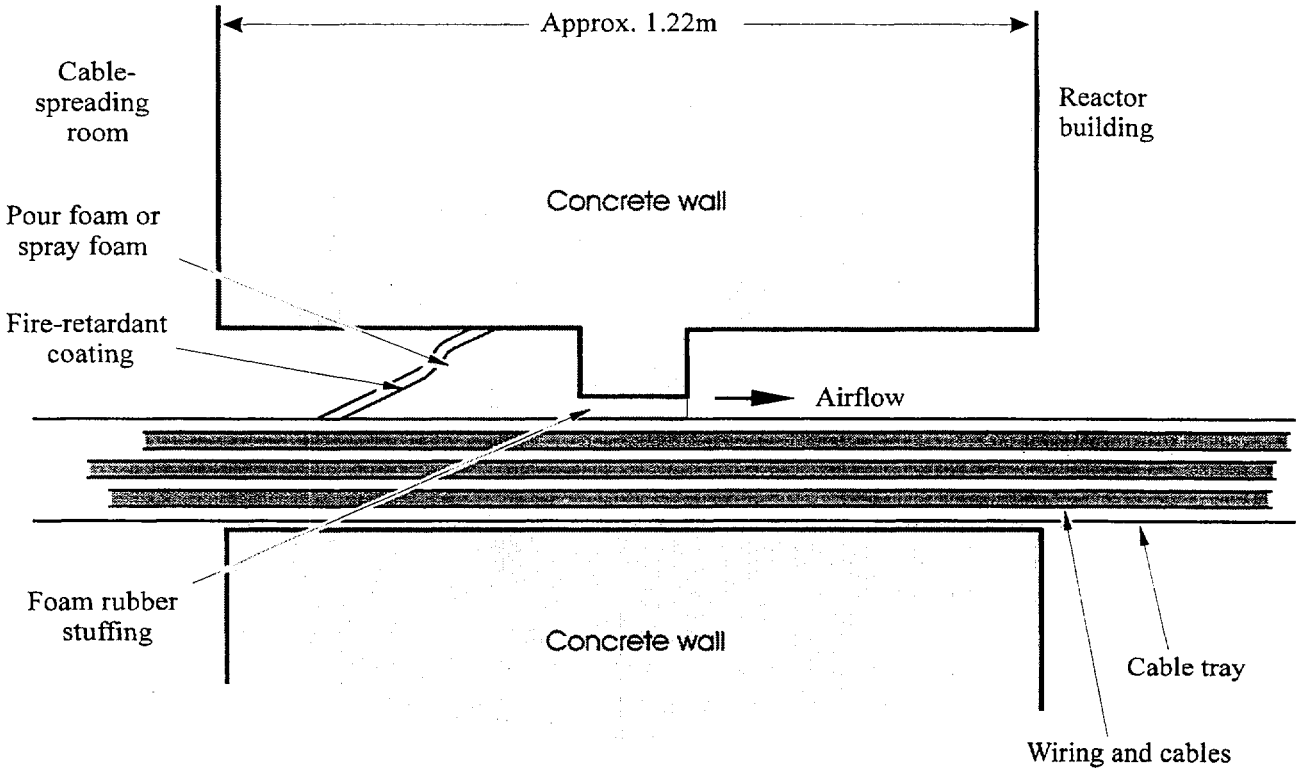
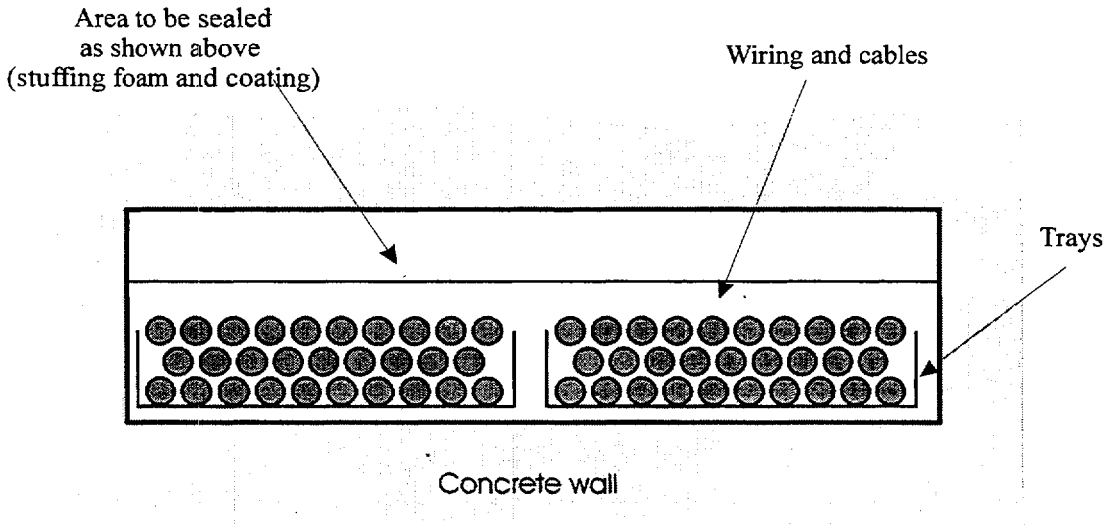


Figure 1.6-2 The Browns Ferry nuclear plant



Side view



Front view

Figure 1.6-3 Cable-tray penetration, overall simplified depiction (not to scale)

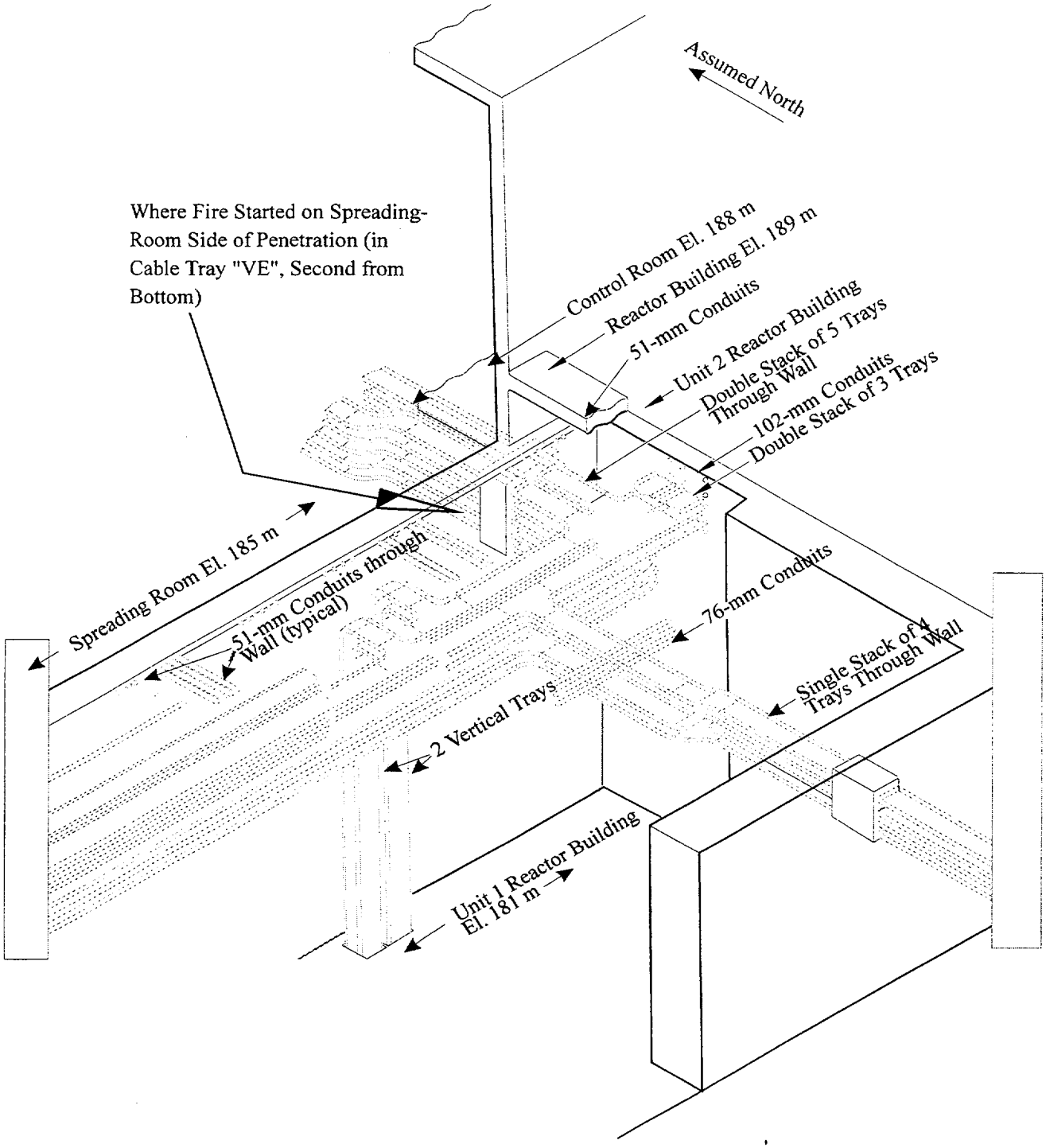


Figure 1.6-4 Area where fire started

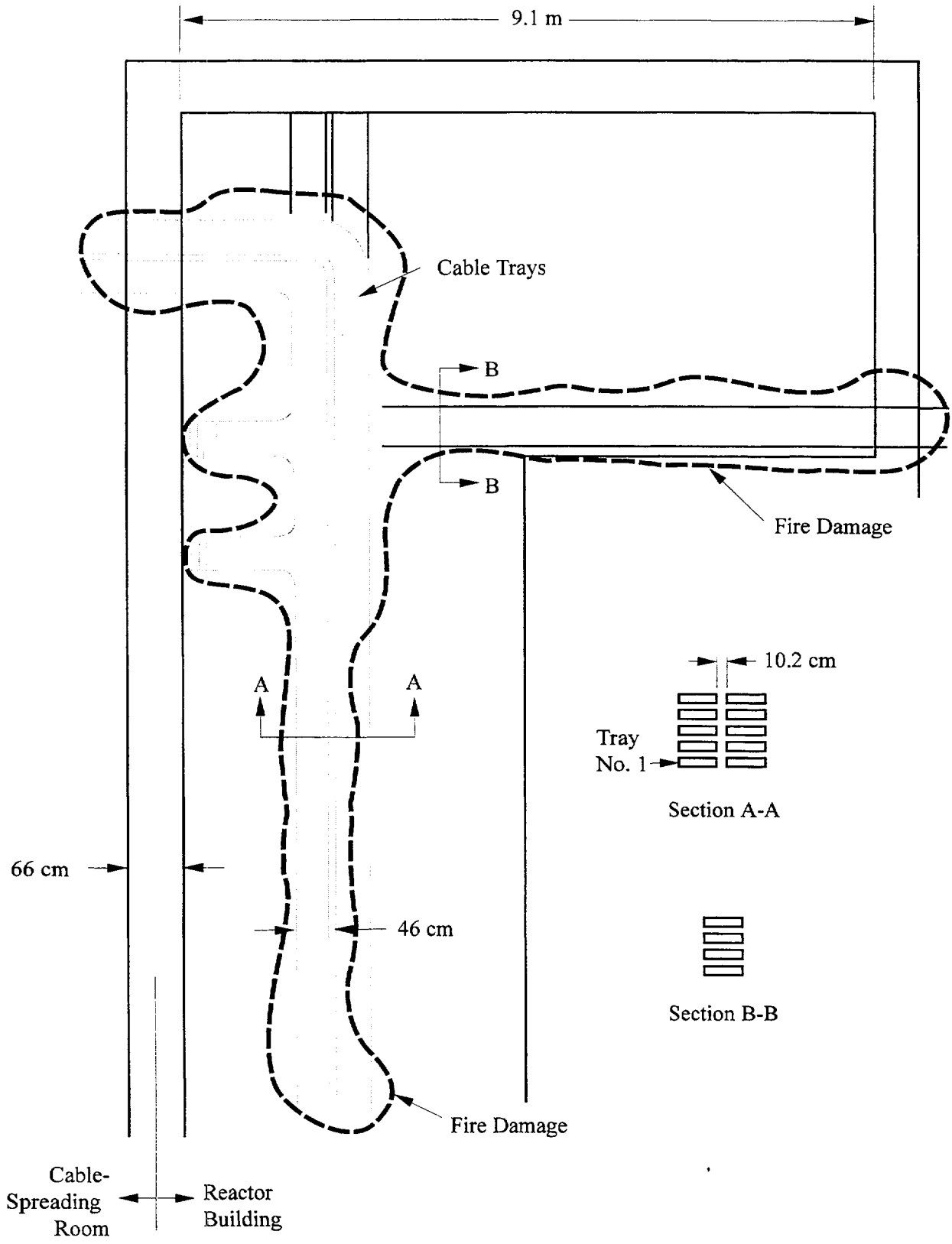
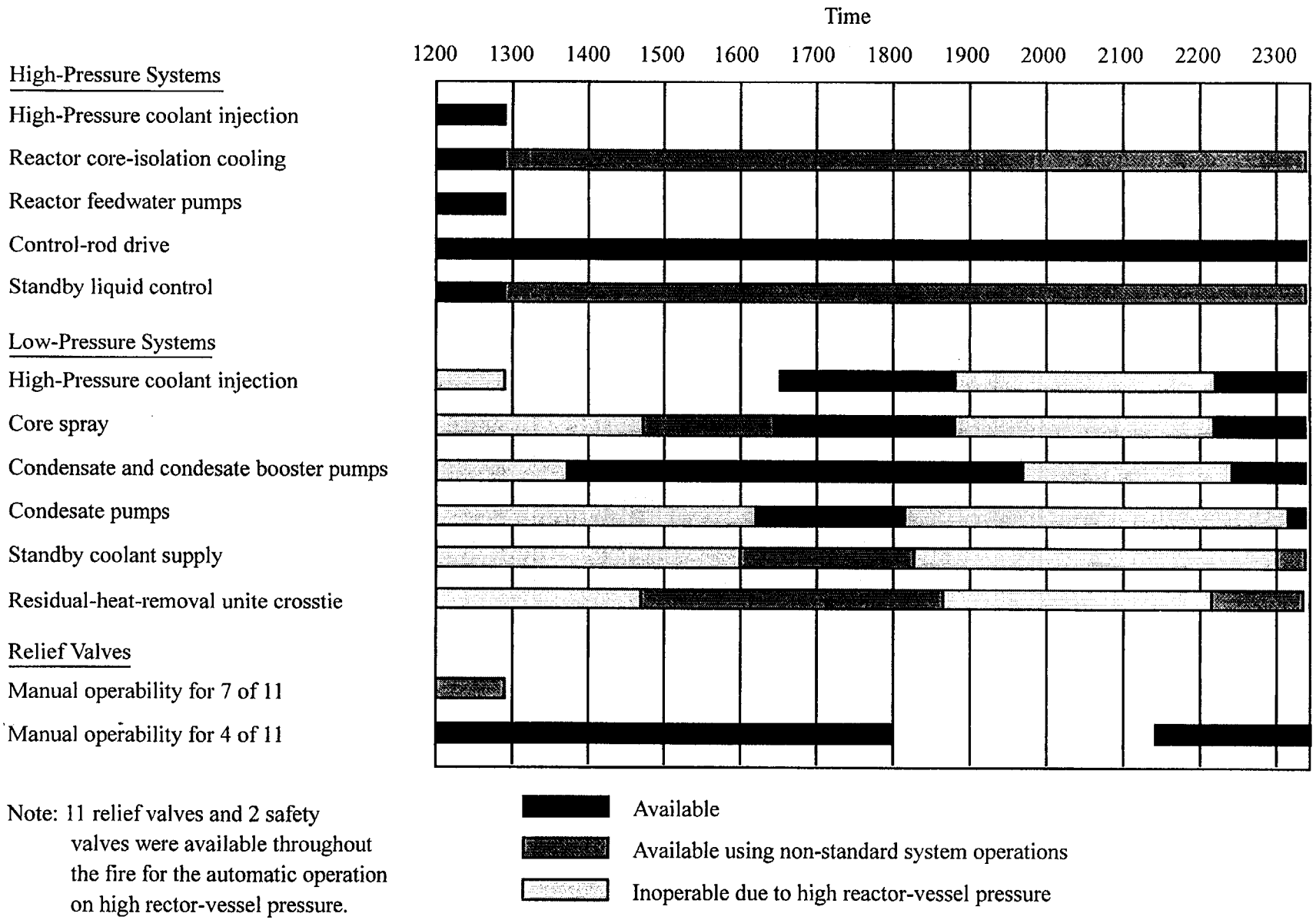


Figure 1.6-5 Fire-damaged area



Note: 11 relief valves and 2 safety valves were available throughout the fire for the automatic operation on high rector-vessel pressure.

Figure 1.6-6 Equipment availability during and immediately following the March 22, 1975 fire

References for Section 1.6

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

Appendix 1A
PRA Terms and Concepts

This appendix introduces term and concepts employed in probabilistic risk assessments (PRAs). PRA methods are used to identify the particular accidents that are possible and to estimate their likelihoods and consequences. Increasingly, 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 (see Section 2.6). Responsible participation in these processes requires a basic understanding of the estimation methods and their limitations. More in-depth material is available in NRC courses devoted to PRA.[1]

1A.1 Risk

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 2×10^{-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. Estimates of core damage frequencies for various U.S. nuclear power plants range from approximately 10^{-3} to 10^{-6} per reactor year.

Potential health and economic consequences of severe 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 1A-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.

1A.2 The PRA Process

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 appendix describes the limitations of PRA methods, the reader should note that the overall benefits of the methods far outweigh the limitations.

PRAs can be performed for non-nuclear as well as for nuclear facilities, but the focus here is on the risks of nuclear power plant accidents. Traditionally, nuclear power plant PRAs have been conducted at one of three levels. Figure 1A-1 illustrates the activities and/or products associated with each level.[2]

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 (see Section 1A.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 and other attributes such as the elevation, energy, and timing of the release that can have an important effect on offsite doses.

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.

1A.3 Analysis of Initiating Events

Accidents 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.

The first step in performing a PRA is to identify possible initiating events and determine their frequencies. 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.

Accidents are often classified by their initiators. 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. Transient initiators are usually events related to the balance of plant (BOP). 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.

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, loss of offsite power is included as an initiator in all analyses of internal events. Fires internal to the plant have traditionally been classified as external events (although many analysts now agree they should be classified as internal events).

1A.3.1 Internal Initiating Events

Internal initiating events usually receive the most attention in PRAs, and their frequencies are generally less difficult to estimate than the frequencies of external initiators.[3]

Table 1A-2 lists transient initiators for BWRs and PWRs. Initiators requiring similar plant responses are grouped together. Note that the listed initiators are often more specific than the design-basis initiators postulated and analyzed in Safety Analysis Reports (see Section 1.4), although there is considerable overlap. Design-basis initiators can lead to core damage if additional failures occur (a design-basis initiator can lead to a beyond-design-basis accident).

The initiators and generic frequencies listed in Table 1A-2 are based on both historical data and engineering analyses. Such generic frequencies are often used as a starting point, but they are obtained by averaging over groups of plants and, thus, may not be accurate for a particular plant. A set of internal initiating event groups and their frequencies for one of the NUREG-1150 plants is shown in Table 1A-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 1A-2 and 1A-3 may be found in NUREG/CR-4550,[4] which is one of the supporting documents for NUREG-1150.

1A.3.2 External Initiating Events

In addition to the internal initiating events discussed above, there are external initiators that can occur with variable magnitudes. Traditionally these have included:

1. Aircraft impacts,
2. Plant-internal and external flooding,
3. Extreme winds and tornadoes (and associated missiles),
4. Plant-internal and external 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.

Note that these initiators include not only naturally occurring phenomena, but also unintentional human-caused events and failures within the reactor site, not directly related to reactor operations.

An external initiating event of sufficient magnitude may have the potential to directly cause multiple component failures and lead to core damage with few, if any, additional independent failures. Plant-internal fires and seismic events are the two most important external initiating events for most plants.

Hazard analyses are performed to assess the likelihood of external 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.

1A.3.2.1 Plant-Internal Fires

Fire in a nuclear power plant can initiate a serious accident by rendering vital plant equipment inoperable. The term plant-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. 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 determine the rate at which a 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.

1A.3.2.2 Seismic Events

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 1.4.2), 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.

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.

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 are easy to obtain, but data are 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 very large 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 has been 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. NUREG-1150 used seismic hazard curves 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.[5] 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).[6] Figures 1A-2 and 1A-3 present the two markedly different families of hazard curves that were used for the Peach Bottom site in NUREG-1150.

1A.3.2.3 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 plant-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.

1A.3.2.4 Other Naturally Occurring 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.

1A.3.2.5 Human-Caused External Initiators

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.

1A.3.3 Accidents at Low Power and Shutdown

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.[7,8] 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 in shutdown.

While it is true that the decay heat generation rate decreases to about 1% 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.

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 1A-4 presents initiating event frequencies for the Grand Gulf plant while in Plant Operation State (POS) 5[9], which basically includes the Cold Shutdown Mode of Operation. These frequencies are per year of operation in POS 5.

1A.3.4 Sabotage Not Treated in PRA

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 seeking to cause a large release of radioactive material or a disgruntled worker seeking revenge on a single individual. Requirements for physical protection of plants and materials are described in 10 CFR Part 73.[10]

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.

It is generally accepted that the frequency of sabotage threats decreases as their severity increases, but 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 threats to the facility can be repelled reliably. These threats are analyzed without

regard to their probabilities, although they are selected based on current knowledge of real threats.

1A.4 Accident Sequence Development

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.

1A.4.1 Multiple Versus Single Failures

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 1A-5 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 which is set forth in 10 CFR 50 Appendix A:[11]

*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 (0.063 m^3/s) in order to prevent core damage following certain accident initiators. The plant systems will be successful if they provide 1000 gpm (0.063 m^3/s) on demand. This is the injection *success criteria* for such accidents. The plant systems will withstand single failures if 1000 gpm (0.063 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 (0.063 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 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 train might fail to open. Terminology used to distinguish various types of multiple failures is discussed in Section 1A.4.3.

1A.4.2 Use of Event Trees and Fault Trees

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 diagramed 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 1A-4. Consider a LOCA initiated by a small pipe break (event S2). The front-line systems that should automatically respond to prevent core damage are the reactor protection system (RPS) and the High Pressure Injection (HPI) System. 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 1A-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, and $p_{fADS|S2,RPS,fHPI}$ 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 $(1-p_{fRPS|S2})$ are essentially equal to one.

The fact that system failure probabilities are small is, of course, desirable; however, it

also means that the failure probabilities of such systems cannot be directly quantified based on failure data. 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 1A-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 1A-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 1A-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 1A-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 auto actuation signal failure (ASF) 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:

$$ISF = ASF*OFA + VFO + POM + PFS + PFR + PPF$$

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 PPF in the last term on the right hand side, failure of power to the pump (PPF), 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.

1A.4.3 Failure Terminology

1A.4.3.1 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. 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.

1A.4.3.2 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).

1A.4.3.3 Common Cause Failures

A *common cause failure* is the simultaneous failure or unavailability of more than one component due to some underlying common cause, such as design errors or environmental factors.

It should be noted that by this definition common cause failures include the explicitly dependent failures discussed in the following section. However, the term common cause is more often used to describe situations in which for some unknown reason redundant components fail with a higher frequency than would be calculated under the assumption that the components failed independently. The term common mode failure is also used to describe this type of failure (and is perhaps more appropriate).

As indicated in Figure 1A-6, 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.[12]

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.

Common cause events can be placed directly on fault trees. 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 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 independently 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.

1A.4.3.4 Subtle Failures

Subtle failures are best explained by example. They require detailed knowledge of the design and operation of plant systems and can, therefore, be difficult to uncover. Six examples follow.

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.

Pump Room Cooling

Given the loss of room cooling at a certain plant, the maximum room temperature remains below the temperature for which a pump and its control circuits are qualified. However, 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.

Air Binding of Cooling Water Systems

There have been several incidents involving the failure or partial failure of 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.

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 failed is further upstream and only blocked flow from one RHR heat exchanger.

Normal Operating Configuration

The normal operating configuration of systems cannot always be inferred from plant piping and instrumentation diagrams (P&IDs). For example, a P&ID may show valves as normally closed when, in reality, the plant operates with these valves open. One 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, only one of the two room coolers is normally operated. Further discussion revealed that power to the operating cooler fan could be taken from Division 1 while power to supply the cooling water to the cooler heat exchanger was being taken from Division 2. Because of this operating configuration, several single failures of the three high-pressure injection pumps were identified.

Locked Door Dependencies

The plant configuration is not always obvious during special types of accidents such as a station blackout. 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.

1A.4.4 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. 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 2.1) and Chernobyl (Section 2.3) 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 LOCA, 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.

1A.4.5 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 1A-7, 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 1A.3.2.2 discussed the development of hazard curves, and consequence analysis is discussed in Chapter 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.

The use of event trees and fault trees for accident sequence development was discussed in Section 1A.4.2. 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. The threat of core damage posed by fire in a particular area of the plant depends on the frequency of ignition in the area, the amount and nature of combustible material in the area, the nature and efficacy of automatic and manual fire-suppression systems in the area, the proximity of vital equipment. Coincident failures of fire protection systems and other systems must be considered. Only a small fraction of the fires that could occur in a nuclear power plant would be expected to lead to core damage. Fires in the control room and emergency switchgear areas are important in view of the potential for simultaneous failure of several systems by fires in these areas. Thus, in the past these areas have received particular attention in fire protection programs. Fire analyses include credit for the fire protection programs required by Appendix R to 10 CFR Part 50.[13]

1A.5 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 1A.4.3.4), 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 1A-8. 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% of the distribution. Figure 1A-8 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 1A.3.2.2), 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 1A-8, 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 1A-1 Consequence weighted risk

Accident Scenario	Estimated Frequency (accid/yr)	Estimated Consequence (deaths/accid)	Consequence-Weighted Risk (deaths/yr)
S_1	2.0×10^{-5}	1	2.0×10^{-5}
S_2	0.2×10^{-5}	3	0.6×10^{-5}
S_3	0.6×10^{-5}	7	4.2×10^{-5}
S_4	0.3×10^{-5}	5	1.5×10^{-5}
Total	3.1×10^{-5}		8.3×10^{-5}

Table 1A-2 Transient initiating event frequencies

Reactor/Group	Initiating Event	Frequency/Reactor Year
BWR Groups		
LOSP	LOSP	0.08
	Loss of auxiliary power (transformer)	0.02
	Group Total	0.10
Loss of PCS	Electric load rejection with turbine bypass failure	0.004
	Turbine trip with turbine bypass valve failure	0.004
	MSIV closure	0.27
	Inadvertent closure of one MSIV	0.21
	Partial MSIV closure	0.06
	Loss of condenser vacuum	0.41
	Pressure regulator fails open	0.08
	Pressure regulator fails closed	0.10
	Turbine bypass fails open	0.04
	Turbine bypass or control valves increase pressure (closed)	0.42
	Cause unknown	0.06
	Group Total	1.66
IORV	IORV	0.14
PCS Available	Electric load rejection	0.45
	Turbine trip	0.87
	Recirculation control failure, increasing flow	0.18
	Recirculation control failure, decreasing flow	0.05
	One recirculation pump trip	0.06
	Recirculation pump trip (all)	0.03
	Abnormal startup of idle recirculation pump	0.02
	Recirculation pump seizure	0.004
	FW--increasing flow at power	0.14
	Loss of FW heater	0.02
	Trip of one FW or condensate pump	0.20
	Rod withdrawal at power	0.01
	Inadvertent insertion of rods	0.06
	Detected fault in RPS	0.05
	Inadvertent startup of HPCI/HPCS	0.01
	Scram from plant occurrences	0.58
	Spurious trip via instrumentation, RPS fault	1.11
	Manual scram, no out-of-tolerance condition	0.87
	Group Total	4.71
FW Lost but Condenser Available	Loss of all FW flow	0.07
	FW, low flow	0.49
	Group Total	0.56

Table 1A-2 Transient initiating event frequencies (continued)

Reactor/Group Event	Initiating Event	Frequency/Reactor Year
PWR Groups		
LOSP	Loss of offsite power	0.15
Loss of PCS	Inadvertent safety injection signal	0.05
	Total loss of FW flow (all loops)	0.16
	Closure of all MSIVs	0.04
	Increase in FW flow (all loops)	0.02
	FW flow instability--operator error	0.29
	FW flow instability--miscellaneous mechanical cause	0.34
	Loss of all condensate pumps	0.01
	Loss of condenser vacuum	0.14
	Loss of circulating water	0.05
	Group Total	1.10
PCS Available	Loss of RCS flow (one loop)	0.28
	Uncontrolled rod withdrawal	0.01
	CRD mechanical problems and/or rod drop	0.50
	Leakage for control rods	0.02
	Leakage in primary system	0.05
	Low pressurizer pressure	0.03
	Pressurizer leakage	0.005
	High pressurizer pressure	0.03
	Containment pressure problems	0.005
	CVCS malfunction--boron dilution	0.03
	Pressure/temperature/power imbalance--rod position error	0.13
	Startup of inactive coolant pump	0.002
	Total loss of RCS flow	0.03
	Loss or reduction in FW flow (one loop)	1.50
	Full or partial closure of MSIV (one loop)	0.17
	Increase in FW flow (one loop)	0.44
	Loss of condensate pumps (one loop)	0.07
	Steam generator leakage	0.03
	Condensate leakage	0.04
	Miscellaneous leakage in secondary system	0.09
	Sudden opening of steam relief valves	0.02
	Turbine trip, throttle valve closure, EHC problems	
1.19		
	Generator trip or generator caused faults	0.46
	Pressurizer spray failure	0.03
	Spurious trips--cause unknown	0.08
	Auto trip--no transient condition	1.49
	Manual trip--no transient condition	0.47
	Group Total	7.20

Table 1A-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 1A-4 Initiating event frequencies for Plant Operating State 5 (cold shutdown)

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

Table 1A-4 Initiating event frequencies for Plant Operating State 5 (cold shutdown) (continued)

Initiating Event Nomenclature	Description	Mean Frequency per Year for POS 5
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
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 1A-5 Safety function system requirements

Boiling Water Reactors (BWRs)

Safety Function	Plant Systems
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

Pressurized Water Reactors (PWRs)

Safety Function	Plant Systems
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 1A-6 Collections and summaries of actual failure events

Title	Source	Reference
1. Licensee Event Reports	USNRC	
2. Licensee Event Report Summaries	Idaho National Engineering Laboratory	
Valves		NUREG/CR-1363
Pumps		NUREG/CR-1205
Electrical Power		NUREG/CR-1362
Circuit Breakers, Protective Relays		NUREG/CR-4212
Initiating Events		NUREG/CR-3862
Selected I&C Components		NUREG/CR-1740
Control Rods and Drive Mechanisms		NUREG/CR-1331
3. In-Plant Reliability Data Systems	Oak Ridge National Laboratory	
Pumps		NUREG/CR-2886
Valves		NUREG/CR-3154
Electrical Power Components (Diesels, Batteries, Chargers and Inverters)		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 1A-7 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 1A-6 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

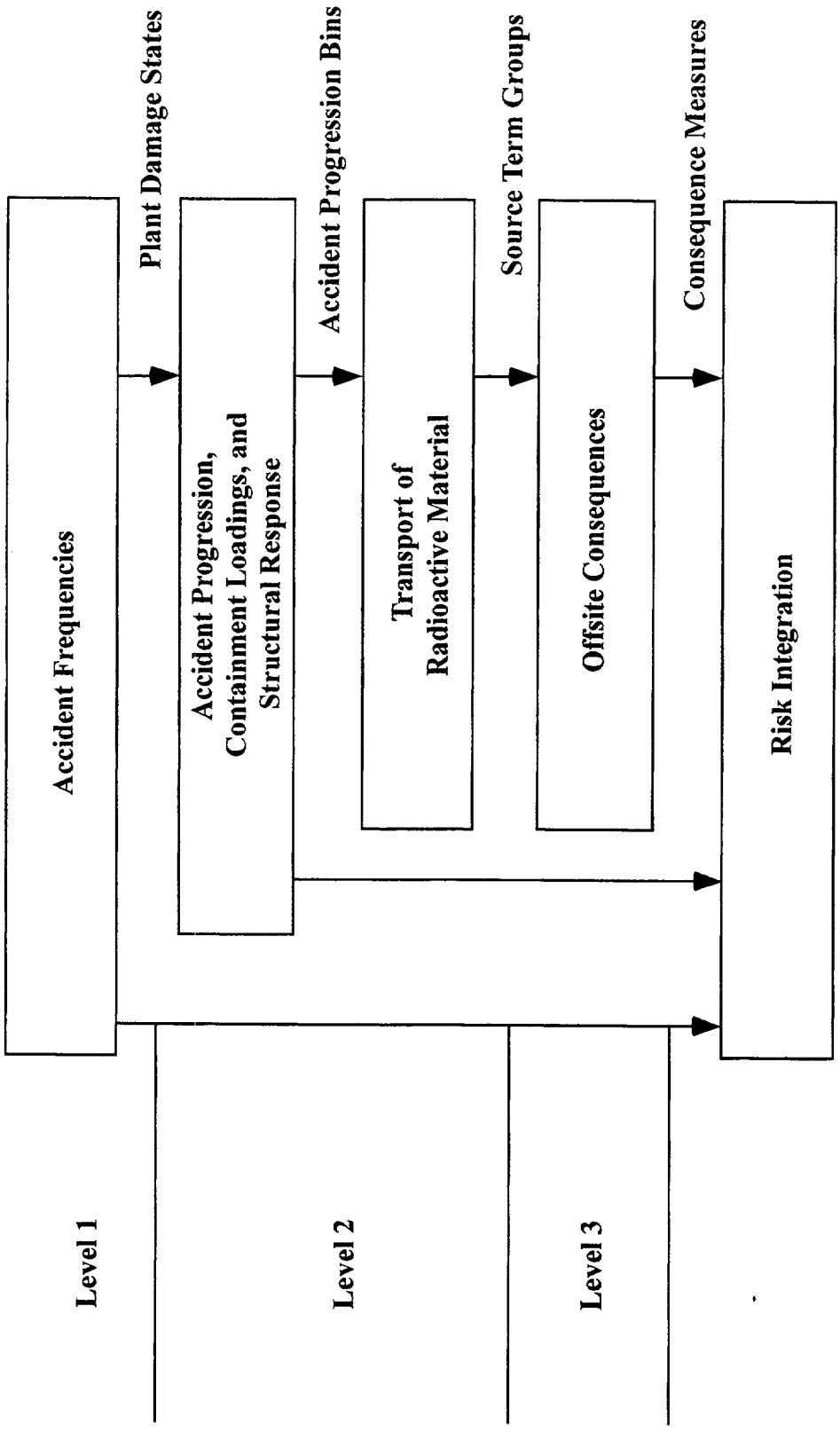


Figure 1A-1 Three levels of probabilistic risk assessment

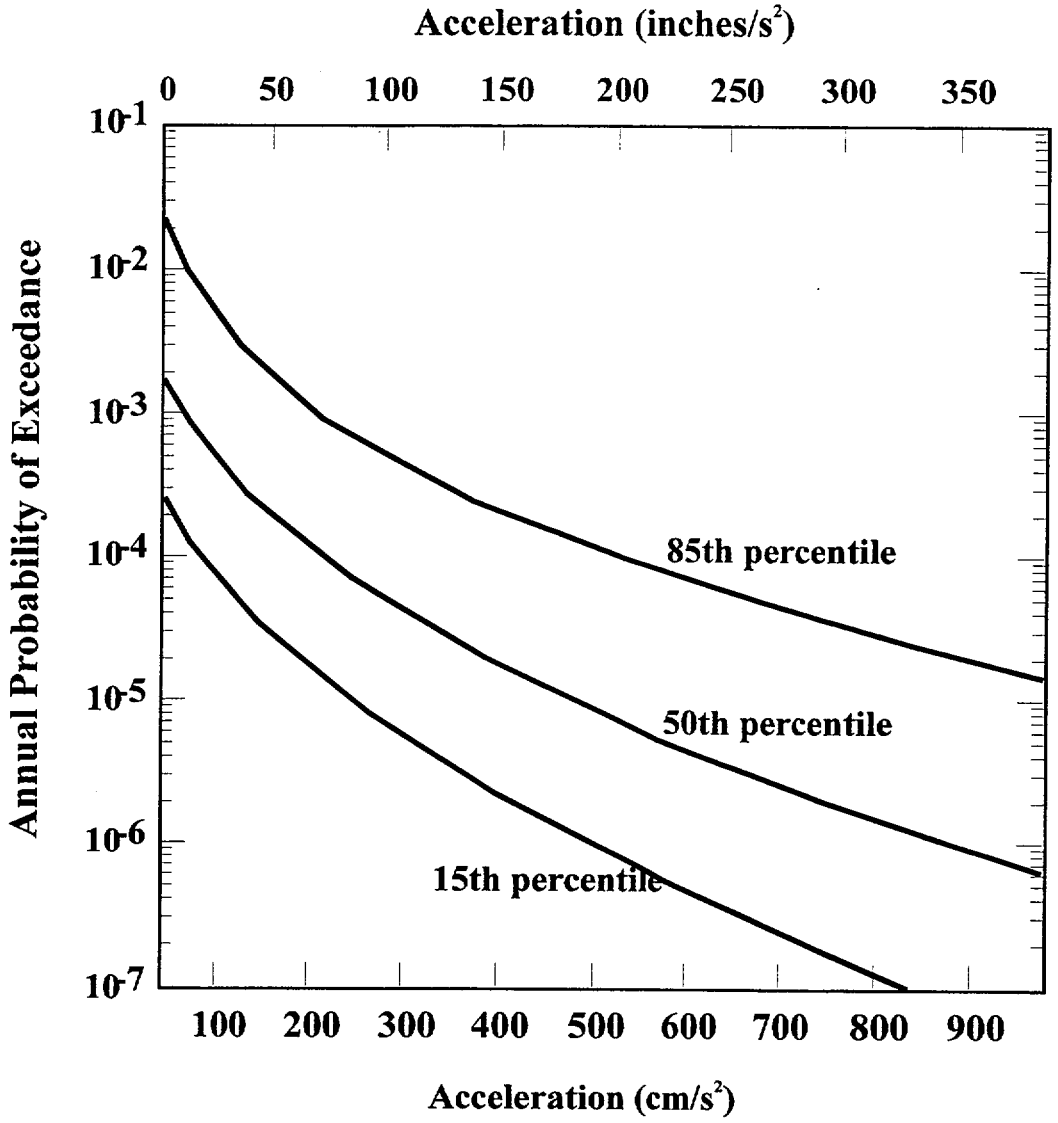


Figure 1A-2 LLNL hazard curves for Peach Bottom site

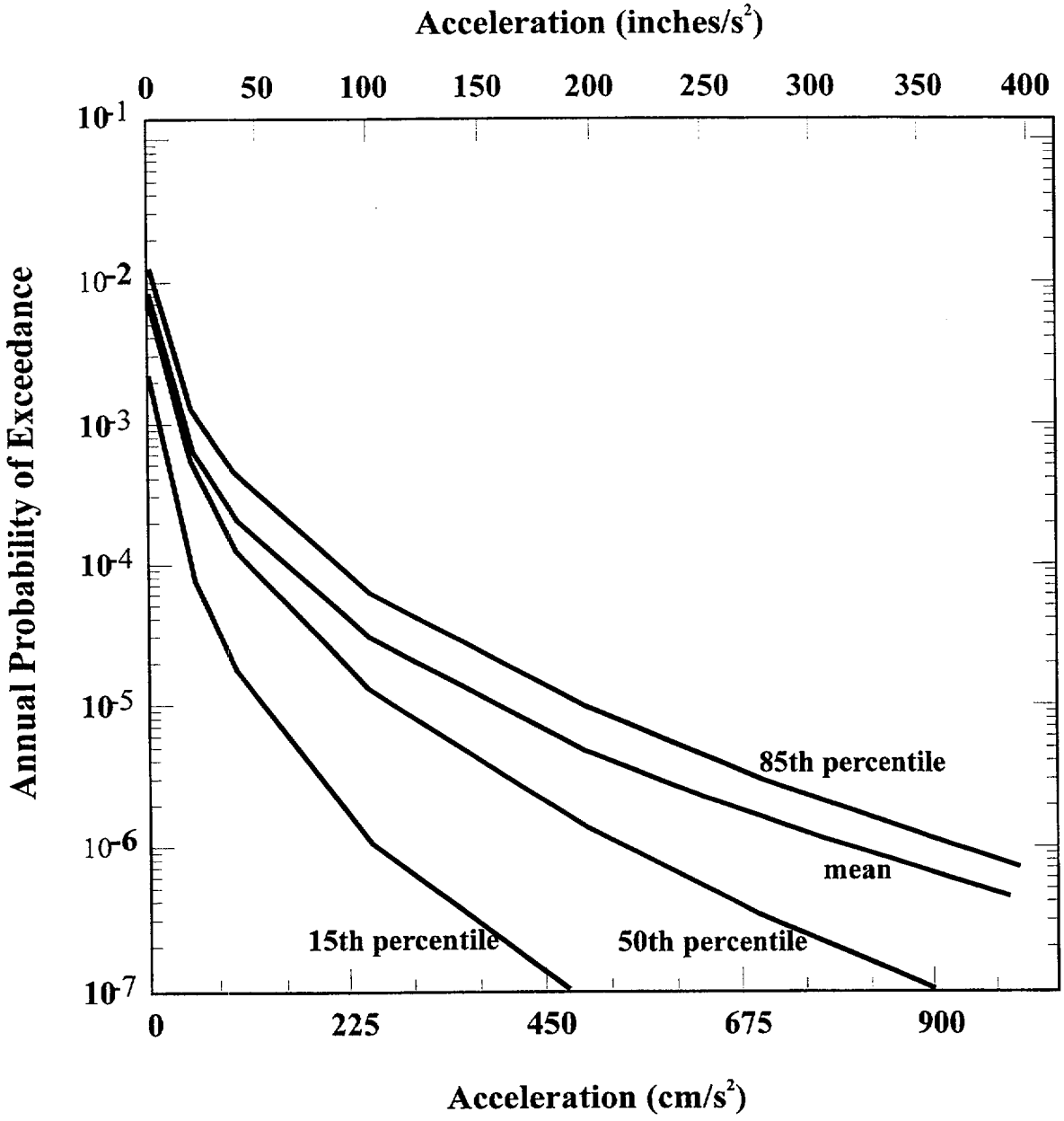


Figure 1A-3 EPRI hazard curves for Peach Bottom site

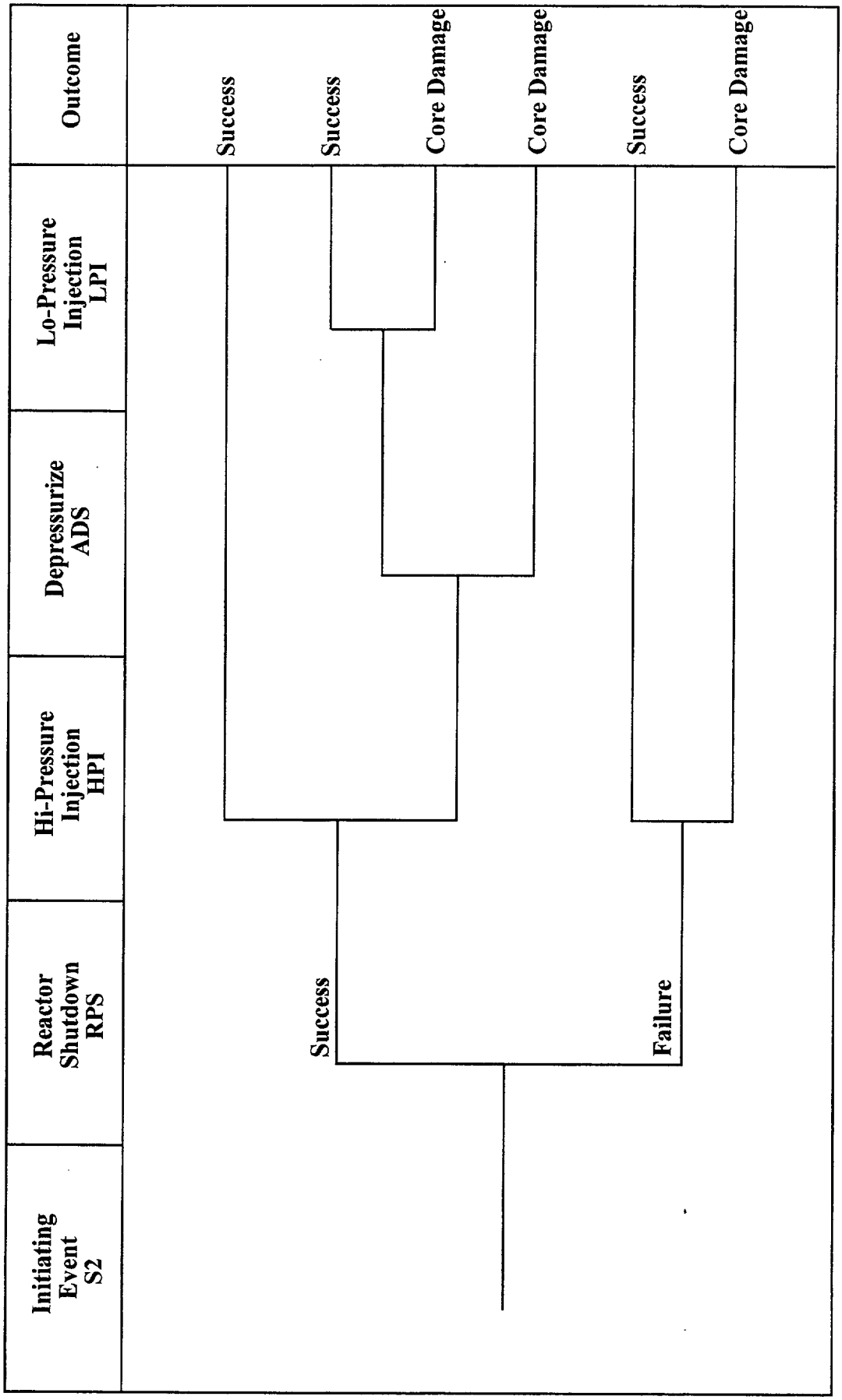


Figure 1A-4 Example event tree

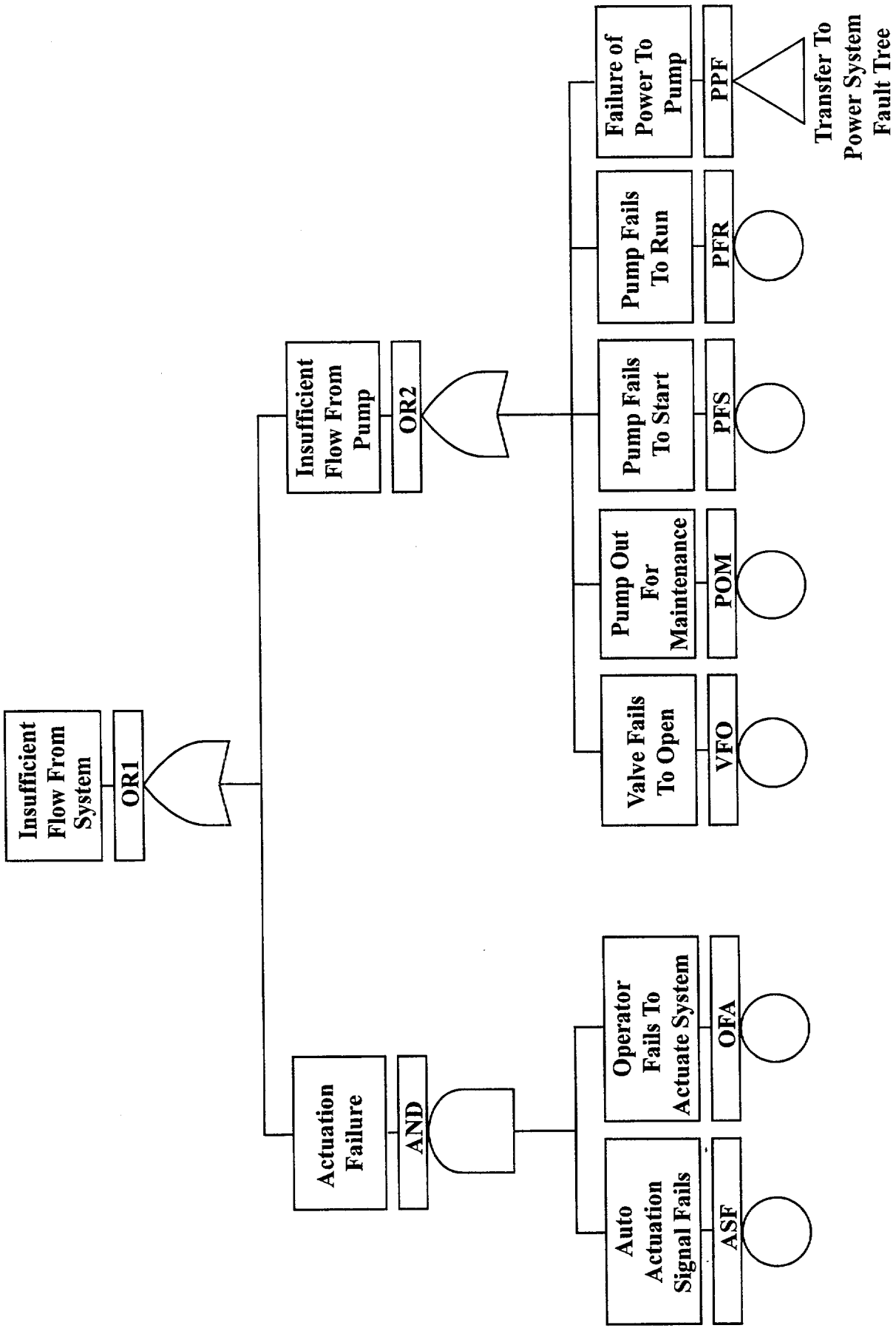


Figure 1A-5 Example fault tree

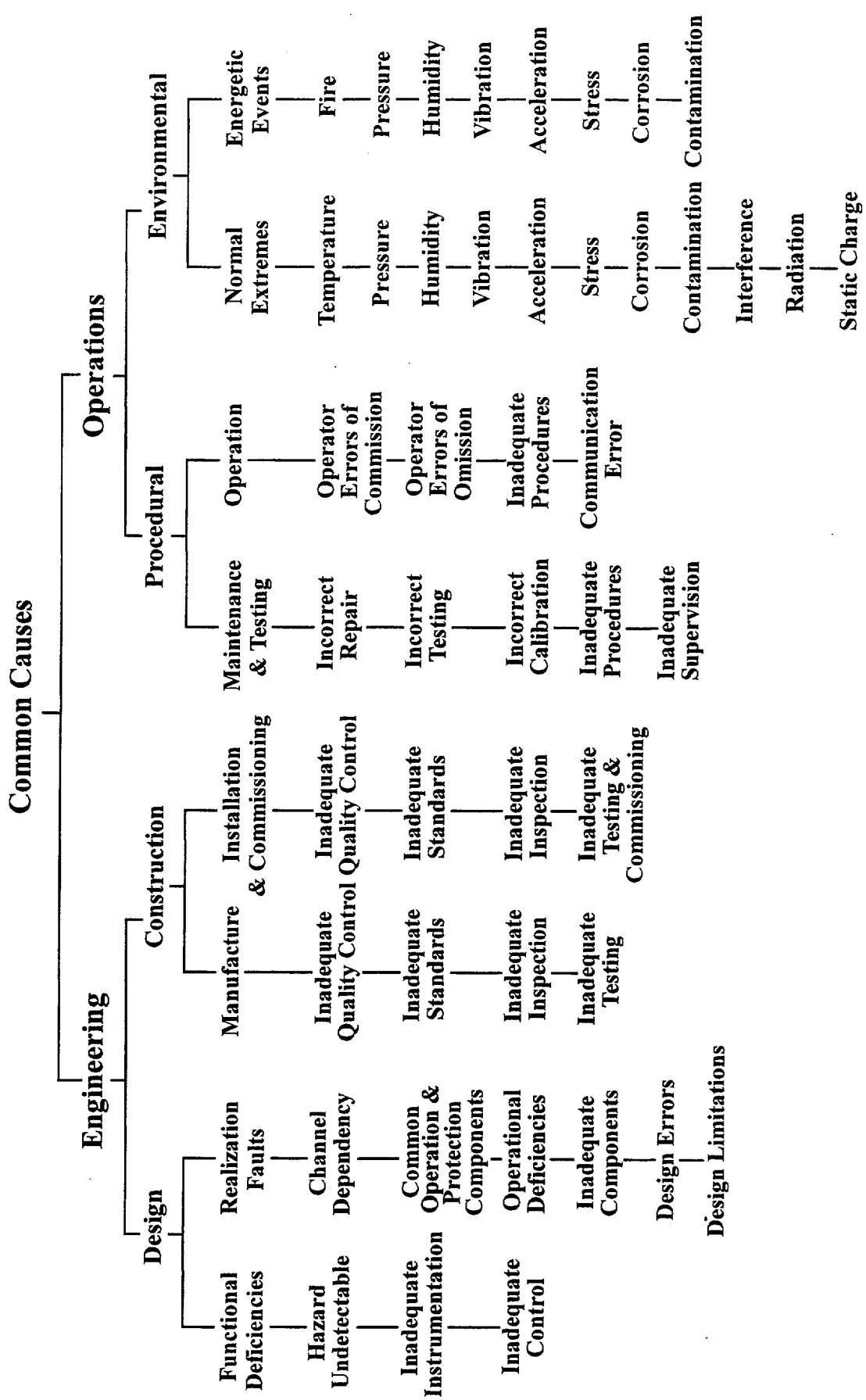


Figure 1A-6 Common causes of failure

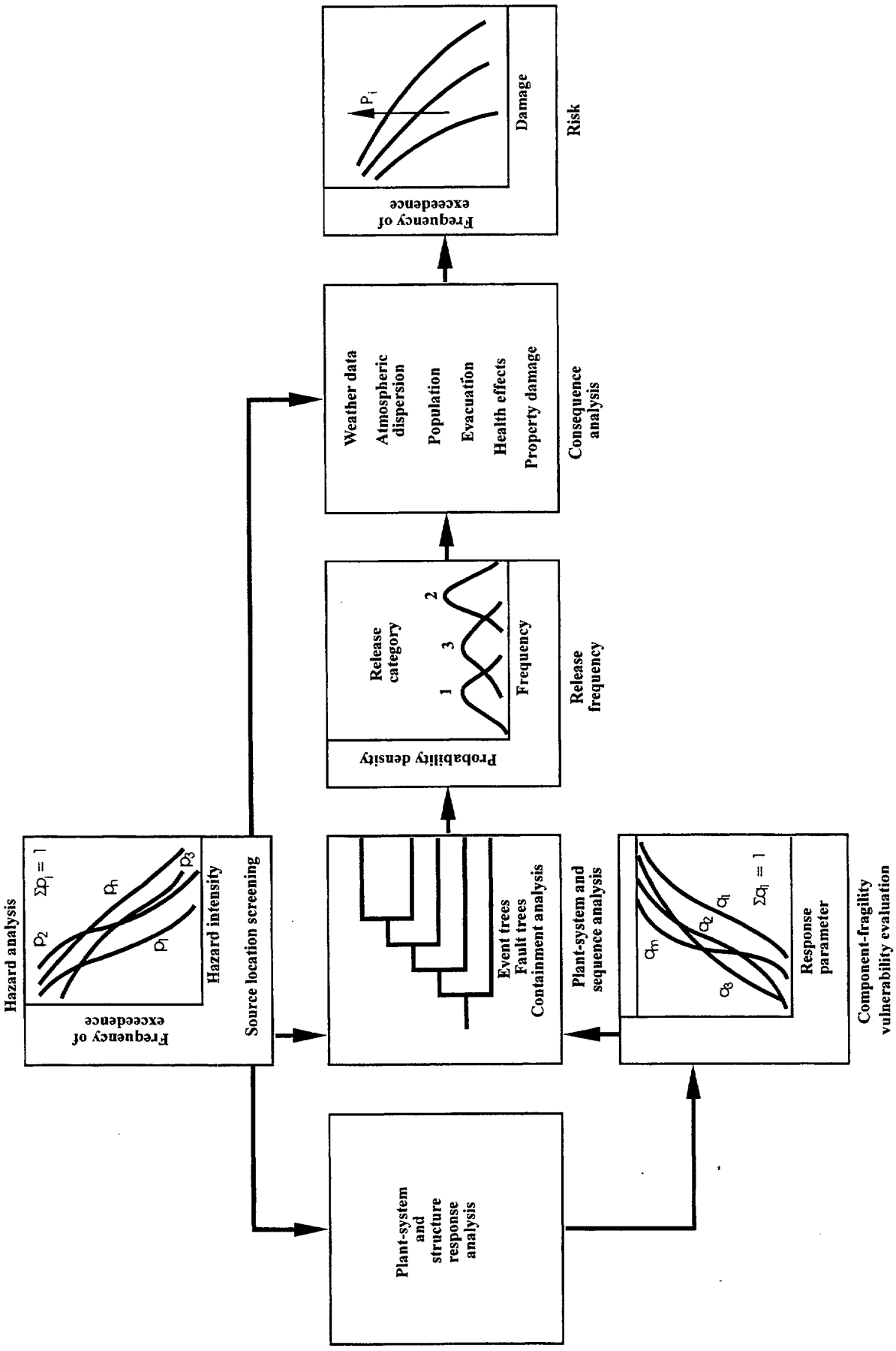


Figure 1A-7 Risk assessment procedure for external events

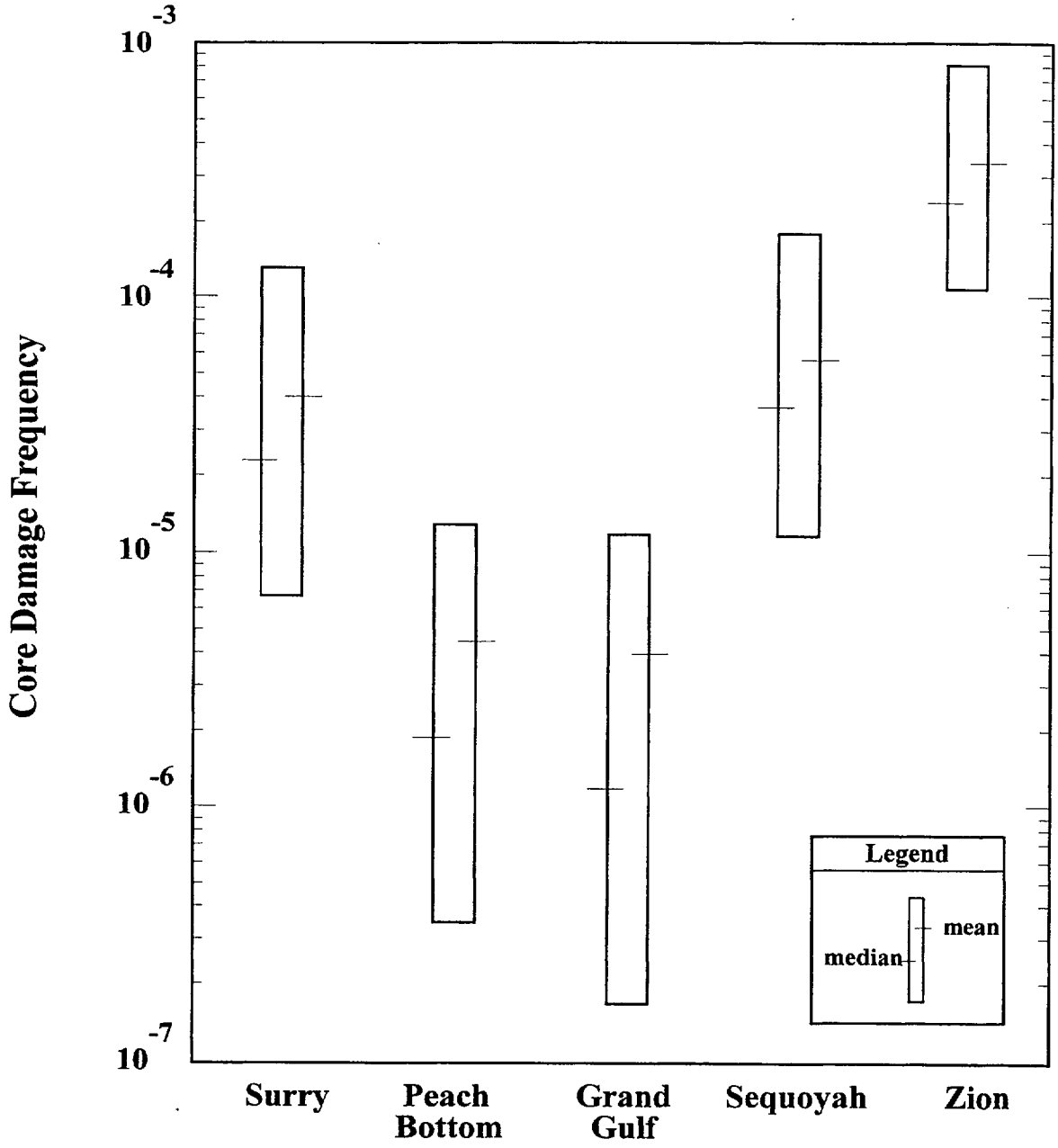


Figure 1A-8 Internal core damage frequency ranges (5th to 95th percentile)

References for Appendix 1A

1. U. S. Nuclear Regulatory Commission, "PRA Course," NUREG/CR-4350, SAND 85-1495, Volumes 1 through 7, August 1985.

2. U. S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 1990.

3. U. S. Nuclear Regulatory Commission, NUREG 75/014, October 1975.

4. D. M. Ericson, Jr., et al., "Analysis of Core Damage Frequency: Internal Events Methodology," U. S. Nuclear Regulatory Commission, NUREG/CR-4550, Vol. 1, Rev. 1, January 1990.

5. G. E. Cummings, "Summary Report on the Seismic Safety Margins Research Program," Lawrence Livermore National Laboratories, NUREG/CR-4431, UCID-20549, January 1986.

6. Seismicity Owners Group and Electric Power Research Institute, "Seismic Hazard Methodology for the Central and Eastern United States," EPRI NP-4726, July 1986.

7. J. M. Lanore, et al., "A Probabilistic Safety Assessment of the Standard French 900 MWe Pressurized Water Reactor," CEA/IPSN- France, EPS 900, April 1990.

8. D. W. Whitehead, "BWR Low Power and Shutdown Accident Sequence Frequencies Project, Phase 2-Detailed Analysis of Pos 5," U. S. Nuclear Regulatory Commission, August 31, 1992.

9. D. W. Whitehead, 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," U. S. Nuclear Regulatory Commission, NUREG/CR-6143, 1994.

10. *U. S. Code of Federal Regulations,* Title 10, Part 73, January 1, 1991.

11. *U. S. Code of Federal Regulations,* Title 10, Part 50, Appendix A, January 1, 1991.

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

13. *U. S. Code of Federal Regulations,* Title 10, Part 50, Appendix R, January 1, 1991.

14. *U. S. Code of Federal Regulations,* Title 10, Part 50.72, January 1, 1991.

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

2.0 Severe Accident Perspectives

2.0.1 Introduction

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 Browns Ferry fire demonstrated that accidents beyond those specifically addressed during design could occur and be very serious. The Reactor Safety Study indicated that such accidents dominate the risk posed by commercial nuclear power plants. Nevertheless, only after the TMI-2 accident occurred in 1979 was there significant regulatory interest in so-called beyond-design-basis accidents.

Events at TMI-2 and Chernobyl forever altered the preexisting mindset that, because plants are designed to be safe, severe accidents are not credible. This chapter discusses the TMI-2 and Chernobyl accidents and their impact commercial reactor regulation. The evolving development and use of information regarding the risks associated with severe accidents is emphasized.

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 regulatory approach taken by the NRC continues to evolve to reflect experience with operating plants and other developments that have safety implications.

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 the design. In fact, experience demonstrates that significant safety improvements can often be achieved with relatively simple, inexpensive changes to existing plants. On the other hand, 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 Chapter 2

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

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

2. Describe the changes that occurred after the TMI-2 accident in:

   a. the NRC
   b. the nuclear industry
   c. nuclear power plants
   d. operator training
   e. emergency response
   f. severe accident research.

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

4. Discuss perspectives provided by individual plant examinations and NUREG-1150 with respect to:

   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.

5. Give three examples of risk-influenced regulations and regulatory guidelines since the TMI-2 accident.

6. Explain the basis for and key elements of NRC's policies and practices with respect to severe accidents and safety goals.

2.1 The TMI-2 Accident

2.1.1 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 PWRs, Unit 1 rated at 792 MWe and Unit 2 rated at 880 MWe. Figure 2.1-1 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 2.1-1 include the core flood tank, the reactor coolant drain tank, and the reactor building sump. The entire nuclear steam supply system depicted in Figure 2.1-1 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]

2.1.2 Pre-existing Problems

The TMI-2 reactor, the 880 MWe unit, was operating at 97% of rated power before the accident. Figure 2.1-2 is a simplified drawing that depicts the pre-accident conditions in the reactor coolant system. Figure 2.1-2 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 2.1-3 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.

2.1.3 Loss of Feedwater

A fairly detailed chronology of the TMI-2 accident is provided in Table 2.1-1. 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 reduced 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 2.1-4. 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 2.1-4.

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

2.1.4.1 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 2.1-4. 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 signaled 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 2.1-4 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 2.1-4.

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.

2.1.4.2 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.

2.1.4.3 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 2.1-4.

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 2.1-4. 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 and the letdown line. The stage was set for a severe accident unless the loss of coolant was diagnosed and corrected.

Figure 2.1-5 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.

2.1.4.4 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 to 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 2.1-6. 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.

2.1.4.5 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 the recovery of measurable steam generator level.

2.1.4.6 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 2.1-7. 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.

2.1.4.7 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% 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 2.1-8 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.

2.1.5 Initial Core Damage (101 min. to 174 min.)

2.1.5.1 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 fact, 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.

2.1.5.2 Hydrogen from Zircaloy Oxidation

Figure 2.1-9 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.

2.1.5.3 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° 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.

2.1.5.4 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 offscale 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 2.1-10 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.

2.1.6 Quenching and Related Core Damage (174 min. to 375 min.)

2.1.6.1 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 2.1-11. 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.

2.1.6.2 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 a pathway by which hydrogen and 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 2.1-12. 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 hot-legs, 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.

2.1.6.3 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 metric tonnes (2×10^4 kg) 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.

2.1.6.4 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.

2.1.7 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.

2.1.7.1 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. 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 2.1-13 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 the 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.

2.1.7.2 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 2.1-14 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.

2.1.7.3 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 2.1-15, the reactor building again isolated, engineered safeguards actuated, and the reactor building sprays came on. Figure 2.1-15 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 2.1-16 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 2.1-17 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.

2.1.7.4 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 2.1-18 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 2.1-19. 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.

2.1.7.5 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 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.

Table 2.1-1 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.

Table 2.1-1 Chronology of Major TMI-2 Accident Events (continued)

Elapsed Time h:min:s	Event or Condition
>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.

Table 2.1-1 Chronology of Major TMI-2 Accident Events (continued)

Elapsed Time h:min:s	Event or Condition
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 2.1-7. 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 2.1-8. 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 2.1-9. 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.

Table 2.1-1 Chronology of Major TMI-2 Accident Events (continued)

Elapsed Time h:min:s	Event or Condition
2:38:23	Letdown cooler A radiation monitor went offscale 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 foot level of the core. 90% of the core exit thermocouples >700°F.
2:48:00	*Figure 2.1-10. 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 2.1-11. 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 2.1-12 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.

Table 2.1-1 Chronology of Major TMI-2 Accident Events (continued)

Elapsed Time h:min:s	Event or Condition
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 hours 42 minutes, 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.

Table 2.1-1 Chronology of Major TMI-2 Accident Events (continued)

Elapsed Time h:min:s	Event or Condition
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 2.1-13. 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 the 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 2.1-14. 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.

Table 2.1-1 Chronology of Major TMI-2 Accident Events (continued)

Elapsed Time h:min:s	Event or Condition
9:50:00	*Figure 2.1-15. 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 2.1-16 Reactor Coolant Pressure Near Minimum (400 psig).*
11:06:00	Pressurizer level decreased to 180 inches in the next 18 minutes. Loop A temperature was increasing.
11:08:00	Second depressurization attempt ends.
13:00:00	*Figure 2.1-17. 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 2.1-18. Repressurized, Flow Blocked by Hydrogen.*
15:33:00	Operator started reactor coolant pump 1A started, ran it for 10 seconds, 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 2.1-19. Forced Circulation Reestablished.*

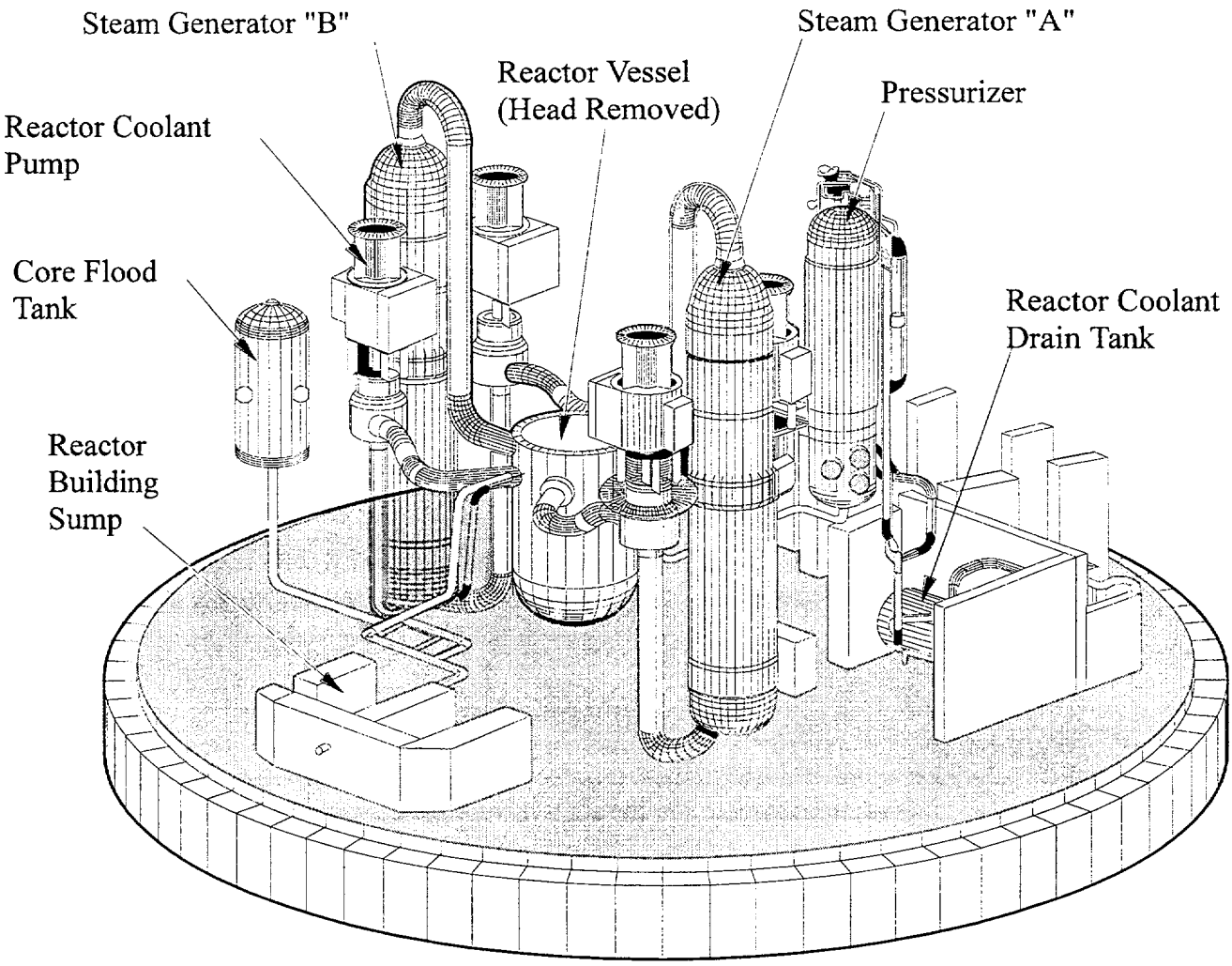


Figure 2.1-1 Arrangement of the primary reactor coolant system and related support system for the Three Mile Island, Unit 2 (TMI-2) Reactor (courtesy of R. Schauss and Construction Systems Associates)

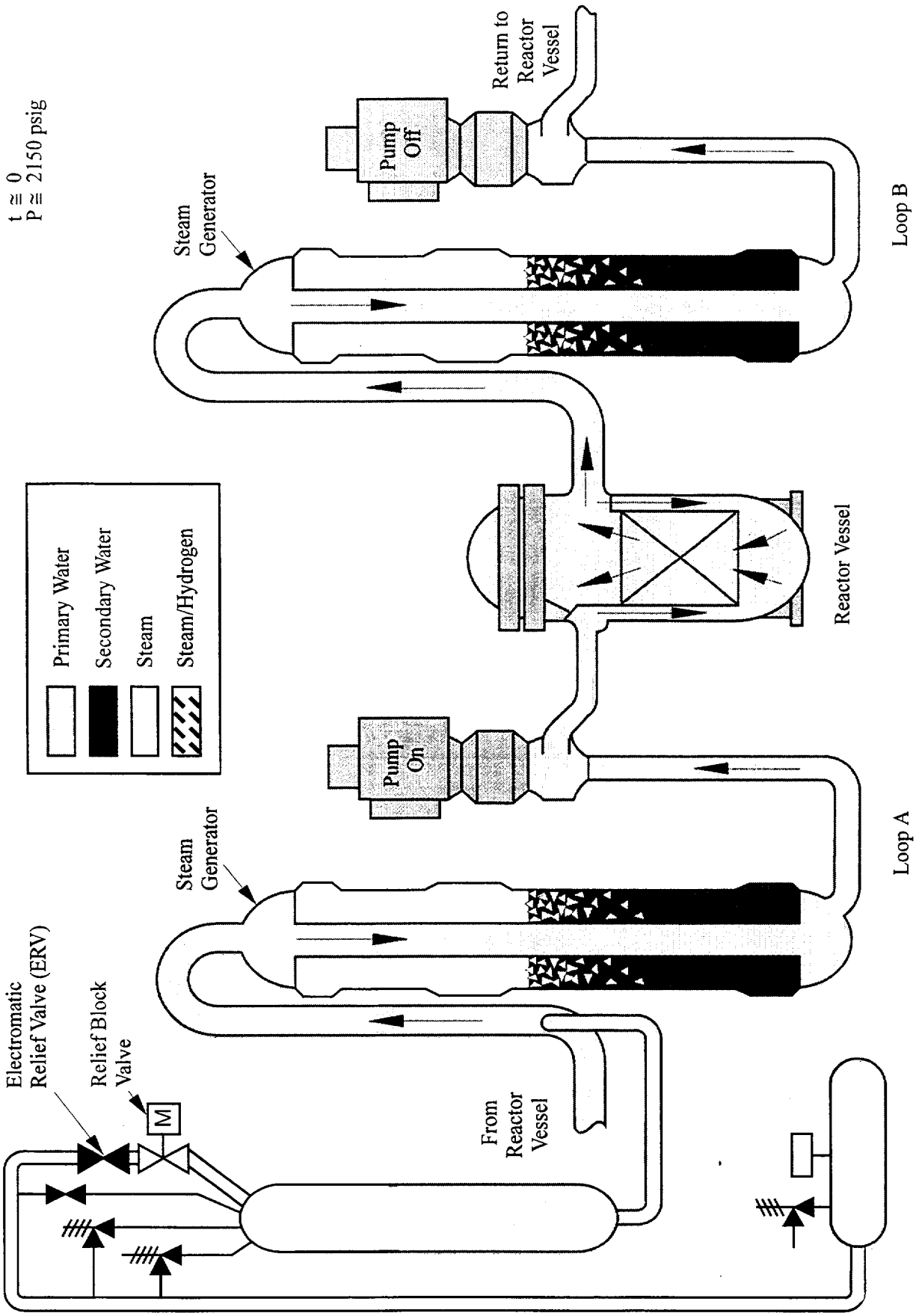


Figure 2.1-2 TMI-2 scenario: initial condition - standby operation at 97% power

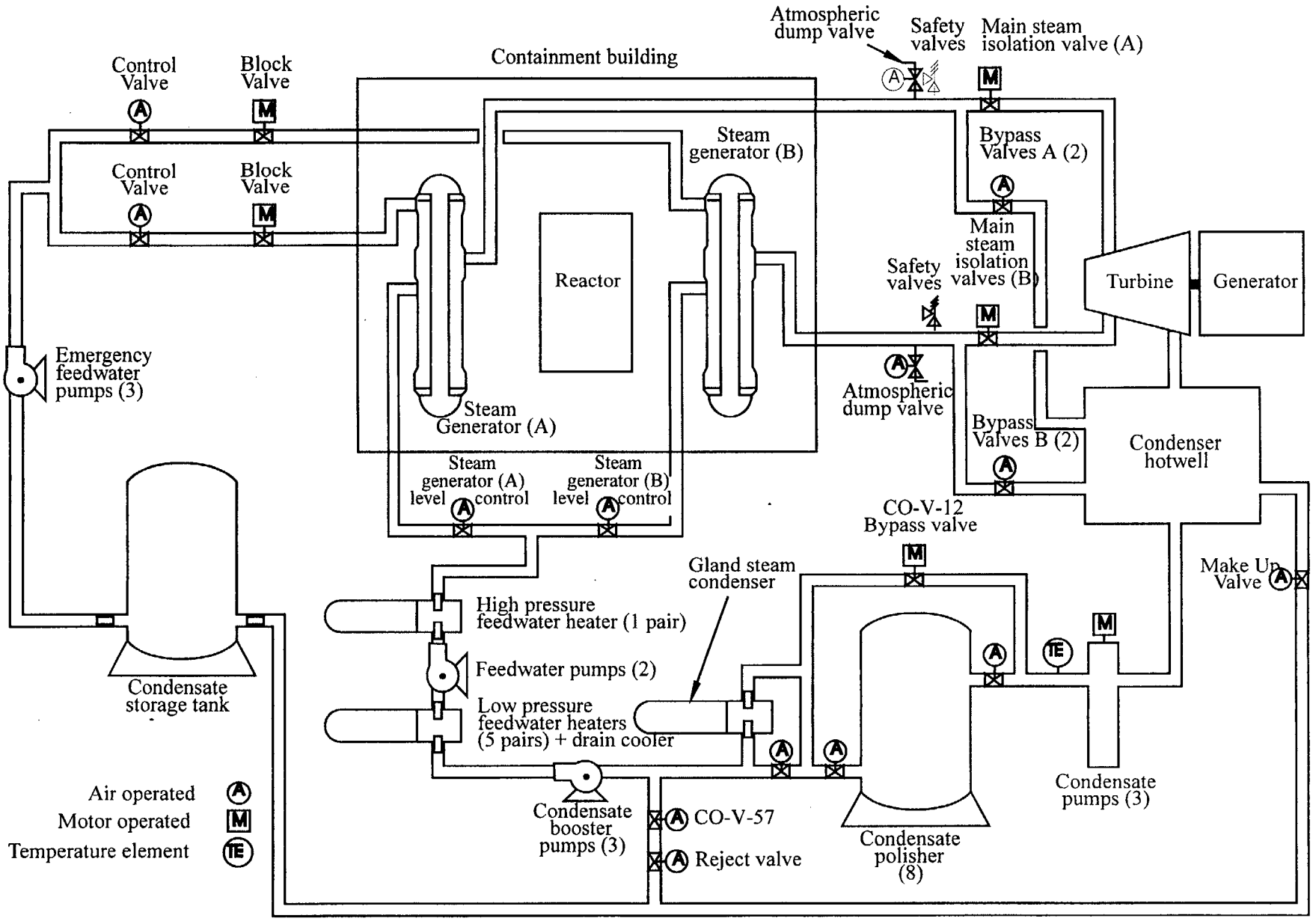


Figure 2.1-3 Condensate and feedwater systems

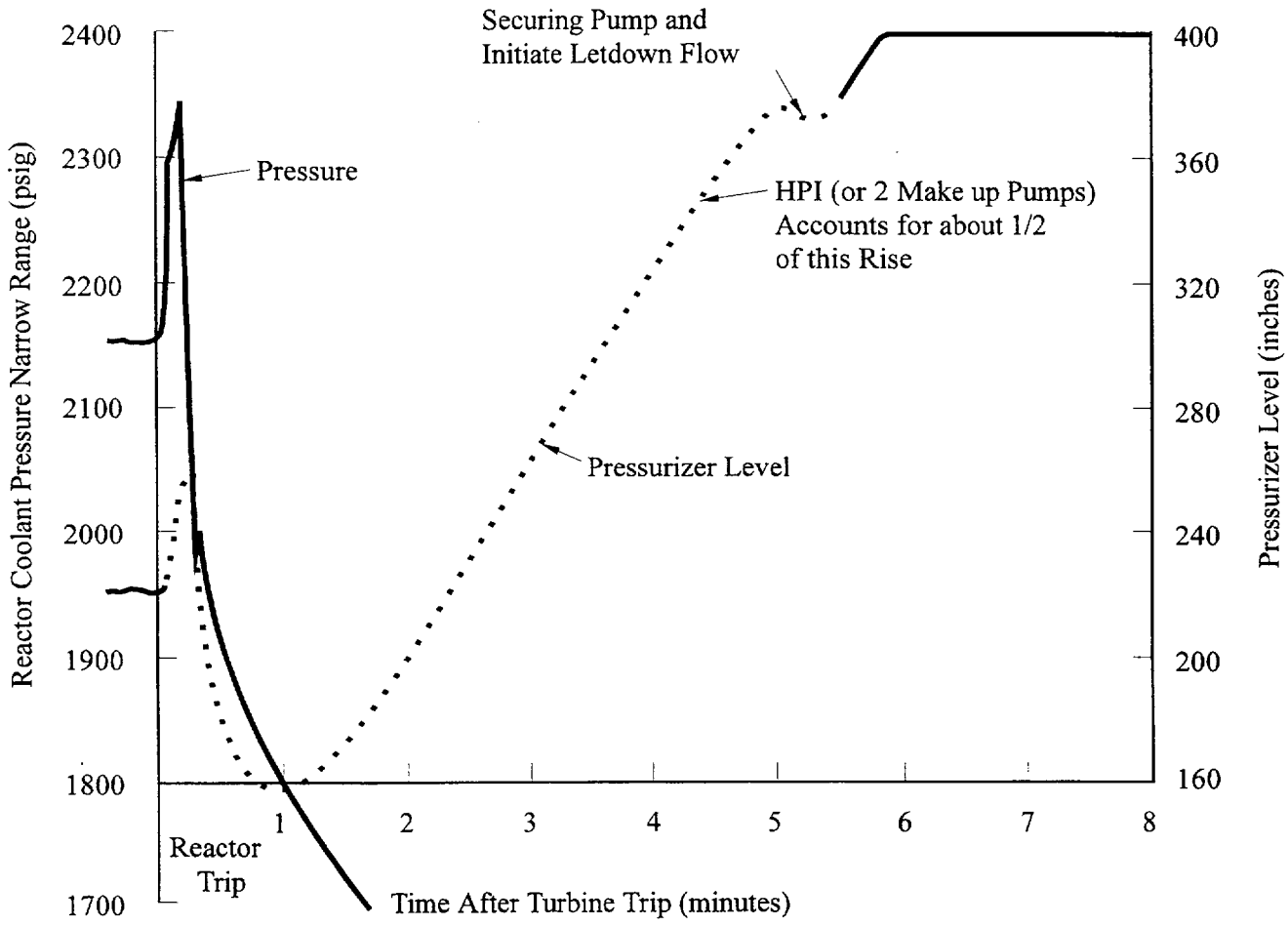


Figure 2.1-4 TMI-2 scenario: reactor coolant pressure and pressurizer level vs. time

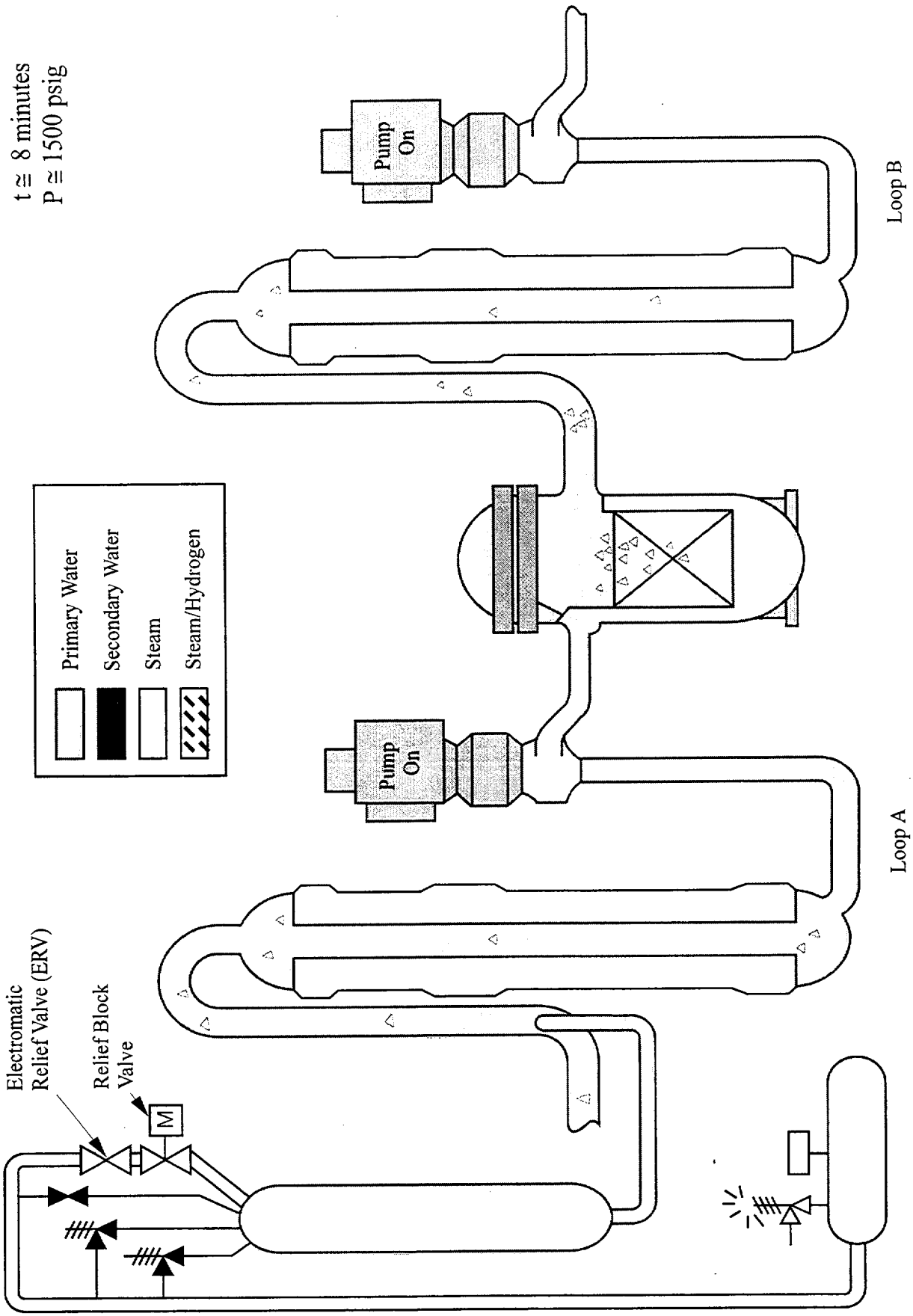
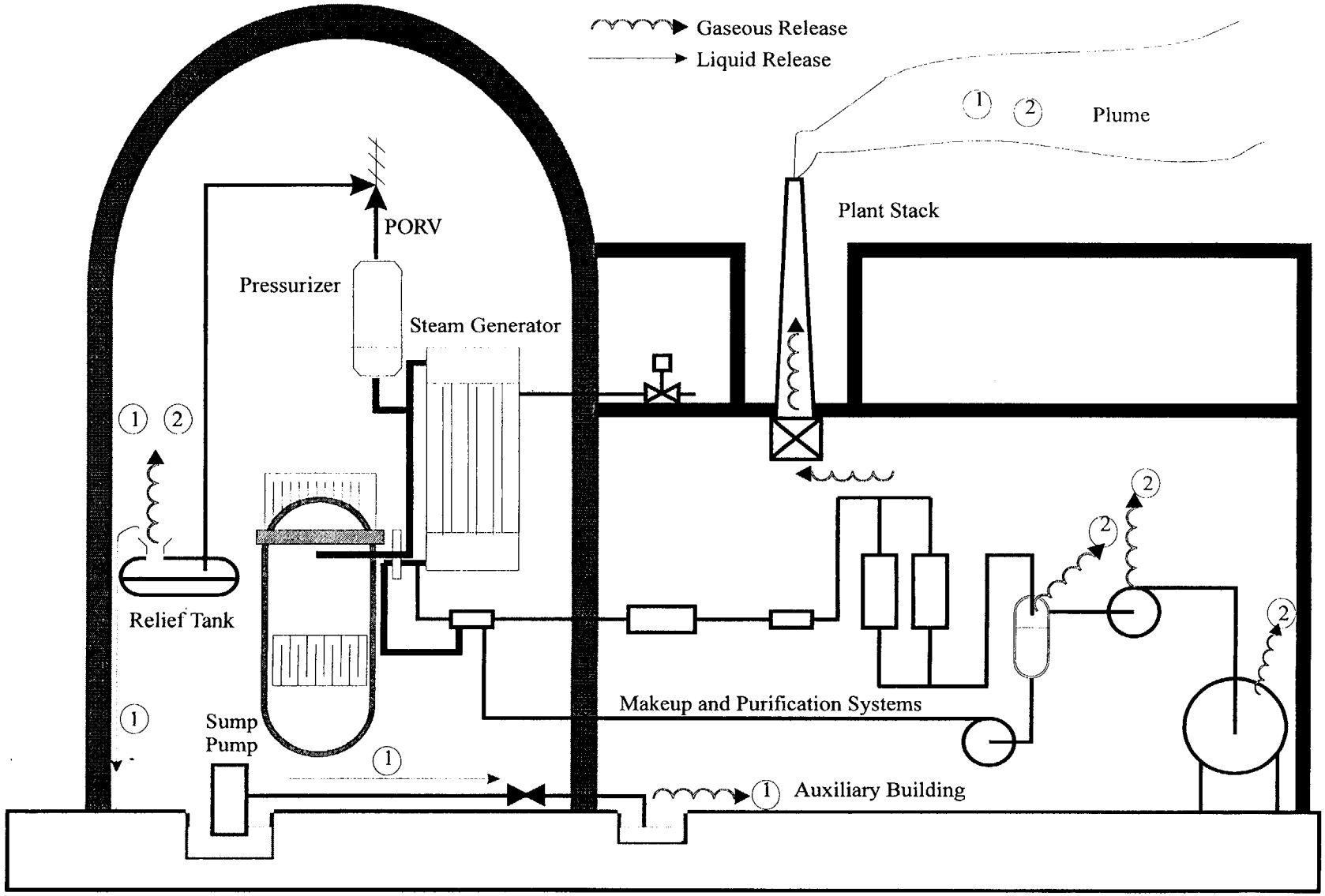


Figure 2.1-5 TMI-2 scenario: system nearly liquid solid, liquid expanding with increasing temperature



1. Early (first 38 minutes) 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 2.1-6 TMI-2 accident radioisotope release pathways

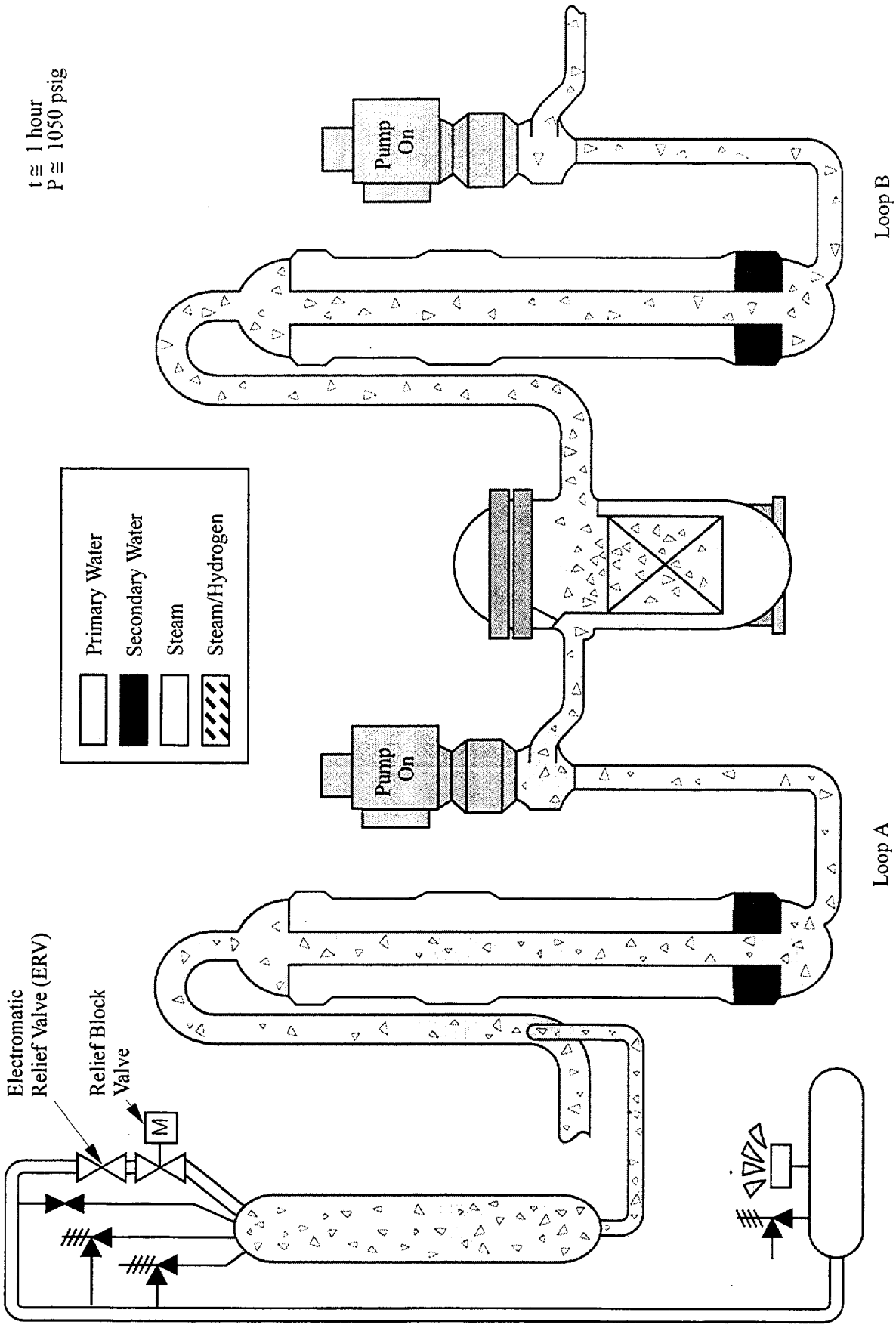


Figure 2.1-7 TMI-2 scenario: primary system pressure and temperatures nearly constant following secondary steam condition, primary voids increasing

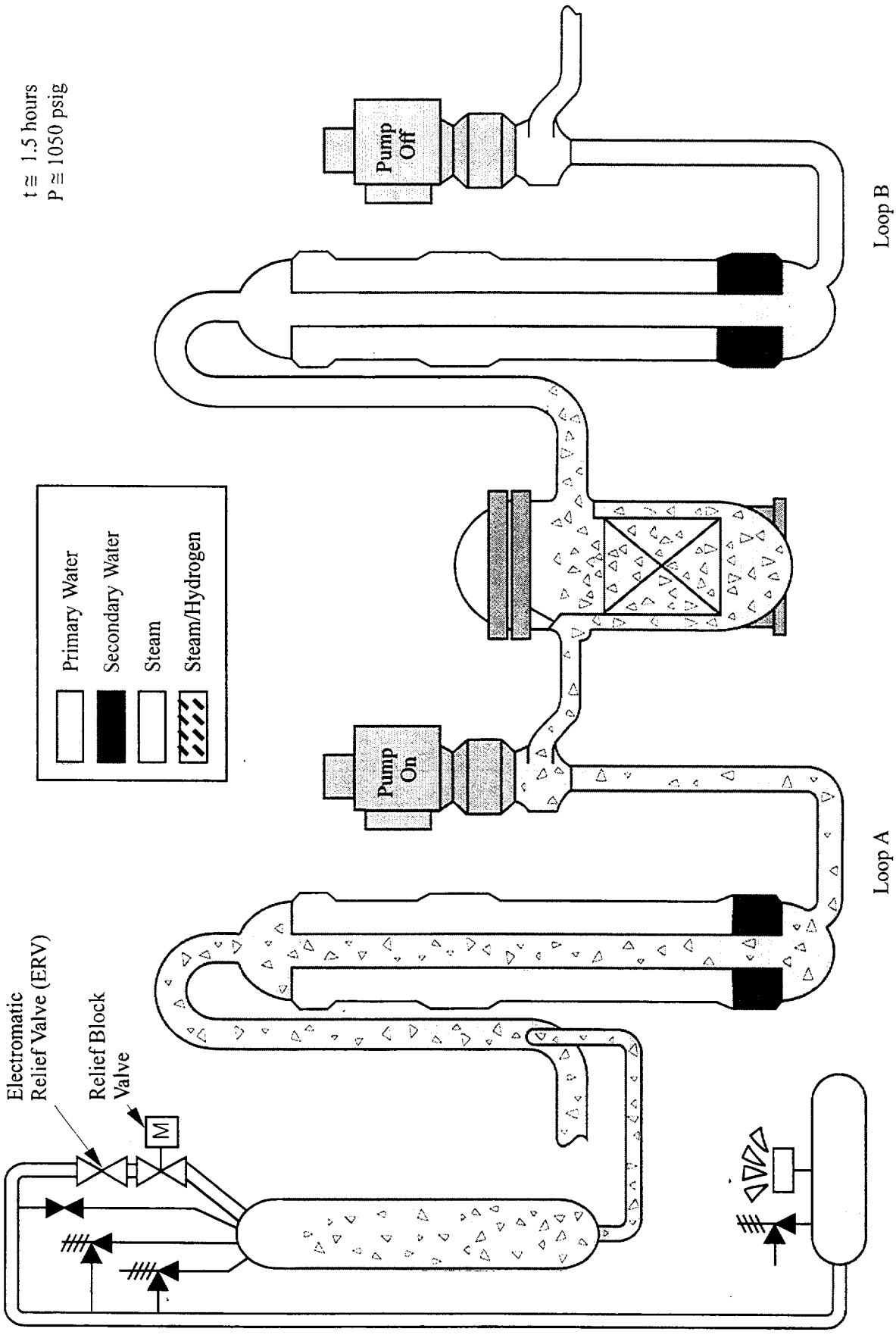


Figure 2.1-8 TMI-2 scenario: loop A pumps operating, loop B stagnant after shutdown of loop B pumps, primary voids increasing

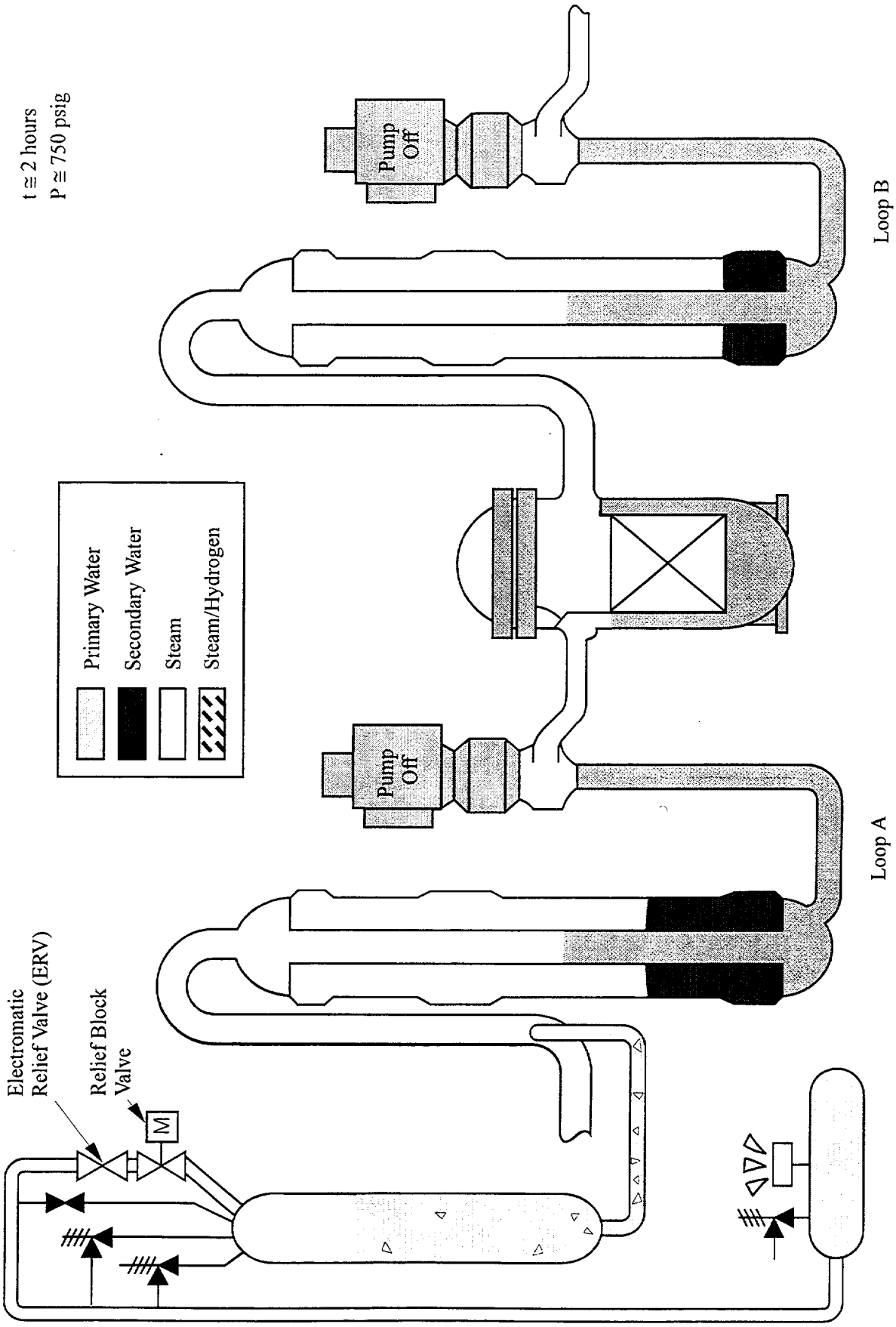


Figure 2.1-9 TMI-2 scenario: all pumps off, reactor core drying out and heating up, superheated steam flowing to pressurizer and to one steam generator and condensing

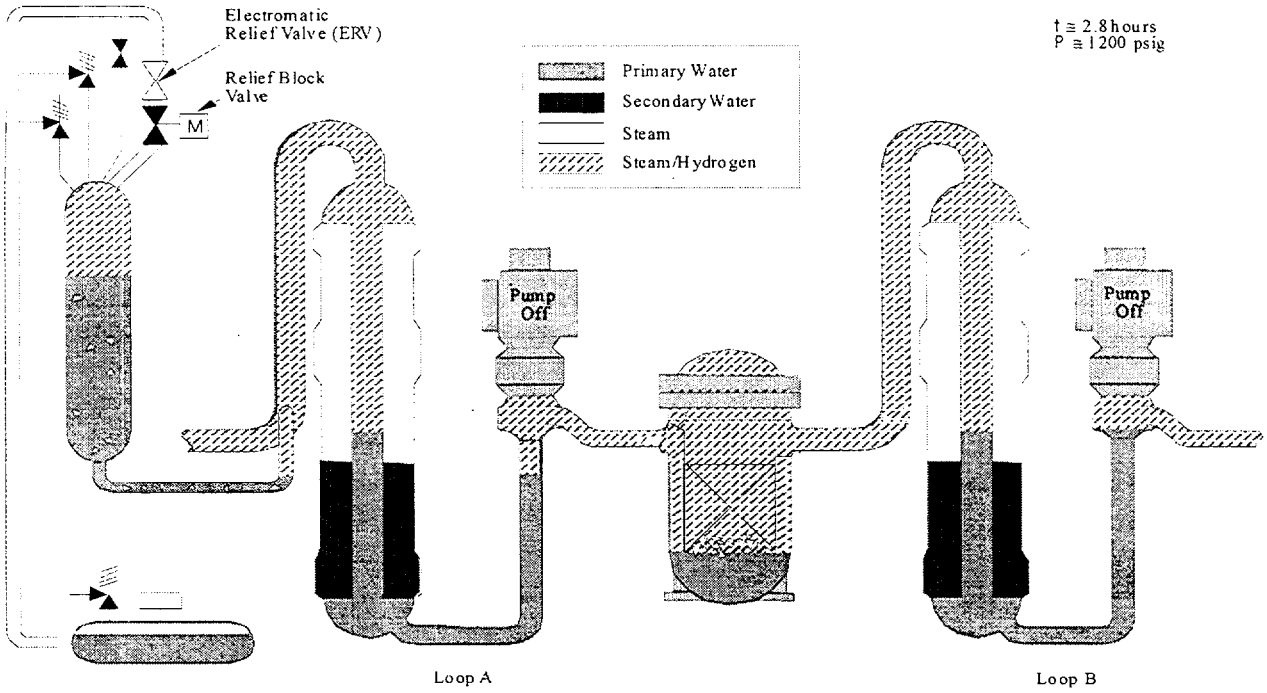


Figure 2.1-10 TMI-2 scenario: core dryout and heatup continuing, hydrogen generation by steam - zirconium reaction in hotter regions

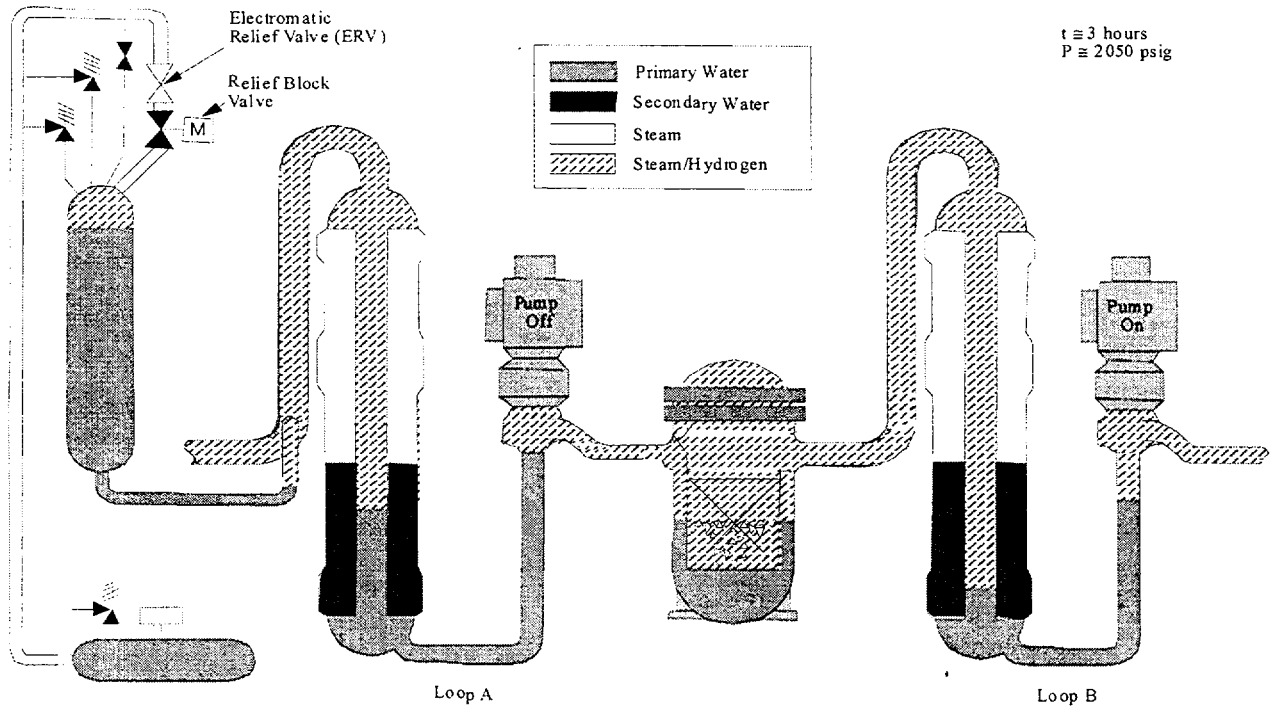


Figure 2.1-11 TMI-2 scenario: core partially quenched by fluid during loop B pump start, heatup resumes

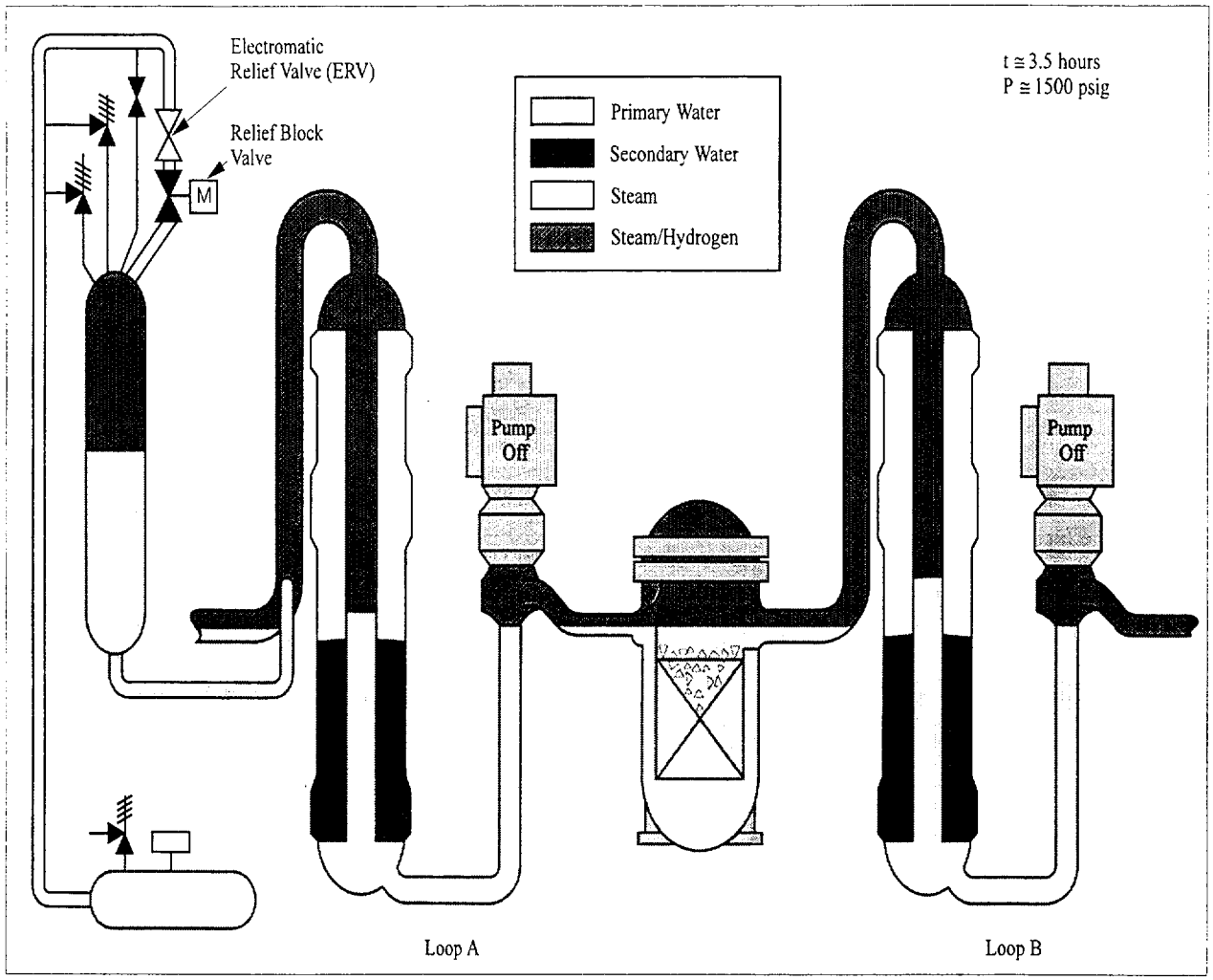


Figure 2.1-12 TMI-2 reactor vessel refilled by manual initiation of safety injection, core temperatures decreasing

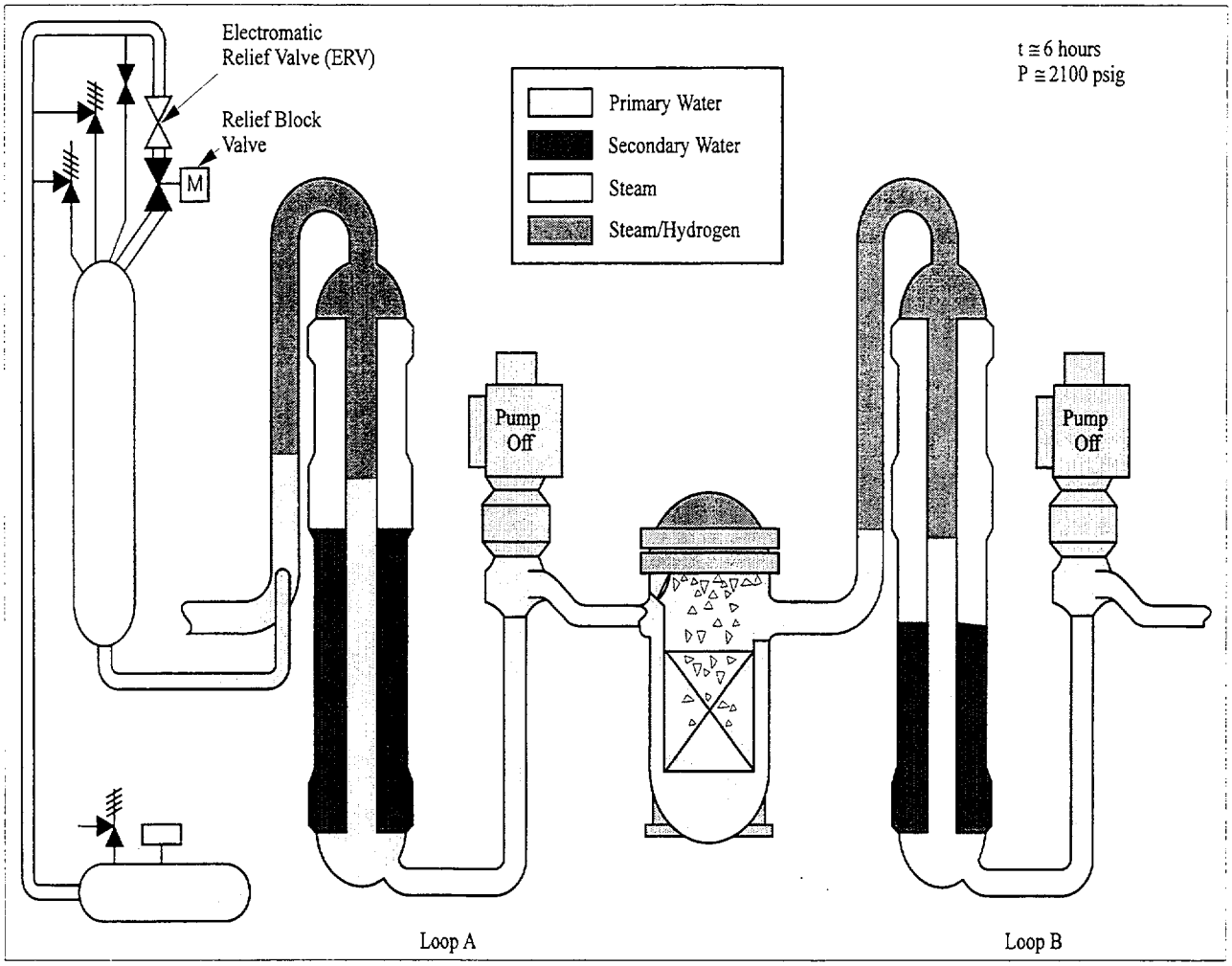


Figure 2.1-13 TMI-2 scenario: system pressurized by high-pressure injection system intermittent liquid release through top of pressurizer, heat removal by heatup of injected water, steam generator heat transfer blocked by hydrogen

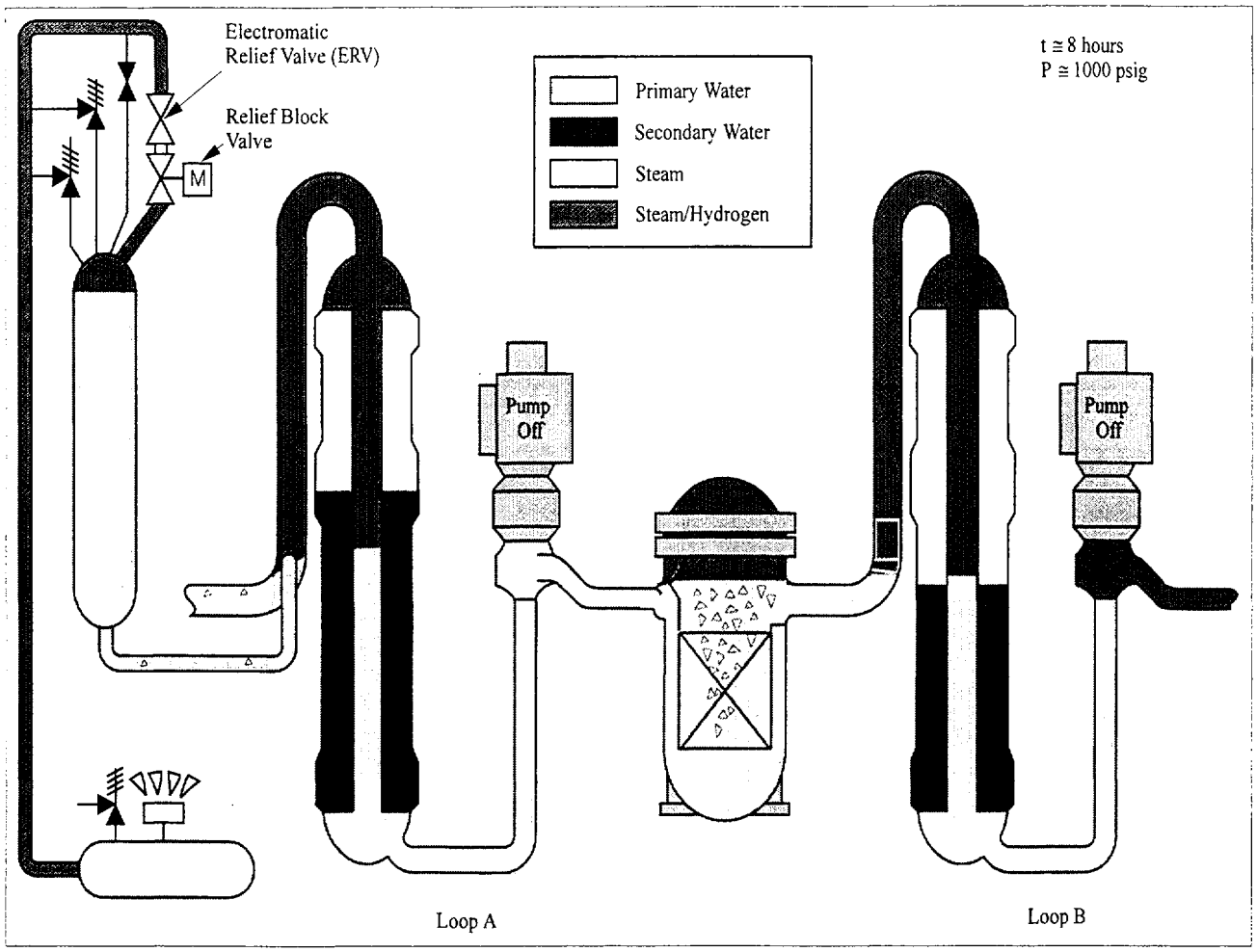


Figure 2.1-14 TMI-2 scenario: primary system depressurizing and releasing hydrogen through the pressurizer into the containment

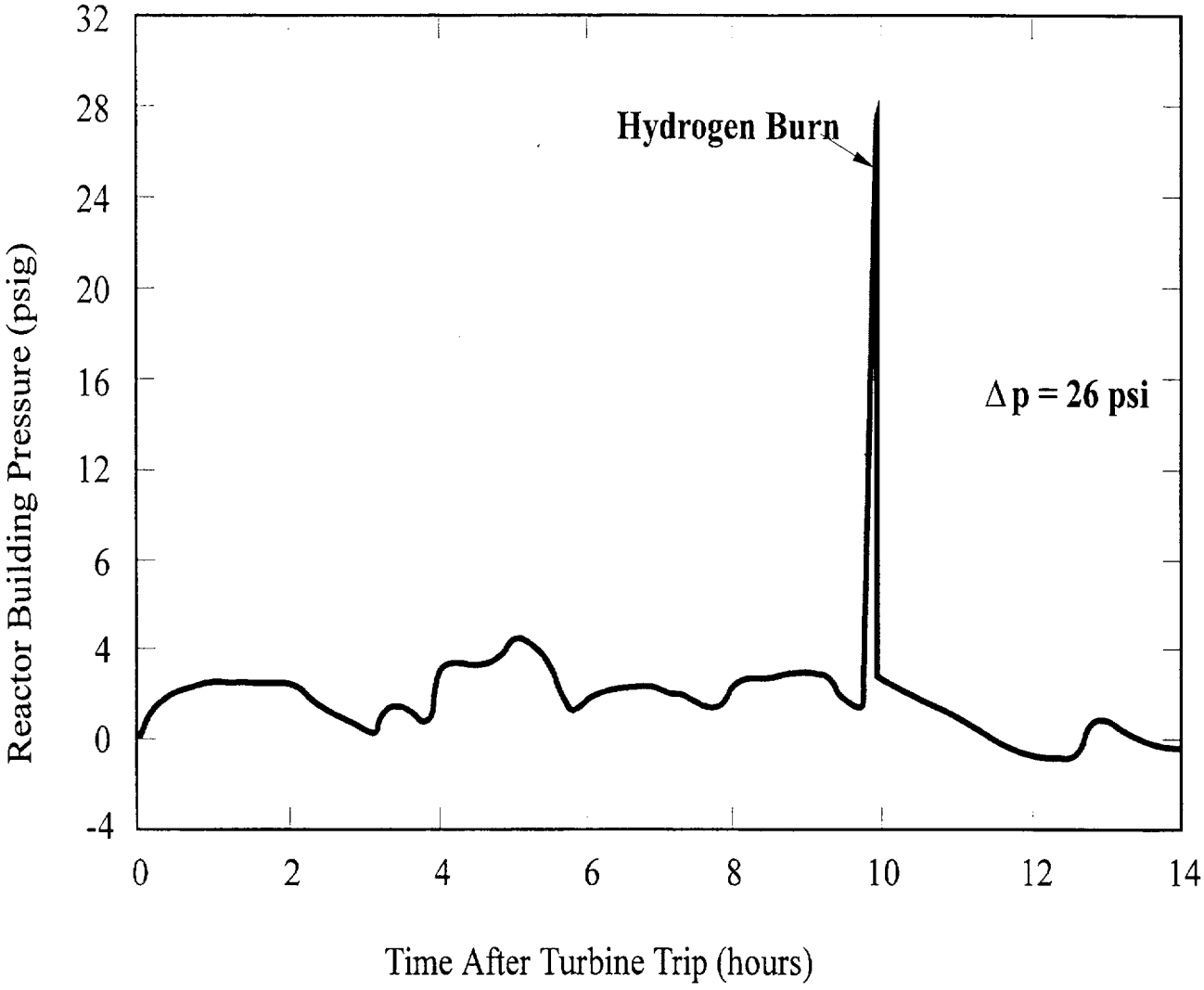


Figure 2.1-15 TMI-2 containment pressure versus time

References for Section 2.1

1. U.S. Nuclear Regulatory Commission, "Investigation Into The March 28, 1979 Three Mile Island Accident by Office of Inspection and Enforcement," NUREG-0600, 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," U. S. Nuclear Regulatory Commission, NUREG/CR-1250, Volume II Part 2, January 1980.

4. U. S. Nuclear Regulatory Commission, "TMI-2 Lessons Learned Task Force" Final Report, NUREG-0585, 1980.

5. U. S. Nuclear Regulatory Commission, "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.

2.2 TMI-2 Implications

2.2.1 Introduction

The TMI-2 accident put to rest the notion that severe nuclear power plant accidents were not credible. Failure to diagnose and compensate for loss of coolant from the stuck open PORV led to substantial core damage (oxidation and melting), which is discussed further in Chapter 3. Yet, in spite of the extensive core damage and the combustion of hydrogen in containment, the radionuclide releases to the environment were 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[1] (see Section 2.2.4). 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.[2] 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.[3,4] 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.

2.2.2 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 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., inspection and enforcement, operating experience, and research) 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. The 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 four areas (operations, maintenance, engineering, and plant support). 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.

2.2.3 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.[2]

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 industry-wide 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 industry-wide basis.

2.2.4 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.[1] The items approved for implementation by NRC are identified in the

report "Clarification of TMI Action Plan Requirements" (NUREG-0737, November 1980).[5] The staff issued further criteria on auxiliary feedwater system improvements (derived from NUREG-0667), and instrumentation (Regulatory Guide 1.97, Revision 2).[6,7] 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, attention had been on the design-basis large break LOCA. A major shift in emphasis toward small breaks and transients resulted from 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 LOCAs. 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 Chapter 4.

2.2.5 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, 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.

2.2.6 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 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.[8] 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.

2.2.7 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 1980) 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.[11] 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 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.[12] Therefore, in cases in which state and/or local officials declined to participate in emergency planning, the NRC and FEMA 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.

2.2.8 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).[13] 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 chapters.

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 IDCOR group concentrated on developing models for assessing the risks of severe accidents. IDCOR models were used to analyze four of the five NUREG-1150 reference plants. This facilitated the identification and resolution of modeling differences.

2.2.9 Severe Accident Policy

In August 1985, when the bulk of the actions required by the TMI Action Plan had been completed, the NRC issued a policy statement on severe accidents.[14] 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.[15,16] 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 IPE 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.

IPE results were to be reported to the NRC within three years according to guidance provided in NUREG-1335. The results of the IPEs have been reviewed by the NRC. Section 2.5 provides a discussion of these results, which will be used, in part, to deal with Unresolved Safety Issues and Generic Safety Issues. The IPE submittals indicate

whether particular issues apply to the plant and the utility's case for resolution.

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.

References for Section 2.2

1. U. S. Nuclear Regulatory Commission, "NRC Action Plan Developed as a Result of the TMI-2 Accident," NUREG-0660, May 1980.

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

3. M. Rogovin, et al., "Three Mile Island, A Report to the Commissioners and to the Public," U. S. Nuclear Regulatory Commission, NUREG/CR-1250, January 1980.

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

5. U. S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements," NUREG-0737, November 1980.

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

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

8. U.S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements," NUREG-0737, Supplement 1, January 1983.

9. *Federal Register,* Vol. 45, 55,402, August 19, 1980.

10. J. Samuel Walker, "A Short History of Nuclear Regulation 1946-1990," Historical Office, Office of the Secretary, Nuclear Regulatory Commission, June 1991, p.38.

11. U. S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five US Nuclear Power Plants," NUREG-1150, December 1990.

12. *Federal Register*, Vol. 50, 32,138, August 8, 1985.

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

14. U. S. Nuclear Regulatory Commission, "Individual Plant Examination: Submittal Guidance," NUREG-1335, August 1989.

2.3 The Chernobyl Accident

The worst nuclear power plant accident occurred on April 26, 1986 at unit 4 of the nuclear power station at Chernobyl in the Ukraine. A violent explosion destroyed the Chernobyl-4 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 that lasted several days. The areas around the plant were highly contaminated and 31 workers died, 28 from acute radiation sickness.

The radioactive plume spread far into other parts of the former 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.[1]

In many ways, the pre-Chernobyl attitude toward nuclear safety in the former Soviet Union was similar to the pre-TMI attitude in the United States. Influenced by the "it can't happen" mindset, operating personnel who were impatient to conduct a test took actions that violated procedures and began the accident. The accident took on catastrophic proportions as the result of undesirable reactor design features.[2] 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.

2.3.1 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 2.3-1, the RBMK design is a graphite-moderated, light water cooled, pressure tube reactor.[3] The RBMK-1000 design generates approximately 1000 MWe. The reactor has 1661 vertical pressure tubes that contain 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.

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. The Russian design document speaks of compartmentalized containment to limit the spread of radionuclides in the event of a pipe rupture. Much of the primary system piping is contained in small concrete compartments. Each compartment is designed to withstand a double-ended guillotine break of the largest pipe in the compartment. The structure surrounding the reactor was designed to withstand the rupture of 3 pressure tubes.

2.3.2 The Chernobyl Experiment

The Chernobyl accident began on April 25 with an experiment.[1] The experiment was a test designed 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 members 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.

2.3.3 The Sequence of Events

The material in this section was taken primarily from a September 11, 1986 special issue of *Nuclear News*.[3] 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 was 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% (3200 MWt) to half that power. 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 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 over-compensated, 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 resulting in 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 2.3-1, 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.

2.3.4 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/lb_m (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.

2.3.5 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. In addition, as discussed in Chapter 4, all U.S. power reactors employ large strong containment structures. Such a structure might not have been effective against the enormous energy releases of Chernobyl, but would be effective in many postulated severe accidents at U.S. plants.

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 from Chernobyl in many other 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 N Reactor.

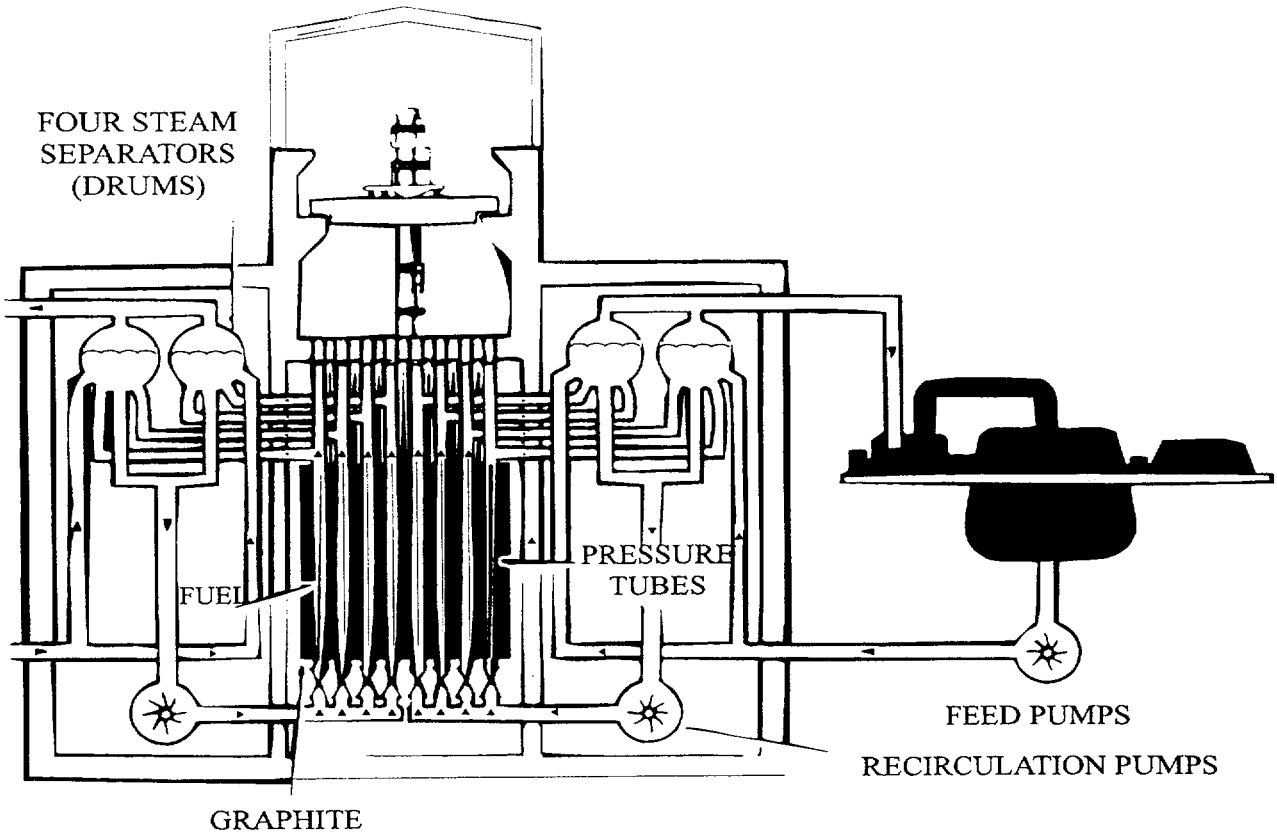
Supporters of nuclear power emphasized that a Chernobyl-type accident could not occur in commercial U.S. plants (or other nations), which featured safety systems and containments to prevent the release of radionuclides. But nuclear critics pointed to Chernobyl as the prime example of the hazards of nuclear 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.

The Chernobyl accident could not be repeated at a U.S. nuclear power plant due to fundamental differences in reactor design. Nevertheless, risk assessments of U.S. plants have identified possible severe accidents in which containment fails and very large releases of radionuclides occur. Most of these releases would not be accompanied by explosions or fires like those at Chernobyl where the radioactive plume was lofted high into the atmosphere and away from local residents. As discussed in Chapter 5, a large release from U.S. plant could, under unfavorable meteorological conditions, result in more early fatalities than occurred at Chernobyl. While uncontained severe accidents leading to such releases are not considered likely, one should avoid the mindset that "it can't happen here."

Table 2.3-1 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.



Schematic diagram of the RBMK-1000, a heterogeneous water-graphite channel-type reactor (source: Soviet report to IAEA)*

*Reprinted with special permission from IAEA

Figure 2.3-1 Boiling water pressure tube graphite moderated reactor

References for Section 2.3

1. R. A. Knief, "Nuclear Engineering, Theory and Technology of Commercial Nuclear Power," Second Edition, Hemisphere Publishing, 1992, p. 458.

2. N. A. Shteynberg et al., "On the Causes and Circumstances of the Accident at Unit 4 of Chernobyl Nuclear Power Plant on 26 April 1986," Report of USSR GPAN Commission, NRC Translation 2932, 1991.

3. American Nuclear Society, "Special Report," *Nuclear News*, La Grange Park, Illinois, September 11, 1986.

2.4 Risk Influences and the Development of Safety Goals

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. Quantitative risk limits have not generally been imposed in NRC regulations; however, quantitative risk estimates do provide supporting rationale and impetus for regulatory decisions. As PRA has improved over the years, the weight given to quantitative risk estimates has increased.

The next sections describe the role that quantitative risk estimates played in addressing past important regulatory issues. Then, the development of the backfit rule and safety goals are discussed.

2.4.1 Past Risk-Influenced Regulatory Practices

Risk considerations, both qualitative and quantitative, have influenced a number of existing regulations and in fact have always been present in the minds of decision makers. The remainder of this section will give examples illustrating how the consideration of risk has evolved from an ad hoc approach to a more systematic process.

2.4.1.1 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 1.4-1). An "anticipated transient without scram" or ATWS event would occur if the RPS failed to scram the reactor given such a transient. Appendix 2B provides more information about the RPS and ATWS.

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. This concern was based on 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.

ACRS member S. H. 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 Oak Ridge National Laboratory (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 performed these analyses.

WASH-1270

In September 1973 the NRC publicly adopted a position on ATWS with the

publication of the WASH-1270 report.[4] Along with providing for important plant design changes, an 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.

Unfortunately, the resolution of ATWS was short lived. In the ensuing years a number of positions were taken by the NRC and the industry. In 1975 the NRC proposed additional design changes. The industry countered by pointing out that the Reactor Safety Study did not show ATWS as a major contributor to risk for LWRs. The industry followed up with a series of reports indicating low risk to the public.

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 (5×10^{-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.

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.

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.

Due to the serious nature of Salem 1 ATWS event, the NRC issued Inspection and Enforcement Bulletin No. 83-01[6] on the same day (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 satisfactorily 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).[7] 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.[8] 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.

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.[9] 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. Appendix 2B reproduces the final ATWS rule and also discusses the key changes that were considered.[10]

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.[11] Industry response to this challenge has been positive as indicated in Figure 2.4-1.

Interestingly, the final rule says nothing about quantitative risk goals. In this case, risk arguments provided the impetus for the rule but are not present in the final rule.

2.4.1.2 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. In July 1981, Section 10.4.9 of the Standard Review Plan[12] required that, as part of their review, the NRC assure that an AFWS reliability analysis be performed in accordance with NUREG-0737[11] using the methodology defined in NUREG-0611[13] and NUREG-0635.[14] 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.[15] The new guidance called for operating plants to demonstrate a 10^{-4} unreliability using plant-specific data. This guidance is an example of the use of quantitative risk estimates, although they apply only to a particular system and not to the risk of a severe accident.

2.4.1.3 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.[16] 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 2.4-1 and the following important findings regarding station blackout.[17]

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,[18] 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.[19]

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 2.4.1.1) 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,[20] which was prepared for the resolution of Generic Safety Issue B-56, "Diesel Reliability."

2.4.1.4 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 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.

Implementation of the Backfit Rule continues to evolve, due to ambiguity concerning terms like "substantial additional protection." The "cost justified" standard is changing due to revised economic analysis. Previously, the cost benchmark had been $1000/person-rem. Changes that cost less

than this amount were considered cost justified. That benchmark was changed in 1995 to $2000/person-rem.[29,30] Processes for performing these calculations are also evolving, as PRA technology improves.

2.4.2 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.[31]

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) and are intended to apply to the industry as a whole, rather than individual plants. However, an actual safety goal implementation approach is still evolving as discussed in Section 2.6. Since 1986 the NRC has struggled with implementation and the possible inclusion of "subsidiary" safety goals. For example, one topic 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,"

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.[32] 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. Current views on the subsidiary goals are contained in Section 2.6.

The NRC has not yet attempted to apply the 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.

2.4.3 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 2.4.1.1. Subsequently, as noted in Section 2.2, the TMI-2 investigators recommended that the NRC explicitly identify a safety goal -- a level of risk at which reactors would be safe enough. As discussed in the previous sections, the NRC established both qualitative and quantitative safety goals in August 1986 to more clearly delineate acceptable levels of risk.[29]

Despite the concerns noted in the previous section, implementation of the Safety Goal Policy began to take shape in the form of guidance for backfitting. The evolution of the Backfit Rule was discussed in detail in Section 2.4.1.4. 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.[33] The approach is based on comparison of the core damage frequency to 10^{-4} per year and the conditional containment failure probability (as a surrogate for large release) to 10^{-6} per reactor year. Figure 2.4-2 summarizes the interim implementation guidance. A proposed backfit would be evaluated in terms of core damage frequency and conditional containment failure probability. Figure 2.4-2 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 and other regulatory analyses 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-informed 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) and other plant-specific PRAs, as discussed in Section 2.5.

Table 2.4-1 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}

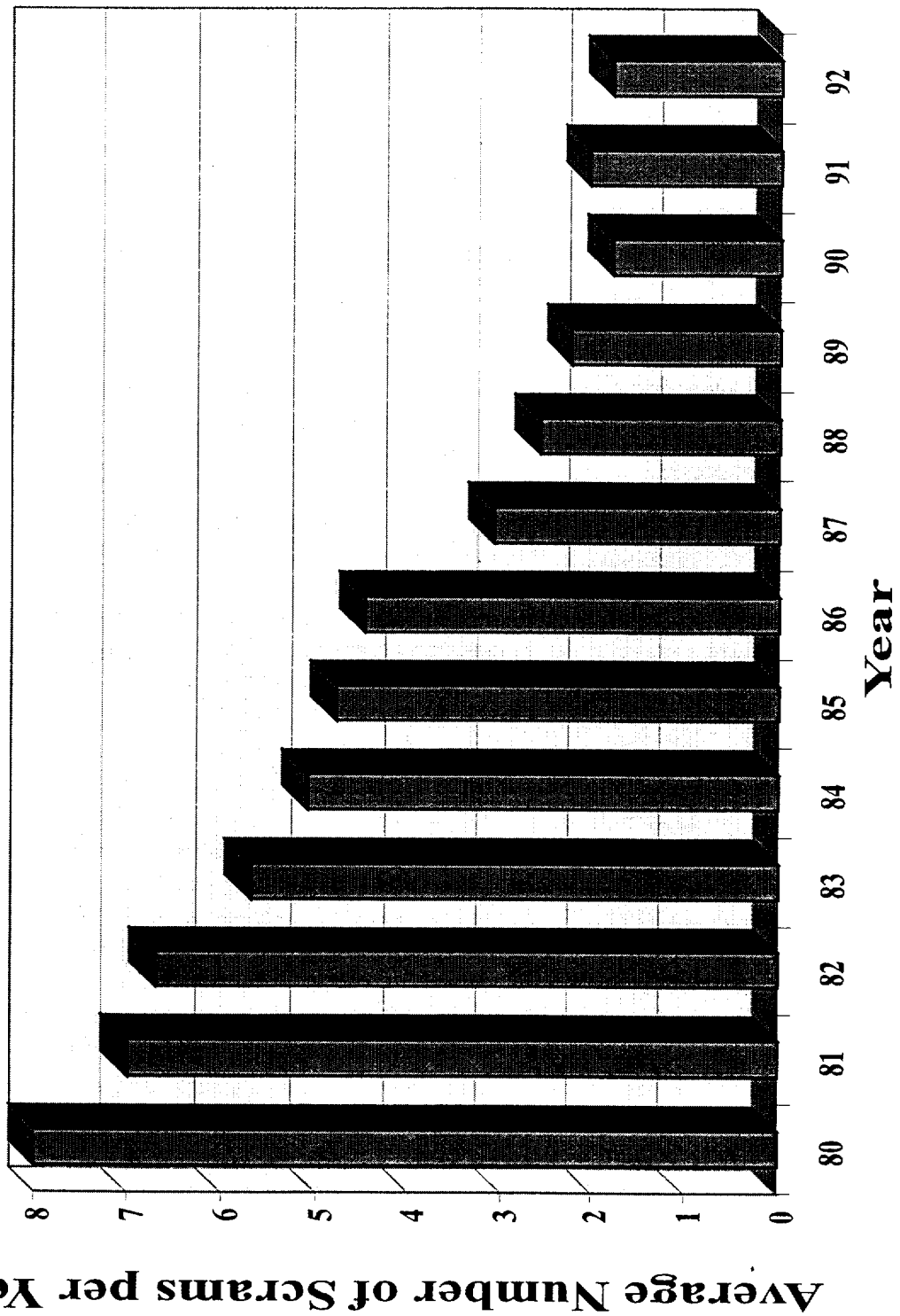


Figure 2.4-1 Average number of scrams per year

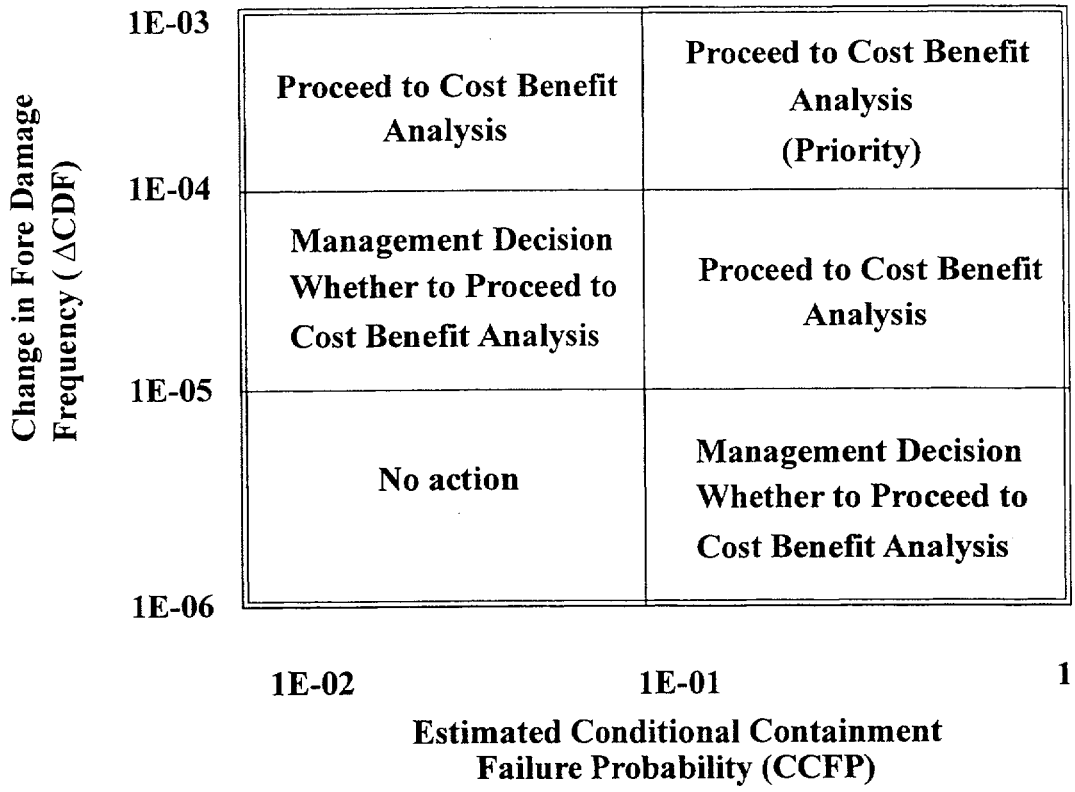


Figure 2.4-2 Safety Goal Implementation Guidance

References for Section 2.4

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, Wisconsin, 1981, p. 239.
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. 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.
7. 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.
8. U. S. Nuclear Regulatory Commission, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," NUREG-1000, Vol. 1, April 1983.
9. 46 FR 57521, "Proposed ATWS Rule," November 24, 1981.
10. 49 FR 26036, "Statement of Considerations for ATWS Rule," June 26, 1984.
11. U. S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements," NUREG-0737, November 1980, Item II.E.1.1.
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. U. S. Nuclear Regulatory Commission, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants," NUREG-0611, January 1980, Appendix III and Annex 1 of Appendix X.
14. U. S. Nuclear Regulatory Commission, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants," NUREG-0635, January 1980, Appendix III and Annex 1 of Appendix X.
15. U. S. Nuclear Regulatory Commission, "A Prioritization of Generic Safety Issues", NUREG-0933, December 1986.
16. "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, October 1975.

17. U. S. Nuclear Regulatory Commission, "Evaluation of Station Blackout Accidents at Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-44," NUREG-1032, June 1988, p. 1-1.

18. 10 CFR 50.63, "Loss of All Alternating Current Power," July 21, 1988.

19. 53 FR 23203, "Statement of Considerations for Final Station Blackout Rule," June 21, 1988.

20. 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.

21. *U. S. Code of Federal Regulations*, Title 10, Part 50.109.

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

23. *U. S. Code of Federal Regulations*, Title 10, 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.

29. U. S. Nuclear Regulatory Commission, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission," Final Report, Revision 2, NUREG/BR-0058, November 1995.

30. U. S. Nuclear Regulatory Commission, "Reassessment of NRC's Dollar Per Person-Rem Conversion Factor Policy," NUREG-1530, December 1995.

31. *U. S. Code of Federal Regulations*, Title 10, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement, *Federal Register*, August 4, 1986.

32. 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.

33. 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