2.5 Risk Assessment and Operational Perspectives

Utilities are required to report plant operating data to the NRC under certain circumstances. The NRC uses this information for various safety purposes, ranging from deciding whether a plant may continue to operate after occurrence of an event to assessing long term trends in equipment failures. The range of information that is reported and the NRC's use of the information is described in this section. In addition, as discussed in Section 2.4 and 2.6, estimates of core damage frequency and other risk measures are increasingly being used to resolve safety issues, set policies, and make safety decisions. Because of this, it is important to understand the current estimates of risk for commercial nuclear power plants. This section provides a summary of key risk analyses that have been performed and the current understanding of risk based on these analyses.

2.5.1 Operating Plant Data

Each year the NRC receives an extensive amount of information from licensees and other sources regarding nuclear power plant experience. Table 2.5-1 lists some of the sources of information and indicates those that are required by law. Prompt phone notifications and written Licensee Event Reports (required by 10 CFR 50.72 and 10 CFR 50.73) are the predominant sources of information having potential safety implications.[1,2] The NRC systematically reviews and analyzes the information it receives to identify instances where the margin of safety established through licensing has been degraded. In such cases, the NRC then identifies and implements corrective actions that will restore the originally intended margin of safety. Any proposed improvements in this margin of safety must be separately identified and justified as new licensing actions.

The feedback of operating data or experience is an inherent and important aspect of NRC activities and involves all NRC organizational elements at one time or another. The principal NRC organizations involved are the Office of Nuclear Reactor Regulation (NRR) and, previously, the Office for Analysis and Evaluation of Operational Data (AEOD). AEOD was established several months after the TMI-2 accident to identify and feed back significant safety lessons of operational experience to the NRC, its licensees, the nuclear industry as a whole, and the public. In the 1990s, AEOD was dissolved and its functions were moved into NRR and the Office of Nuclear Regulatory Research (RES). Table 2.5-2 lists some of the NRC-originated documents that are used to disseminate relevant nuclear power plant experience. Of particular interest to licensees are Bulletins, Information Notices, and NRR Generic Letters.

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

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

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

2.5.2 Precursor Program

Given the years of nuclear power plant experience accrued in the U.S., one would expect a large number of accident sequences that could potentially lead to core damage to have been revealed by incidents involving beyond-design-basis initiators and/or sequences of events. Such incidents are commonly referred to as precursors of severe accidents. The NRC collects and evaluates data for the purpose of identifying such precursors.

When the NRC determines that a particular event, usually identified in a Licensee Event Report (LER), is worth further investigation, the Accident Sequence Precursor (ASP) Program is used to evaluate the potential core damage frequency importance of the event. The ASP program uses a simplified set of event trees and fault trees for the analysis, in essence performing a mini-PRA. The intent of the program is not a high degree of accuracy, but rather, relative insights and selection of events for further NRC study. In the analysis of an event, the probabilities of failure that actually occurred are set to 1.0 and additional failures that could have led to core damage are quantified to determine how close the particular event came to core damage. This results in an estimate of the core damage frequency that is conditional on the event, and is called the conditional core damage probability. Table 2.5-3 shows the results of ASP analyses of several precursor events. For example, this table indicates that the Browns Ferry Fire came closer to core damage than most other precursors.

The modeling of precursor events has changed significantly over the life of the program, introducing variability into the reported results that prevent meaningful examination of trends in the conditional core damage probabilities. However, it is instructive to examine the mix of contributors found to be important to precursors over the life of the program. For the past several years, more than half of the precursor events have involved electric power-related issues. Events involving the degradation of auxiliary feedwater have generally been found to be the second most common.

Several studies of precursors have been conducted.[3] Regulatory actions have been taken to reduce the threat from some of the accidents identified in precursor studies. For example, station blackout, loss of feedwater, and Anticipated Transients Without Scram (ATWS) are discussed in Section 2.4.

2.5.3 NUREG-1150 Perspectives

NUREG-1150, which was published in December 1990, documents the results of an extensive NRC-sponsored PRA.[4] The study examined five plants of varying designs to give an understanding of risk for these particular plants. Selected insights regarding classes of plants were also obtained in the study, and these were further developed through the IPE program discussed in Section 2.5.5. The improved PRA methodology used in the NUREG-1150 study significantly enhanced the understanding of risk at nuclear power plants, and can be considered as a replacement for the Reactor Safety Study.

The five nuclear power plants analyzed in NUREG-1150 are:

- Unit 1 of the Surry Power Station, a Westinghouse-designed three-loop reactor in a subatmospheric containment building, located near Williamsburg, Virginia;

- Unit 1 of the Zion Nuclear Power Plant, a Westinghouse-designed four-loop reactor in a large, dry containment building, located near Chicago, Illinois;

- Unit 1 of the Sequoyah Nuclear Power Plant, a Westinghouse-designed four-loop reactor in an ice condenser containment building, located near Chattanooga, Tennessee;

- Unit 2 of the Peach Bottom Atomic Power Station, a General Electric-designed BWR-4 reactor in a Mark I containment building, located near Lancaster, Pennsylvania; and

- Unit 1 of the Grand Gulf Nuclear Station, a General Electric-designed BWR-6 reactor in a Mark III containment building, located near Vicksburg, Mississippi.

A Level 3 PRA for internal events was performed for each of these plants. As we proceed through the remainder of Section 2.5.3, the results and insights of NUREG-1150 will be presented within the context of current PRA methods. See Appendix 1A for a summary of these methods.

The frequency of core damage initiated by external events has been analyzed for two of the plants in NUREG-1150, Surry and Peach Bottom. The analysis examined a broad range of external events (e.g., lightning, aircraft impact, tornadoes, and volcanic activity). Most of these events were assessed to be insignificant contributors by means of bounding analyses. However, seismic events and fires were found to be potentially major contributors and thus were analyzed in detail.

The following sections provide a summary of the key results from the NUREG-1150 study. The internal events results are discussed first, followed by the seismic results, and then the fire results.

2.5.3.1 Internal Events Results

The internal-event core damage frequency distributions from NUREG-1150 are included as Figure 2.5-1.[44] The bars in Figure 2.5-1 show the 90% uncertainty ranges along with the mean and median values.

Figure 2.5-1 reflects core damage frequencies that are relatively low. Except for a particular sequence involving component cooling water at Zion (plant changes have subsequently been made to address this), there are no serious vulnerabilities that yield unusually high risk. This is due in part to good design and operating procedures. It is also due to the fact that these plants have been studied before and previously identified vulnerabilities have been fixed. A similar result occurred because of the Individual Plant Examination (IPE) program, which is discussed in Section 2.5.5. Through PRAs that were performed for that program, many plant shortcomings were uncovered and then fixed for plants that had not previously been evaluated using PRA.

The various accident sequences that contribute to the core damage frequency from internal initiators can be grouped by common factors into categories. NUREG-1150 uses the accident categories depicted in Figures 2.5-2 and 2.5-3: station blackout, anticipated transients without scram, other transients, reactor coolant pump seal LOCAs, interfacing system LOCAs, and other LOCAs. The selection of such categories is not unique, but merely a convenient way to group the results.

The existence of a highly dominant accident sequence does not of itself imply that a safety problem exists. For example, if a plant has an extremely low estimated core damage frequency, the existence of a single dominant accident sequence would have little significance. Similarly, if a plant was modified to eliminate the dominant accident sequence, another accident sequence or group of accident sequences would become dominant. Nevertheless, the identification of dominant accident sequences and the failures that contribute to those sequences provide understanding of why the core damage frequency is high or low relative to other plants and desired goals. This qualitative understanding of the core damage frequency is necessary to make practical use of the PRA results and improve the plants, if necessary.

The remainder of this section summarizes the internal events results for the BWR and PWR plants examined in NUREG-1150. A somewhat detailed description of results is provided here to give concrete examples of plant-specific and generic factors that can be important to risk. This paves the way to the generic discussion of risk, based on the IPE results, that is included in Section 2.5.5.

2.5.3.1.1 NUREG-1150 Boiling Water Reactor Observations

As shown in Figure 2.5-2, the internal-event core damage frequencies for Peach Bottom and Grand Gulf are extremely low. Therefore, even though dominant accident sequences and contributing failure events can be identified, these items should not be considered as safety problems for the two plants. In fact, these dominating factors should not be overemphasized because, for core damage frequencies below 1×10^{-5}, it is possible that other events outside the scope of these internal-event analyses are the ones that actually dominate. In the cases of these two plants, the real perspectives come not from understanding why particular sequences dominate, but rather why all types of sequences considered in NUREG-1150 have low frequencies for these plants.

LOCA sequences can be expected to have low core damage frequencies at BWRs because of the numerous systems available to provide coolant injection. While low for both plants, the frequency of LOCAs is higher for Peach Bottom than for Grand Gulf. This is primarily because Grand Gulf is a BWR-6 design with a motor-driven high-pressure core spray system, rather than a steam-driven high-pressure coolant injection system as'is Peach Bottom. Motor-driven systems are typically more reliable than steam-driven systems and, more importantly, can operate over the entire range of pressures experienced in a LOCA sequence.

It is evident from Figures 2.5-2 and 2.5-3 that station blackout plays a major role in the internal-event core damage frequencies for Peach Bottom and Grand Gulf. Each of these plants has features that tend to reduce the station blackout frequency, some of which would not be present at other BWRs.

Grand Gulf, like all BWR-6 plants, is equipped with an extra diesel generator dedicated to the high-pressure core spray system. While effectively providing a third train of redundant emergency AC power for decay heat removal, the extra diesel also provides diversity, based on a different diesel design and plant location relative to the other two diesels. This results in a low probability of common-cause failures affecting all three diesel generators. The net effect is a highly reliable emergency AC power capability. In those unlikely cases where all three diesel generators fail, Grand Gulf relies on a steam-driven coolant injection system that can function until the station batteries are depleted. At Grand Gulf the batteries are sized to last for many hours prior to depletion so that there is a high probability of recovering AC power prior to core damage. In addition, there is a diesel-driven firewater system available that can be used to provide coolant injection in some sequences involving the loss of AC power.

Peach Bottom is an older model BWR that does not have a diverse diesel generator for the high-pressure emergency core coolant system. However, other factors contribute to a low station blackout frequency at Peach Bottom. Peach Bottom is a two-unit site, with four diesel generators available. Any one of the four diesels can provide sufficient capacity to power both units in the event of a loss of offsite power, given that appropriate crossties or load swapping between Units 2 and 3 are used. This high level of redundancy is somewhat offset by a less redundant service water system that provides cooling to the diesel generators. Subtleties in the design are such that if a certain combination of diesel generators fails, the service water system will fail, causing the other diesels to fail. In addition, station DC power is needed to start the diesels. (Some emergency diesel generator systems, such as those at Surry, have a separate dedicated DC power system just for starting purposes.) In spite of these factors, the redundancy in the Peach Bottom emergency AC power system is considerable.

While there is redundancy in the AC power system design at Peach Bottom, a more significant factor is a high-quality diesel generator maintenance program. Plant-specific data analysis determined that the diesel generators at Peach Bottom were an order of magnitude more reliable than at an average plant.

Finally, Peach Bottom, like Grand Gulf, has station batteries that are sized to last several hours in the event that the diesel generators do fail. With two steam-driven systems to provide coolant injection and several hours to recover AC power prior to battery depletion, the station blackout frequency is further reduced.

Unlike most PWRs, the response of containment is often a key in determining the core damage frequency for BWRs. For example, at Peach Bottom, there are a number of ways in which containment conditions can affect coolant injection systems. High pressure in containment can lead to closure of primary system relief valves, thus failing low-pressure injection systems, and can also lead to failure of steam-driven high-pressure injection systems due to high turbine exhaust backpressure. High suppression pool temperatures can also lead to the failure of systems that are recirculating water from the suppression pool to the reactor coolant system. If the containment ultimately fails, certain systems can fail because of the loss of net positive suction head in the suppression pool, and also the reactor building is subjected to a harsh steam environment that can lead to failure of equipment located there.

Despite the concerns described in the previous paragraph, the core damage frequency for Peach Bottom is relatively low, compared to the PWRs studied in NUREG-1150. There are two major reasons for this. First, Peach Bottom has the ability to vent the wetwell through a 6-inch diameter steel pipe, thus reducing the containment pressure without subjecting the reactor building to steam. While this vent cannot be used to mitigate ATWS and station blackout sequences, it is valuable in reducing the frequency of many other sequences. The second important feature at Peach Bottom is the presence of the control rod drive hydraulic cooling system, which can provide sufficient coolant to the vessel in some accident sequences, and which is not affected by either high pressure in containment or containment failure. Other plants of the BWR-4 and BWR-5 designs are potentially vulnerable to containment-related problems. As a result, the NRC has negotiated changes to containment venting for BWR-4 plants. These changes are discussed further in Chapter 4.

The Grand Gulf design is generally much less susceptible to containment-related problems than Peach Bottom. The containment design and equipment locations are such that containment rupture will not result in discharge of steam into the building containing the safety systems. Further, the high-pressure core spray system is designed to function with a saturated suppression pool so that it is not affected by containment failure. Finally, there are other systems that can provide coolant injection using water sources other than the suppression pool. Thus, containment failure is relatively benign as far as system operation is concerned, and there is no obvious need for containment venting.

2.5.3.1.2 NUREG-1150 Pressurized Water Reactor Observations

The three PWRs examined in NUREG-1150 reflect much more variety in terms of dominant accident sequences than the BWRs. While the sequence frequencies are generally low, it is useful to understand why the variations among the plants occurred.

For LOCA sequences, the frequency is significantly lower at Surry than at the other two PWRs. A major portion of this difference is directly tied to the additional redundancy available in the injection systems. In addition to the normal high-pressure injection capability, Surry can crosstie to the other unit at the site for an additional source of high-pressure injection. This reduces the core damage frequency due to LOCAs and also certain groups of transients involving stuck-open relief valves.

In addition, at Sequoyah there is a particularly noteworthy emergency core cooling interaction with containment engineered safety features in LOCAs. In this (ice condenser) containment design, the containment sprays are automatically actuated at a very low pressure setpoint, which would be exceeded for virtually all small LOCA events. This spray actuation, if not terminated by the operator, can lead to a rapid depletion of the refueling water storage tank at Sequoyah. Thus, an early need to switch to recirculation cooling may occur. Portions of this switchover process are manual at Sequoyah and, because of the timing and possible stressful conditions, lead to a significant human error probability.

Thus, LOCA-type sequences are the dominant accident sequence type at Sequoyah.

Station blackout-type sequences have relatively similar frequencies at all three PWRs. Station blackout sequences can have very different characteristics at PWRs than at BWRs. One of the most important findings of NUREG-1150 is the importance of reactor coolant pump seal failures for the Westinghouse plants that were studied. During station blackout, all cooling to the seals is lost for these plants and there is a significant probability that they will ultimately fail, leading to an induced LOCA and loss of inventory. Because the NUREG-1150 PWRs do not have systems capable of providing coolant makeup without AC power, core damage will result if power is not restored. The seal LOCA reduces the time available to restore power and thus increases the station blackout-induced core damage frequency. New seals have been proposed for Westinghouse PWRs and could reduce the core damage frequency if implemented, although they might also increase the likelihood that any resulting accidents would occur at high pressure, which has implications for the accident progression analysis.

Apart from the generic reactor coolant pump seal question, station blackout frequencies at PWRs are determined by the plant-specific electric power system design and the design of other support systems. Battery depletion times for the three PWRs were projected to be shorter than for the two BWRs. A unique characteristic of the Surry plant is a gravity-fed service water system with a canal that may drain during station blackout, thus failing containment heat removal. When power is restored, the canal must be refilled before containment heat removal can be restored.

The dominant accident sequence type at Zion is not a station blackout, but it has many similar characteristics. Component cooling water is needed for operation of the charging pumps and high-pressure safety injection pumps at Zion. Loss of component cooling water (or loss of service water, which will also render component cooling water inoperable) will result in loss of these high-pressure systems. This in turn leads to a loss of reactor coolant pump seal injection. Simultaneously, loss of component cooling water will also result in loss of cooling to the thermal barrier heat exchangers for the reactor coolant pump (RCP) seals. Thus, the reactor coolant pump seals will lose both forms of cooling. As with station blackout, loss of component cooling water or service water can both cause a small LOCA (by seal failure) and disable the systems needed to mitigate it. The importance of this scenario is increased further by the fact that the component cooling water system at Zion, although it uses redundant pumps and valves, delivers its flow through a common header. The licensee for the Zion plant has made procedural changes and is also considering both the use of new RCP seal materials and the installation of modifications to the cooling water systems.

ATWS frequencies are generally low at all three of the PWRs. This is due to the assessed reliability of the shutdown systems and the likelihood that only slow-acting, low-power-level events will result. While of low frequency, it is worth noting that interfacing-system LOCA (V) and steam generator tube rupture (SGTR) events do contribute significantly to risk for the PWRs. This is because they involve a direct path for fission products to bypass containment.

There are large uncertainties in the analyses of these two accident types, but these events can be important to risk even at frequencies that may be one or two orders of magnitude lower than other sequence types.

Most Westinghouse PWRs have developed procedures for using feed and bleed cooling and secondary system blowdown to cope with loss of all feedwater. These procedures have led to substantial reductions in the frequencies of transient core damage sequences involving the loss of main and auxiliary feedwater. Appropriate credit for these actions was given in these analyses. However, there are plant-specific features that will affect the success rate of such actions. For example, the loss of certain power sources (possibly only one bus) or other support systems can fail power-operated relief valves (PORVs) or atmospheric dump valves or their block valves at some plants, precluding the use of feed and bleed or secondary system blowdown. Plants with PORVs that tend to leak may operate for significant periods of time with the block valves closed, thus making feed and bleed less reliable. On the other hand, if certain power failures are such that open block valves cannot be closed, then they cannot be used to mitigate stuck-open PORVs. Thus, both the system design and plant operating practices can be important to the reliability assessment of actions such as feed and bleed cooling.

2.5.3.2 NUREG-1150 Seismic Analysis Observations

Figures 2.5-4 and 2.5-5 show the results of the core damage frequency analysis for seismic-initiated accidents, as well as internally and fire-initiated accidents, for Surry and Peach Bottom, respectively. Examination of these figures shows that the core damage frequency distributions of the seismic events are comparable to those of the internal events. It is evident that the seismic events are significant in the total safety profile of these plants. The key features of the seismic results for Surry and Peach Bottom are discussed in the following two sections.

The analysis of the seismically induced core damage frequency begins with the estimation of the seismic hazard, that is, the likelihood of exceeding different earthquake ground-motion levels at the plant site. At the time the NUREG-1150 study was performed, there was no agreement on a model for the seismic hazard. NUREG-1150 used seismic hazard curves for Peach Bottom and Surry that were part of an NRC-funded Lawrence Livermore National Laboratory project that resulted in seismic hazard curves for all nuclear power plant sites east of the Rocky Mountains.[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] Both sets of results are presented in this section. Since the NUREG-1150 study was completed, resolution on the seismic hazard curves has been achieved.[7]

As can be seen in Figures 2.5-6 and 2.5-7, the shapes of the seismically induced core damage frequency distributions are considerably different from those of the internally initiated and fire-initiated events. In particular, the 5th to 95th percentile range is much larger for the seismic events. In addition, as can be seen in Figures 2.5-4 and 2.5-5, the wide disparity between the mean and the median and the location of the mean relatively high in the distribution indicate a wide distribution with a tail at the high end but peaked much lower down. This is a result of the uncertainty in the seismic hazard curve.

The difference between the mean and median is an important distinction. The mean is the parameter quoted most often, but the bulk of the distribution is well below the mean. Thus, although the mean is the "center of gravity" of the distribution (when viewed on a linear rather than logarithmic scale), it is not very representative of the distribution as a whole. Instead, it is the lower values that are more probable. The higher values are estimated to have low probability, but, because of their great distance from the bulk of the distribution, the mean is "pulled up" to a relatively high value. In a case such as this, it is particularly evident that the entire distribution, not just a single parameter such as the mean or the median, must be considered when discussing the results of the analysis.

2.5.3.2.1 Surry Seismic Analysis

The core damage frequency probability distributions, as calculated using the Livermore and EPRI methods, have a large degree of overlap. The differences between the means and medians of the two resulting distributions are not very meaningful because of the large widths of the two distributions.

As shown in Figure 2.5-8, the breakdown of the Surry seismic analysis into principal contributors is reasonably similar to the results of other seismic PRAs for other PWRs. The total core damage frequency is dominated by loss of offsite power transients resulting from seismically induced failures of the ceramic insulators in the switchyard. This dominant contribution of ceramic insulator failures has been found in virtually all seismic PRAs to date.

A site-specific but significant contributor to the core damage frequency at Surry is failure of the anchorage welds of the 4kV buses. These buses play a vital role in providing emergency AC electrical power since offsite power as well as emergency onsite power passes through these buses. Although these welded anchorages have more than adequate capacity at the safe shutdown earthquake (SSE) level, they do not have sufficient margin to withstand (with high reliability) earthquakes in the range of four times the SSE, which are contributing to the overall seismic core damage frequency results.

Another area of generic interest is the contribution due to vertical flat-bottomed storage tanks (e.g., refueling water storage tanks and condensate storage tanks). Because of the nature of their configuration and field erection practices, such tanks have often been calculated to have relatively smaller margin over the SSE than most components in commercial nuclear power plants. Given that all PWRs in the United States use the refueling water storage tank as the primary source of emergency injection water (and usually the sole source until the recirculation phase of ECCS begins), failure of the refueling water storage tank can be expected to be a substantial contributor to the seismically induced core damage frequency.

2.5.3.2.2 Peach Bottom Seismic Analysis

As can be seen in Figure 2.5-8, the dominant contributor in the seismic core damage frequency analysis is a transient sequence brought about by loss of offsite power. The loss of offsite power is due to seismically induced failures of onsite AC power. Peach Bottom has four emergency diesel generators, all shared between the two units, and four station batteries per unit. Thus, there is a high degree of redundancy.

However, all diesels require cooling provided by the emergency service water system, and failure to provide this cooling will result in failure of all four diesels.

There is a variety of seismically induced equipment failures that can fail the emergency service water system and result in a station blackout. These include failure of the emergency cooling tower, failures of the 4 kV buses (in the same manner as was found at Surry), and failures of the emergency service water pumps or the emergency diesel generators themselves.

The various combinations of these failures result in a large number of potential failure modes and give rise to a relatively high frequency of core damage based on station blackout. None of these equipment failure probabilities is substantially greater than would be implied by the generic fragility data available. However, the high probability of exceedance of larger earthquakes (as prescribed by the hazard curves for this site) results in significant contributions of these components to the seismic risk.

2.5.3.3 NUREG-1150 Fire Analysis Observations

The core damage likelihood due to a fire in any particular area of the plant depends upon the frequency of ignition of a fire in the area, the amount and nature of combustible material in that area, and the nature and efficacy of the fire-suppression systems in that area. In NUREG-1150, fire analyses were performed for the Surry and Peach Bottom plants.

Similar to the seismic results, Figure 2.5-9 shows the results of the core damage frequency analysis for fire-initiated accidents are comparable to those of the internal events for Surry and Peach Bottom. It is evident that the fire events are significant in the total safety profile of these plants. The key features of the fire results for Surry and Peach Bottom are discussed below, followed by a summary of common characteristics of fire sequences for the two plants.

2.5.3.3.1 Surry Fire Analysis

Figure 2.5-9 shows the dominant contributors to core damage frequency resulting from the Surry fire analysis. The dominant contributor is a transient resulting in a reactor coolant pump seal LOCA, which can lead to core damage. The scenario consists of a fire in the emergency switchgear room that damages control power for the high-pressure injection and component cooling water pumps. Cable trays for the two redundant power trains were run one on top of the other with approximately 8 inches of vertical separation in a number of plant areas, which gives rise to the common vulnerability of these two systems due to fire. In addition, the Halon fire-suppression system in the emergency switchgear room is manually actuated.

The other principal contributor is a spuriously actuated pressurizer PORV. In this scenario, fire-related component damage in the control room includes control power for a number of safety systems.

2.5.3.3.2 Peach Bottom Fire Analysis

Figure 2.5-9 shows the mechanisms by which fire leads to core damage in the Peach Bottom analysis. Station blackout accidents are the dominant contributor, with substantial contributions also coming from fire-induced transients and losses of offsite power.

Control room fires are of considerable significance in the fire analysis of this plant. The cable spreading room below the control room is significant but not dominant in the fire analysis. The remaining physical areas of significance are the emergency switchgear rooms.

2.5.3.3.3 General Observations on Fire Analysis

Figures 2.5-8 and 2.5-9 clearly indicate that fire-initiated core damage sequences are significant in the total probabilistic analysis of the two plants analyzed. These analyses include credit for the fire protection programs required by Appendix R to 10 CFR Part 50.[8]

Although the two plants are of completely different design, with completely different fire-initiated core damage scenarios, the possibility of fires in the emergency switchgear areas is important in both plants. The importance of the emergency switchgear room at Surry is particularly high because of the reactor coolant pump seal LOCA scenario. Further, the importance of the control room at Surry is comparable to that of the control room at Peach Bottom.

This is not surprising in view of the potential for simultaneous failure of several systems by fires in these areas. Thus, in the past such areas have generally received particular attention in fire protection programs. It should also be noted that the significance of various areas also depends upon the scenario that leads to core damage. For example, the importance of the emergency switchgear room at Surry could be altered (if desired) not only by more fire protection programs but also by changes in the probability of the reactor coolant pump seal failure.

2.5.4 Individual Plant Examinations

The NRC issued Generic Letter (GL) 88-20 in November 1988, requesting that all licensees perform an Individual Plant Examination (IPE) "to identify any plant-specific vulnerabilities to severe accidents and report the results to the Commission." The purpose and scope of the IPE effort includes examining internal events occurring at full-power, including those initiated by internal flooding. In response, the staff received 75 IPE submittals covering 108 nuclear power plant units. The staff then examined the IPE submittals to determine what the collective IPE results imply about the safety of U.S. nuclear power plants and how the IPE program has affected reactor safety.[9] A summary of the Level 1 findings is provided in the following sections. Insights related to accident progression are discussed in Chapter 4.

2.5.4.1 Vulnerabilities and Plant Improvements

The primary goal of the IPE Program was for licensees to "identify plant-specific vulnerabilities to severe accidents that could be fixed with low-cost improvements." However, GL 88-20 did not specifically define what constitutes a vulnerability; hence, the IPEs exhibit considerable diversity in the criteria used to define a vulnerability. The wording used in some submittals is such that it is not always clear whether a licensee is identifying a finding as a "vulnerability" or as some other issue worthy of attention. Therefore, a problem considered to be a vulnerability at one plant may not have been specifically identified as a vulnerability at another plant. In fact, only four licensees with boiling water reactor (BWR) plants and 15 licensees with pressurized water reactor (PWR) plants explicitly stated that their plants had vulnerabilities. However, nearly all of the licensees identified other areas warranting investigation for potential improvements.

Over 500 proposed improvements were identified by the licensees to address perceived weaknesses in plant design or operation. Most of these plant improvements are classified as procedural/ operational changes (approximately 45%), design/hardware changes (approximately 40%), or both. Few of the improvements involve maintenance-related changes. Typically, the procedural or design changes indicate revised training in order to properly implement the actual change. Many of these proposed improvements have already been implemented at the plants, and others are still under consideration.

Some improvements are associated with other requirements (primarily the station blackout rule) and utility activities. However, although these improvements were not necessarily identified as a result of the IPE, in some cases, the licensee is using the IPE to prioritize the improvements and to support decisions regarding their implementation. The specific improvements vary from plant to plant. However, numerous improvements that had significant impact on plant safety include changes to AC and DC power, coolant injection systems, decay heat removal systems, heating, ventilating and air conditioning, and PWR reactor coolant pump seals.

2.5.4.2 CDF Perspectives from the IPEs

The IPE results indicate that the plant core damage frequency (CDF) is often determined by many different sequences (in combination), rather than being dominated by a single sequence or failure mechanism. The largest contributors to plant CDF and the dominant failures contributing to those sequences vary considerably among the plants (e.g., some are dominated by LOCAs, while others are dominated by station blackout [SBO]). However, for most plants, support systems are important to the results because support system failures can result in failures of multiple front-line systems. Further, the support system designs and dependency of front-line systems on support systems vary considerably among the plants. That variation explains much of the variability observed in the IPE results.

Consistent with previous risk studies, the CDFs reported in the IPE submittals are lower, on average, for BWR plants than for PWR plants, as shown in Figure 2.5-10. Although both BWR and PWR results are strongly affected by the support system considerations discussed above, a few key differences between the two types of plants contribute to this tendency for lower BWR CDFs and cause a difference in the relative contributions of the accident sequences to plant CDF. The most significant difference is that BWRs have more injection systems than PWRs and can depressurize more easily to use low-pressure injection systems. This gives BWRs a lower average contribution from LOCAs. However, the results for individual plants can vary from this general trend. As shown in Figure 2.5-10, the CDFs for many BWR plants are actually higher than the CDFs for many PWR plants. The variation in the CDFs is primarily driven by a combination of the following factors, which are further detailed in Table 2.5-4:

- plant design differences (primarily in support systems such as cooling water, electrical power, ventilation, and air systems)

- variability in modeling assumptions (including whether the models accounted for alternative accident mitigating systems)
- differences in data values (including human error probabilities) used in quantifying the models.

2.5.5 Individual Plant Examinations for External Events

On June 28, 1991, the U.S. Nuclear Regulatory Commission (NRC) issued Supplement 4 to Generic Letter (GL) 88-20, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f)." In particular, the external events considered in the IPEEE program include seismic events; internal fires; and high winds, floods, and other (HFO) external initiating events involving accidents related to transportation and nearby facilities[1].

Along with Supplement 4 to GL 88-20, the NRC issued NUREG-1407, "Procedure and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," in June 1991. In NUREG-1407, the NRC provided guidelines for conducting IPEEEs. Subsequent to the publication of NUREG-1407, the NRC issued Supplement 5 to GL 88-20 on September 8, 1995, to notify licensees of modifications to the recommended scope of the seismic portion of the IPEEE for certain plant sites in the eastern United States (EUS).

The NRC received 70 IPEEE submittals covering all operating U.S. nuclear reactors. (Some submittals covered more than one unit at multi-unit sites with similar or almost identical plant designs.) The staff of the NRC's Office of Nuclear Regulatory Research completed Staff Evaluation Reports (SERs) which document the staff's overall conclusions for each of the IPEEE reviews. A summary of perspectives obtained from the IPEEEs is contained in NUREG 1742 and highlights are presented below.

Scope, Limitations, and General Comments

IPEEE studies have been limited to the consideration of plant behavior under full-power operating conditions. The perspectives documented in this report are somewhat limited for the following reasons: (a) IPEEEs are intended to yield predominantly qualitative perspectives, rather than more quantitative findings; (b) IPEEEs address several different types of initiators of varying importance (for a given plant) and, therefore, require the implementation of different methods of analyses offering varying levels of detail and accuracy; and (c) even for a given type of external initiator, the procedures and methods used by the various licensees to conduct their IPEEEs have also varied considerably.

Additionally, the IPEEE submittals used various sources of information, such as use of seismic hazard curves derived from different sources (e.g., Lawrence Livermore National Laboratory [NUREG/CR-1488 and NUREG/CR-5250]; Electric Power Research Institute [EPRI, 1989]; and site-specific studies), or applied simplified conservative

[1] On November 23, 1988, the NRC issued GL 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities, 10 CFR 50.54(f)," to licensees of nuclear power plants. GL 88-20 outlined the objectives and overall logistics of the Individual Plant Examination (IPE) program, which solely addresses internally initiated events (including internal flooding).

methods in some studies while others used more realistic approaches. These differences make it difficult to draw plant-to-plant comparisons of analysis results. Comparisons of IPEEE results among plants and among the various types of external hazards are also limited because of variations in the quality of submittals.

Seismic Events

Licensees used one of two methodologies to conduct their seismic IPEEEs. The first was a seismic probabilistic risk assessment (SPRA) consisting of at least a Level 1 analysis and a qualitative containment performance analysis. The second was a seismic margins assessment (SMA) method, including a qualitative containment performance analysis.

Almost all licensees reported in their IPEEE submittals that no plant "vulnerabilities" were identified with respect to seismic risk (the use of the term vulnerability varied widely among the IPEEE submittals). However, most licensees did report at least some seismic "anomalies," "outliers," and/or other concerns. In the few submittals which identified a seismic "vulnerability," the concerns identified were comparable to concerns identified as outliers or anomalies in other submittals.

For plants that performed SPRA analyses, most plants reported seismic CDFs between 1E-5 and 1E-4 per reactor-year (ry), with the next most common group falling between 1E-6 and 1E-5/ry, see Figure 2.5-11. Only a small fraction of plants had CDFs higher than 1E-4/ry or less than 1E-6/ry.

For plants that performed SMA analyses, plant HCLPF capacities are between 0.12g and 0.3g, see Figure 2.5-12. Fourteen licensees reported plant HCLPFs of at least 0.3g, ten plants fell between 0.25 and 0.3g, nine plants were between 0.2 and 0.25g, and two plants were between 0.15 and 0.2g. One plant reported a HCLPF value of 0.12g. With the proposed improvements taken into account, SMA results indicate that for all plants the HCLPF is never below the safe shutdown earthquake (SSE) and generally exceeds the SSE, see Figure 2.5-13.

Dominant contributors from SPRAs for seismic failure involve the failure of the electrical systems, which include the failure of offsite power (17% of all contributors); the failure of various components of the electrical system (17%), such as motor control centers (MCCs), switchgear, and relays; the failure of the emergency diesel generator (EDG) (8%); and the failure of the dc batteries (5%). Building and structural failures also contribute significantly (30% of all contributors). Other structures of which failure could cause core damage include block walls, pump house/pump intake structures, dams, and stacks. Failures of frontline and support systems (28% of all contributors), as well as tank failures (11%) also contribute to core damage frequency.

The weak link components identified in the SMA analyses in general were similar to the structures, systems, and components (SSCs) listed as dominant contributors in the SPRAs. Components identified as outliers in the SMAs included many electrical components and their anchorage, various tanks, residual heat removal (RHR) heat exchangers, and structures like the turbine and auxiliary buildings. Many licensees identified block walls located in the proximity of safety-significant equipment as weak link structures.

Seventy percent of the plants proposed improvements as a result of their seismic IPEEE analyses. In some cases these plant improvements were only proposed in the submittals (sometimes without a firm commitment for implementation), while in others the submittals indicated the improvements were already implemented. Improvements vary from simple housekeeping enhancements to more elaborate plant design modifications and can generally be grouped into three general categories: hardware modifications, improved procedures and training, and enhanced maintenance and housekeeping. Based on the improvements described by licensees it is clear that the seismic IPEEE program has had a notable impact on improving plant safety.

Fires

For the purposes of the IPEEE fire assessments, all licensees utilized probabilistic analysis methods in one form or another. By far the most commonly cited analysis approach was the EPRI Fire-Induced Vulnerability Evaluation (FIVE) methodology [EPRI 1992]. The FIVE methodology was cited as being used to support about 81% of the licensees' IPEEE submittals. However, most of these submittals also went beyond the FIVE approach and applied PRA methods as a supplement to the FIVE method.

The selected methodology did have some impact on the final estimates of fire CDF, but ultimately appeared to have little impact on the overall findings of the IPEEE studies (e.g., identification of dominant areas contributing to fire CDF). Since FIVE is primarily a screening method, those licensees who stopped with FIVE screening generally obtained higher total CDF estimates than those who continued with more detailed fire PRA-based quantification of unscreened zones.

Out of all the IPEEE submittals, only two licensees, representing three nuclear power plant units, initially identified fire vulnerabilities. In one case (Quad Cities), the vulnerabilities were identified in the licensee's original IPEEE submittal and a detailed re-analysis by the licensee showed that fire vulnerabilities did not exist. However, the licensee did make plant improvements as a result of the insights gained in the original IPEEE analysis and credited some of those improvements in the re-analysis. In the second case (Millstone 2), two fire vulnerabilities were identified and addressed by the licensee. For each of the two plants the vulnerabilities included fire safety issues in the turbine building which housed important safety-related cables and equipment needed for safe shutdown. Turbine building areas were also identified by many other licensees as important CDF contributors.

Despite the fact that the vast majority of licensees identified no fire-related vulnerabilities, the majority of licensees, over 60%, did identify and/or implement plant improvements to reduce fire risk. A total of approximately 242 fire-related plant improvements were identified by licensees. The majority of the cited plant improvements (about 57%) were associated with various plant procedures including operating procedures, maintenance procedures, combustible controls, enhancements to operator training, enhanced fire brigade training, etc. The remaining improvements (about 43%) were related to physical plant/hardware changes. These included general plant system design changes, enhancements to fire protection features, relocation of critical cables, and upgrading of fire barriers.

The fire-induced CDFs reported by the licensees range from approximately 4E-8 to

2E-4 per reactor-year, see Figure 2.5-14. The IPEEE fire analyses have broadly found fire CDF to be roughly on a par with, and in some cases greater than, internal events CDF. The vast majority of licensees reported fire CDF values that equal at least 10% of the internal events CDF (or greater). About 25% of the submittals reported fire-induced CDF values that exceeded the corresponding plant internal events CDF (as reported in the IPE).

In the vast majority of cases, licensees concluded that the dominant fire CDF contributors were those areas that held both significant fire sources and important equipment and cables, see Figure 2.5-15. Hence, it appears that spatial factors (e.g., the location of fire source and targets), were more significant in determining fire risk than were plant systems design features. Areas devoid of either fire sources or important targets generally were screened.

Overall, the two types of fire analysis zones found most often to be the single highest fire CDF contributors were switchgear areas and MCRs. The next most commonly identified areas were areas of the turbine building and cable spreading rooms for plants with only a single cable spreading room. Other commonly reported areas include electrical equipment rooms, diesel generator rooms, cable vault and tunnel areas, and battery/charger rooms. A range of other areas are identified as important on a plant-specific basis.

In the specific case of the main control room (MCR), fire CDF was dominated by the abandonment scenarios; that is, unsuppressed fires leading to MCR abandonment. In this case, fire CDF estimates were driven largely by two factors, namely, the assumed conditional probability of MCR abandonment and the reliability of human actions associated with plant shutdown using the remote shutdown capability.

Fire sources considered in the fire assessments included both fixed sources (e.g., electrical panels, pumps, transformers, and electrical cables) and transient combustibles. Electrical panel fires were the most significant fire CDF contributors in most submittals. In a minority of submittals, transient combustible fires were also found to be significant.

Fire-induced transients were found to be the most important accident sequences. These included loss of feedwater and main steam isolation valve (MSIV) closure transients, loss of off-site power (LOOP) events, and loss of support system initiators. Loss-of-coolant accidents (LOCAs) induced by spurious opening of pressure-operated relief valves (PORVs) or safety relief valves (SRVs) were generally not identified as significant contributors to the fire-related CDF. However, fire scenarios resulting in reactor coolant pump (RCP) seal LOCAs were important for many Westinghouse pressurized water reactors (PWRs).

High Winds, Floods, and Other External Events

The following types of events were included in the high winds, floods and other (HFO) external events category:

- High winds, including tornadoes, tornado missiles, and hurricanes

- External floods, including intense rainfall resulting in site flooding and roof ponding; flooding from nearby bodies of water including wave runup from rivers, lakes and the ocean; and potential flooding from postulated dam failures

- Accidents related to transportation or nearby industrial facilities

- Other types of external events such as onsite hazardous material spills, hydrogen line breaks, effects from low-temperature conditions such as icing and blockage of cooling water intake lines, blockage of drains and intakes from debris, any other plant-unique hazard

None of the 70 IPEEE submittals identified any HFO-related vulnerabilities; however, 34 submittals reported that they had either made, or were considering, a total of 64 HFO-related plant improvements. Thirty-six plants reported no HFO-related improvements.

All HFO evaluations reviewed have screened out accidents involving transportation and nearby facilities, and have also screened out other plant-unique hazards when encountered.

For those cases where the licensees performed PRAs or CDF bounding analyses for their HFO analysis, the estimated CDF results have varied from plant to plant as shown below.

- For high winds and tornadoes, the plant-specific CDF results vary from less than 2E-7/ry to 6E-5/ry.

- For external flood events, the plant-specific CDF results vary from 2E-8/ry to about 7E-6/ry.

- For transportation and nearby facility accidents, all reported plant-specific CDF results from PRA studies or bounding analyses are below the NUREG-1407 screening criterion of 1E-6/ry.

- One submittal (Haddam Neck) reported bounding analysis CDF results of 8E-6/ry for lightning events and 7E-6/ry for snow and ice.

- One submittal (South Texas) reported CDF results of 8E-6/ry for a chemical release from a nearby chemical facility.

- One submittal (Salem) reported a plant improvement that resulted in an external events CDF reduction of three orders of magnitude from approximately 1E-4/ry to approximately 1E-7/ry. The plant modification cited was the improvement of door penetration seals between the service and auxiliary buildings to protect against external flooding.

2.5.6 Low Power and Shutdown Perspectives

Until recently, PRAs of severe accidents in nuclear power plants have considered initiating events that could occur only during full-power operation. This focus was based on the judgment that the level of risk associated with accidents that could occur during full-power operation was greater than that for accidents during the other modes of operation, such as low-power and shutdown. The primary justification for this view appeared to be that lower decay heat levels are generally associated with these other modes of operation, so more time is available to recover from adverse situations in these modes.

However, there are several factors that could influence the risk associated with accidents initiated during shutdown. These include:

1. The greater need for operator action to prevent core damage (because automatic safety systems are disabled during some of the shutdown modes).

2. The increased unavailability of equipment as a result of planned maintenance. (There is a need for high equipment availability during power operation, which limits the amount and length of maintenance activities that can be performed while the plant is at power.)

3. The breach of containment integrity caused by the opening of penetrations and hatches. (These openings, which are allowed by technical specifications, in many cases are necessary before the activities planned for shutdown can occur.)

In response to such concerns, the NRC undertook a two-phase project to analyze the frequencies, consequences, and risk of accidents during modes of operation other than full-power for two plants, and to compare the results with those from full-power analyses for the same plants[10,11]. The plants selected were Grand Gulf and Surry. The analyses included a limited-scope Level 3 PRA for internal events and a Level 1 PRA for seismic and internal fire and flood sequences. Because of the complexity of the shutdown configurations, detailed analyses were only performed for selected time periods for the two plants.

For Grand Gulf, a period called Plant Operating State 5 (POS 5) was chosen. POS 5 covers cold shutdown operation (where the reactor vessel is at atmospheric pressure and the bulk water temperature is below 200 °F) and the time in the refueling operating condition until the vessel head is detensioned. This period was chosen because of its potentially large contribution to core damage frequency (CDF) and risk. For Surry, the evaluation was conducted for mid-loop operation, in which the reactor coolant system level is lowered to the mid-plane of the hot leg. This period was chosen because many incidents have occurred during mid-loop operation throughout the world, and the apparent risk potential.

The results of the Grand Gulf and Surry evaluations are presented below. It is important to note that such results are highly plant specific because of the unique character of each plant's refueling process. Grand Gulf and Surry have features that may not be present at other plants which tend to reduce the risk during low-power and shutdown operations.

2.5.6.1 Grand Gulf Low Power and Shutdown Observations

Figure 2.5-16 presents a comparison of mean core damage frequency percentages for the major classes of accidents from both the NUREG-1150 full-power and the POS 5 analyses for Grand Gulf. In both analyses, the station blackout class is important because station blackouts cut across multiple systems. However, during POS 5, there are additional accidents (e.g., LOCAs) that can cut across multiple systems. There are differences in the accident progression associated with station blackout accidents at full-power versus during POS 5. These are: (1) almost all the POS 5 station blackout sequences lead to an interfacing system LOCA and the full-power sequences do not; (2) the containment is always open at the start of POS 5 accidents whereas it is isolated at the start of most full-power accidents; and (3) the probability of arresting the core damage process in the vessel is higher for full-power accidents than for POS 5. In the full-power analysis the ATWS class is the second most important class, while ATWS is not possible during POS 5 since the plant is already subcritical. The second most important class for POS 5 is LOCAs.

Table 2.5-5 presents a comparison on a calendar-year basis of the core damage frequency, early fatality risk, and total latent fatality risk for POS 5 and for full-power for Grand Gulf. While the POS 5 mean core damage frequency is about a factor of two lower than the full-power value, there is overlap between the two distributions. The mean early fatality risk of POS 5 is only a factor of 1.7 greater than the full-power risk even though the containment is open during most of the accidents in POS 5. The mean total latent cancer fatality risk of POS 5 is about a factor of 4 greater than the corresponding full-power risk. One reason for this is that in POS 5, the containment is always open, and in full-power the containment is always isolated at the start of an accident. Also, some of the difference is caused by different versions of the consequence code being used for the two studies. The version used for POS 5 generally results in higher estimates for the total latent cancer fatality risk.

2.5.6.2 Surry Low Power and Shutdown Observations

The contribution to the total core damage frequency from internal events during mid-loop operation at Surry was found to be lower by an order of magnitude than that at full-power. This is mainly due to the much smaller fraction of time that the plant is at mid-loop. Figure 2.5-17 presents a comparison of mean core damage frequency percentages for the major classes of accidents from both the NUREG-1150 full-power and the mid-loop analyses for Surry.

Table 2.5-6 presents a comparison on a calendar-year basis of the core damage frequency, early fatality risk, and total latent fatality risk for mid-loop operation and for full-power for Surry. While the mid-loop operation mean core damage frequency is an order of magnitude lower than the full-power value, there is some overlap between the two distributions.

The offsite risk estimates for latent health effects of accidents during mid-loop operation were similar to the risk estimates for full-power operation for Surry. This is due to the lack of mitigative features for a significant fraction of the accidents initiated during mid-loop operation, which causes the releases to the environment to be large. The early health consequences are much lower than the full-power results, despite the unisolated containment, primarily because of the long time after reactor trip when the accidents occur in mid-loop operation (i.e., because of the natural decay of the short-lived isotopes of iodine and tellurium, which are primarily associated with early health effects). The uncertainties in risk for accidents during mid-loop operations are largely due to uncertainties associated with isolating the containment and achieving a pressure retaining capability.

2.5.6.3 Industry Low Power and Shutdown Studies

During the 1990s, there was substantial industry effort to understand and manage low power and shutdown risks. The NRC did not include low power and shutdown in the IPE program; however, most licensees have performed some type of analysis of low power and shutdown risks. In particular, most licensees use some form of risk management tool to help manage planned outages. These efforts have led to safer plant configurations during outages, while in some cases, resulting in shorter outages.

For the most part, the industry outage management activities focus on plant configuration management, that is, assuring that a minimum set of plant equipment is always available to perform key safety functions. These analyses are generally not full scope PRAs and do not routinely calculate risk numbers. Nevertheless, from the studies that have been done and reported at an NRC workshop on low power and shutdown accidents (SAND99-1815), we can draw important conclusions about risk;

1. Low power and shutdown risk can be comparable to full power risk.

2. Short term risks are highly variable and can be much larger than full power risk for certain time periods. Figure 2.5-18 presents the risk estimates for one PWR over a typical outage cycle.

3. The industry is very aware of the risks during low power and shutdown and has taken important steps to manage risks. Nevertheless, precursor events continue to occur, (See Table 2.5-8) and the risks need ongoing attention.

Key findings from both the NRC and industry activities are summarized below:

- Potentially significant operational events occur.

- Risk from LPSD conditions can be comparable to full power.

- LPSD risk at boiling water and pressurized water reactors appears to be dominated by three classes of initiating events (loss of shutdown cooling, loss of coolant, and loss of offsite power).

- Dominant failures associated with LPSD events appear to be human-related.

- The most risk dominant plant operational states are characterized by high decay heat and reduced inventory.

- Risk contributors appear to be very plant-specific.

- Initiating events that have been analyzed for full power conditions must be reexamined to ensure that all LPSD effects are considered.

- Outages other than for refueling may be important contributors to risk.

While much work has been done, we do not have complete estimates of low power and shutdown risk that can be added to full power risk to give us a complete risk picture. Unplanned outages are difficult to account for, and these may be very important to risk, as they often include outages of safety equipment. Also, limited attention has been given to external events during low power and shutdown. For now, we can say that low power and shutdown risks are important, but a complete risk picture is not available.

2.5.7 Station Blackout Sequences

Station blackout has consistently been found to be an important contributor to core damage frequency in PRAs, including the Reactor Safety Study, NUREG-1150, and the IPEs. It has not necessarily been the dominant contributor for each plant in the study, but most plants have a significant contribution from station blackout. Because of the general importance of station blackout, a more detailed examination of this particular sequence is provided in this section. A description is first given of the types of station blackout sequences that can occur, followed by an assessment of the impact of the station blackout rule (based on IPE results).

Types of Station Blackout

Station Blackout sequences are initiated by a loss of offsite power and the associated reactor scram, followed by failure of the station diesels (or gas turbines, if applicable) to start and load. Station blackout sequences are further discriminated into long-term and short-term station blackouts, which are described below for BWRs and PWRs.

For a long-term station blackout sequence in a BWR, water is temporarily injected into the reactor vessel by the steam turbine-driven systems. Most of the U.S. plants (25 of 37) have two independent systems (high-pressure coolant injection [HPCI] plus reactor core isolation cooling [RCIC] or isolation condenser [IC]) that can keep the core covered without the availability of AC power. However, BWR-5 and BWR-6 designs have substituted an electric motor-driven high pressure core spray (HPCS) system in lieu of HPCI so that these plants have only one turbine-driven injection system (RCIC). Similarly, the BWR-2 and early BWR-3 plants employ an AC-dependent feedwater coolant injection system (FWCI) instead of HPCI. Water flow is intermittent as necessary to keep the core covered and continues for as long as DC (battery) power for turbine governor control remains available from the unit batteries (typically about 6 hours).

The short-term designation for BWRs applies to station blackout sequences with early loss of injection. Injection failure might occur in either of two ways. First, there might be direct failure(s) of the steam turbine system(s) during the period in which DC power remains available. Note that for plants with both RCIC and HPCI, this involves *independent* failures of the two systems. Because these are high-pressure injection systems, success of their function does not depend upon reactor vessel depressurization. The second (and much less probable) way in which the early total loss of injection initiating event for short-term station blackout might occur is by common-mode failure of the DC battery systems. At most BWR facilities, the diesel generators have dedicated starting batteries, but if the diesels are started from the unit batteries, failure of these batteries would, upon loss of offsite power, be a contributing cause of the station blackout. Furthermore, without DC power for valve and turbine governor control, the steam turbine-driven injection systems would not be operable. The loss of DC power would also render the safety/relief valves (SRVs) inoperable in the remote-manual mode; thus, the reactor vessel could not be depressurized.

The basic characteristics of the two dominant forms of BWR station blackout sequences can be summarized as follows. DC power remains available during the period of core degradation for short-term station blackout initiated by independent failure of HPCI and RCIC; the decay heat level is relatively high, and the reactor vessel is depressurized during the period after the core becomes uncovered and begins to degrade. For long-term station blackout, the core remains covered for more than 6 hours, so the decay heat level is about 50 percent less during the period of core degradation. However, when injection capability is lost (due to battery failure) the ability to operate the SRVs is also lost. Thus, the reactor 'vessel repressurizes and remains pressurized during and after the period of core degradation.

For a PWR, injection systems are lost in a station blackout because the systems rely on

AC power. However, core cooling is initially available in a long-term station blackout sequence through turbine-driven auxiliary feedwater. Turbine-driven auxiliary feedwater can operate until the batteries deplete, which normally leads to a loss of control. If AC power is not recovered soon after loss of control, core damage will follow. Some plants might be able to manually control feedwater after battery depletion, but a continuous source of feedwater is still needed to prevent core damage.

For a short-term station blackout sequence in a PWR, the turbine-driven auxiliary feedwater system fails at the beginning of the accident. The most frequent cause is failure to start and run for the required time period. The early loss of heat rejection causes the inventory of the reactor coolant systems to boil off, leading to early core damage.

Station blackout results in loss of cooling for reactor coolant pumps at most PWRs. This introduces the potential for seal failure from high temperatures, particularly for plants using the old seal material in Westinghouse pumps. The associated leakage from the reactor coolant system can accelerate core damage. This concern is most important for long-term sequences because there is an extended period without seal cooling before core damage occurs. For short-term sequences, the time to core damage is much shorter, so seal failures are more likely to occur after core damage.

Station Blackout Rule

The Station Blackout Rule, discussed in Section 2.4, requires that an analysis be performed for each nuclear power plant to establish a method to cope with station blackout for a specified duration without core damage occurring (coping method). In some instances, licensees implemented plant modifications to improve the plant's ability to endure a station blackout. The goal of the Station Blackout Rule is to limit the average station blackout contribution to CDF to about 1×100^{-5}/ry. This goal should be interpreted as an aiming point or numerical benchmark, rather than as a hard and fast requirement. In the IPE Insights Program, the IPE results were used to infer the impact of the Station Blackout Rule on the plant CDF. For licensees that modeled the Station Blackout Rule coping method in their IPEs, the staff compared the average station blackout CDF with the rule's goal to determine how well it was achieved. For licensees that did not model the Station Blackout Rule coping method, the staff compared the average station blackout CDF with the rule's goal to provide insight into the margin for improvement in CDF by implementing the Station Blackout Rule.

Ten licensee IPE submittals (covering 15 plant units) reported estimates of the reduction in total CDF that resulted from implementing the Station Blackout Rule. These estimates are shown in Figure 2.5-19. The average reported reduction was $\sim2\times10^{-5}$/ry, ranging from $\sim7\times10^{-6}$ to $\sim6\times10^{-5}$/ry. The average reported percent reduction in total CDF was about 20%, ranging from about 10 to 50%. Licensees that met the Station Blackout Rule using existing equipment were not included in the average CDF reduction calculation.

The range of plant CDF and average CDF for IPEs that accounted for the Station Blackout Rule coping method in their modeling were compared to the CDF for those that did not account for the coping method. Both sets of plants exhibited a wide range of station blackout CDF relative to the Station Blackout Rule goal. Some licensees that modeled the Station Blackout Rule coping method reported station blackout CDF about two orders of magnitude lower than the goal, while others reported station blackout CDF about three times higher than the goal. Similarly, some licensees reported station blackout CDF two orders of magnitude lower than the Station Blackout Rule goal without modeling the Station Blackout Rule coping method, while others reported station blackout CDF close to an order of magnitude higher than the goal. For both sets of plants, the average reported percent station blackout contribution was about 20%, and the average station blackout CDF for the two sets of plants were nearly the same. Table 2.5-7 summarizes key IPE observations regarding containment preference.

These comparisons of IPE results indicate that the Station Blackout Rule had a noticeable, but not enormous impact on the plant CDF. For the limited number of plants that directly reported the impact of the Station Blackout Rule, the average reduction was equal to the value anticipated during the development of the Station Blackout Rule.

2.5.8 Current Understanding of Risk

An improved understanding of nuclear power plant risk has been gained through analysis of operating experience and using risk assessment techniques. As a result of these studies, we conclude that the current fleet of operating plants is safe and that there is no undue risk to the public. On the other hand, many believe that current plants are orders of magnitude safer than the Commission's Quantitative Health Objectives in the Safety Goal Policy. We can not demonstrate that this belief is true; in fact, it is clear that a number of plants approach the QHOs when all risks are considered. The discussions below summarize our understanding of plant risks.

The average internal event full power core damage frequencies estimated for both BWRs and PWRs are generally low, with specific results affected strongly by plant-specific factors such as those discussed in Section 2.5.3 for the NUREG-1150 plants. In both the NUREG-1150 and IPE results, station blackout, transients, and LOCAs are usually the more important contributors for PWRs. For BWRs, LOCAs and ATWSs are generally less important than station blackout and transients. Similarly, the ASP results show a consistently high fraction of precursors that involve electrical system failures.

The BWRs generally (but not always) have core damage frequencies that are lower than those of the PWRs. The LOCA sequences, which often dominate the PWR core damage frequencies, are normally minor contributors for the BWRs. This is not surprising because BWRs have many more systems than PWRs for injecting water into the reactor coolant system. For many transients, the same argument holds. BWRs have many more systems that can provide decay heat removal and makeup for transients that lead to loss of water inventory due to stuck-open relief valves or primary system leakage.

Station blackout accidents contribute a high percentage of the core damage frequency for many of the BWRs. However, when viewed on an absolute scale, station blackout has a higher frequency at the PWRs than at the BWRs. To some extent this is due to design differences between BWRs and PWRs. For example, in station blackout accidents, many PWRs are vulnerable to reactor coolant pump seal LOCAs following loss of seal cooling, leading to loss of inventory with no method for providing makeup. BWRs, on the other hand, have at least one injection system that does not require AC power. While such BWR and PWR design features influence the core damage frequencies associated with station blackout, the electric power system design, which is largely independent of the plant type, is probably more important.

The NUREG-1150 and IPE analyses indicate that for both BWRs and PWRs, other support systems, such as service water, are quite important. Because support systems vary considerably among plants, caution must be exercised when making statements about generic classes of plants, such as PWRs versus BWRs. Once significant plant-specific vulnerabilities are removed, support-system-driven sequences will probably dominate the core damage frequencies of both types of plants. Both types of plants have sufficient redundancy and diversity so as to make multiple independent failures unlikely. Support system failures introduce dependencies among the systems and thus can become dominant.

The risk evaluations for external events from NUREG-1150 and the IPEEEs indicate that seismic and fire events can be important, but that the results are highly plant-specific. Seismic risk is strongly affected by electric power failures and failures of related components such as motor control centers. Structural failures, such as block walls collapsing on important equipment can also be significant. Fire risk is dominated by fires in areas where fire sources and important equipment are collocated. Switchgear rooms, control rooms, and turbine buildings are examples of important fire areas. Seismic and fire sequences can be similar to internal event sequences, e.g., station blackout. However, a wide variety of plant specific sequences can be observed in the seismic and fire PRAs. Seismic and fire core damage frequencies can be as high or higher than internal event frequencies at some plants.

Evaluations of risk during low-power and shutdown for Grand Gulf and Surry indicate that the risk during these modes can be important. Industry studies confirm that the annual risk can be of the same order as full power risk. In fact, the short-term risk can be significantly higher during particular shutdown modes than during full power. Plant configurations with reduced water inventory, substantial decay heat, and reduced safety system availability are particularly important.

Section 2.4 described the safety goals that have been set for commercial nuclear power plants. Information is now available from the IPEs that can be used to infer how operating plants compare with the safety goals. This inference was made as part of the IPE Insights Program. When comparing the IPE results with the safety goals, it is important to note that the scope of the IPE program is limited to accidents initiated by internal events (excluding internal fires) that occur during full-power operation.

The CDFs for all BWRs and most PWRs fall below the 1×10^{-4}/ry subsidiary objective; however, nine licensees representing 15 PWR units reported CDFs above 1×10^{-4}/ry. Conditional containment failure probabilities for bypass and early containment failure are below the 0.1 subsidiary objective for most of the PWRs. All of the conditional containment failure probabilities for bypass events in BWRs are below 0.1; however, most of the conditional containment failure probabilities for early containment failure are above 0.1. This result is expected because of the nature of BWR pressure suppression containments.

Although offsite consequences were not generally calculated in the IPEs, by extrapolating the NUREG-1150 health effects to the IPEs, an indication of how the IPEs compare to the quantitative health objectives can be obtained. Through this extrapolation, the staff concluded that most of the IPE results are likely to meet the NRC's quantitative health objectives. The IPE results imply risk levels below the individual latent cancer fatality health objective. In addition the IPE results also suggest risk levels below the individual early fatality health objective. Seventeen plants produced results that might approach one or both of the QHOs. Although relatively more plants exceeded the proposed subsidiary objectives, only a fraction of these are found to have the potential for individual early fatality risk levels that could approach the corresponding quantitative health objective.

The picture is less clear when all risks are considered. For commercial LWRs, the QHOs are obtained for core damage frequencies in the range of 5E-4 and higher per year or large early release frequencies in the range of 3E-5 and higher. Clearly, considering full power internal and external events, along with low power/shutdown events, will result in a significant number of plants with CDFs well above 1E-4 per year. Therefore, while it is likely that the fleet of plant, on average, meets the Safety Goals, large margins do not exist. This fact becomes important when considering risk informing the regulations to reduce "excessive margins."

Table 2.5-1 NRC Sources of reactor operational data

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

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

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

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

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

Table 2.5-2 NRC Feedback of nuclear power plant experience

Operating Reactors Licensing Actions Summary (NUREG-1272) Vol. 9, No. 1 (AEOD Annual Report)

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

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

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

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

AEOD - published case studies (about one per year)

AEOD - special studies (about 2 per year)

AEOD - published engineering evaluations (10 in 1990)

AEOD - published technical review reports (18 in 1990)

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

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

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

Performance Indicators for Operating Commercial Nuclear Power Plants (Quarterly)

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

Table 2.5-3 Precursors and severe accidents

Date	Type	Event	Cond. Core Damage Probability	Reference
24-Mar-71	LOSP	LaCrosse loss of offsite power	4×10^{-5}	NUREG/CR-2497
19-Jan-74	LOSP	Haddam Neck loss of offsite power	2×10^{-4}	NUREG/CR-2497
22-Mar-75	Fire	Browns Ferry Fire	1.5×10^{-1}	NUREG/CR-2497
31-Aug-77	LOFW	Cooper loss of feedwater	1×10^{-3}	NUREG/CR-2497
10-Nov-77	Flooding	Surry 2 valve flooding	6×10^{-7}	NUREG/CR-2497
20-Mar-78	Other	Rancho Seco loss of nonnuclear instrumentation	1×10^{-1}	NUREG/CR-2497
06-Mar-79	Service Water	Brunswick loss of RHR service water	2×10^{-5}	NUREG/CR-2497
02-May-79	LOFW	Oyster Creek loss of feedwater flow	2×10^{-3}	NUREG/CR-2497
28-Jun-80	ATWS	Browns Ferry partial failure to scram	9.8×10^{-4}	NUREG/CR-3591
02-Nov-81	LOCA	Sequoyah loss of coolant	9×10^{-4}	NUREG/CR-2497
09-Jun-85	LOFW	Davis Besse loss of feedwater	1.1×10^{-2}	NUREG/CR-4674
20-Mar-90	Shutdown Transient	Vogtle 1 loss of shutdown cooling	1×10^{-3}	NUREG/CR-4674
13-Aug-91	Transient	Nine Mile Point 2	1×10^{-5}	Not Published
2-Aug-95	Unavailability	St. Lucie 1 multiple failures	1.1×10^{-4}	NUREG/CR-4674

Table 2.5-4 Overview of key IPE CDF observations

Accident class	Key observations
Transients (other than station blackouts and ATWS)	Important contributor for most plants because of reliance on support systems; failure of such systems can defeat redundancy in front-line systems Both plant-specific design differences and IPE modeling assumptions contribute to variability in results: • use of alternative systems for injection at BWRs • variability in the probability that an operator will fail to depressurize the vessel for LPI in BWRs • availability of an isolation condenser in older BWRs for sequences with loss of decay heat removal (DHR) • susceptibility to harsh environment affecting the availability of coolant injection capability following loss of DHR • capability to use feed-and-bleed cooling for PWRs • susceptibility to RCP seal LOCAs for PWRs • ability to depressurize the reactor coolant system in PWRs affecting the ability to use LPI • ability to cross-tie systems to provide additional redundancy
SBOs	Significant contributor for most plants, with variability driven by: • number of redundant and diverse emergency AC power sources • availability of alternative offsite power sources • length of battery life • availability of firewater as a diverse injection system for BWRs • susceptibility to RCP seal LOCAs for PWRs
ATWS	Normally a low contributor to plant CDF because of reliable scram function and successful operator responses BWR variability mostly driven by modeling of human errors and availability of alternative boron injection system PWR variability mostly driven by plant operating characteristics, IPE modeling assumptions, and assessment of the fraction of time the plant has an unfavorable moderator temperature coefficient
Internal floods	Small contributor for most plants because of the separation of systems and compartmentalization in the reactor building, but significant for some because of plant-specific designs Largest contributors involve service water breaks
LOCAs (other than interfacing system LOCAs (ISLOCAs) and steam generator tube ruptures (SGTRs))	Significant contributors for many PWRs with manual switch over to emergency core cooling system recirculation mode BWRs generally have lower LOCA CDF than PWRs for the following reasons: • BWRs have more injection systems • BWRs can more readily depressurize to use low-pressure systems
ISLOCAs	Small contributor to plant CDF for BWRs and PWRs because of the low frequency of initiator Higher relative contribution to early release frequency for PWRs than BWRs because of low early failure frequency from other causes for PWRs

Table 2.5-4 Overview of key IPE CDF observations (continued)

Accident class	Key observations
SGTR	Normally a small contributor to CDF for PWRs because of opportunities for the operator to isolate a break and terminate an accident, but important contributor to early release frequency

Table 2.5-5 Distributions for Core damage frequency and aggregate risk for POS 5 and full-power operation for Grand Gulf

Analysis	Descriptive Statistics (All values are per calendar year)			
	Percentiles			
	5th	50th	95th	Mean
	Core Damage Frequency			
POS 5	4.1×10^{-7}	1.4×10^{-6}	5.6×10^{-6}	2.1×10^{-6}
Full Power	1.8×10^{-7}	1.1×10^{-6}	1.4×10^{-5}	4.1×10^{-6}
	Early Fatality Risk			
POS 5	3.7×10^{-11}	2.8×10^{-9}	3.9×10^{-8}	1.4×10^{-8}
Full Power	2.5×10^{-12}	6.1×10^{-10}	2.6×10^{-8}	8.2×10^{-9}
	Total Latent Cancer Fatality Risk			
POS 5	4.3×10^{-4}	1.9×10^{-3}	1.2×10^{-2}	3.8×10^{-3}
Full Power	1.4×10^{-5}	2.4×10^{-4}	2.3×10^{-3}	9.5×10^{-4}

Table 2.5-6 Distributions for Core damage frequency and aggregate risk for mid-loop and full-power operation for Surry

Analysis	Descriptive Statistics (All values are per calendar year)			
	Percentiles			
	5th	50th	95th	Mean
	Core Damage Frequency			
Mid Loop	3.2×10^{-7}	2.0×10^{-6}	1.9×10^{-5}	4.2×10^{-6}
Full Power	9.8×10^{-6}	2.5×10^{-5}	1.0×10^{-4}	4.1×10^{-5}
	Early Fatality Risk			
Mid Loop	1.3×10^{-10}	3.6×10^{-9}	1.6×10^{-7}	4.9×10^{-8}
Full Power	7.6×10^{-10}	7.0×10^{-8}	5.4×10^{-6}	2.0×10^{-6}
	Total Latent Cancer Fatality Risk			
Mid Loop	8.0×10^{-4}	5.3×10^{-3}	5.5×10^{-2}	1.6×10^{-2}
Full Power	3.1×10^{-4}	2.2×10^{-3}	1.9×10^{-2}	5.2×10^{-3}

Table 2.5-7 Key IPE observations regarding containment performance

Failure mode	Key observations
Early failure	On average, the large volume containments of PWRs are less likely to have early structural failures than the smaller BWR pressure suppression containments Overpressure failures (primarily from ATWS), fuel coolant interaction, and direct impingement of core debris on the containment boundary are important contributors to early failure for most BWR containments; hydrogen burns are found important in some Mark III containments The higher early structural failures of BWR Mark I containments versus the later BWR containments are driven to a large extent by drywell shell meltthrough* In a few BWR analyses, early venting contributes to early releases Phenomena associated with high-pressure melt ejection are the leading causes of early failure for PWR containments* Isolation failures are significant in a number of large, dry and subatmospheric containments The low early failure frequencies for ice condensers relative to the other PWRs appear to be driven by analysis assumptions rather than plant features For both BWR and PWR plants, specific design features lead to a number of unique and significant containment failure modes
Bypass	Probability of bypass is generally higher in PWRs, in part, because of the use of steam generators, and because the greater pressure differential between the primary and secondary systems may increase the likelihood of an ISLOCA in PWRs Bypass, especially SGTR, is an important contributor to early release for PWR containment types Bypass is generally not important for BWRs

Table 2.5-7 Key IPE observations regarding containment performance (continued)

Failure mode	Key observations
Late failure	Overpressurization when containment heat removal is lost is the primary cause of late failure in most PWR and some BWR containments High pressure and temperature loads caused by core-concrete interactions are important for late failure in BWR containments Containment venting is important for avoiding late uncontrolled failure in some Mark I containments The larger volumes of the Mark III containments (relative to Mark I and Mark II containments) are partly responsible for their lower late failure probabilities in comparison to the other BWR containments The likelihood of late failure often depends on the mission times assumed in the analysis

* There has been a significant change in the state-of-knowledge reporting some severe accident phenomena in the time since the IPE analyses were carried out.

Table 2.5-8 Shutdown events occurring during 1998 and the early portion of 1999.

Initiating Event Class	Plant/ Date	Event Description/Consequences
Loss of Shutdown Cooling	Limerick 1 2/6/98	Loss of shutdown cooling and mode change. Fuse blew while installing a jumper, causing RHR to isolate. Primary coolant system temperature increased from 191°F to 200°F, changing modes from cold shutdown to hot shutdown.
	Clinton 2/13/98	Loss of shutdown cooling due to loss of nuclear safety Div II. An alert was declared in order to activate the Technical Support Center and to provide for more manpower.
Loss of Coolant	ANO 2 2/2/99	Inadvertent entry into reduced inventory operations. Reactor vessel level dropped 56 inches within approximately 1.5 minutes.
	Quad Cities 2 2/24/99	A draindown event occurred as a result of switching from train B of RHR shutdown cooling to train A when operators failed to perform tasks in the correct order. Water level was reduced from 80 inches indicated to about 45 inches indicated (a loss of approximately 6000 to 7000 gallons).
	FitzPatrick 12/2/99	An operator-induced 100-inch (approximately 14,000 gallons) draindown event occurred when operators attempted to maintain indicated water level at 357 inches above the top of the active fuel using a level instrument with a temporary addition to its reference leg. This temporary addition was in the process of being replaced with the original reference leg components. This replacement activity increased the indicated level, and the operators compensated for this apparent increase in level by increasing the discharge rate.
Loss of Offsite Power	Ft. Calhoun 5/20/98	Transformer explosion results in Loss-of-offsite power (LOOP). Emergency diesel generators (EDGs) start and load. SD cooling interrupted for several seconds. No heat up (time to boiling–2 hours).
	McGuire 1 6/3/98	Explosion of switchyard breaker and LOOP. (1E power was supplied through U2.)
Clinton 1/6/99		LOOP; EDGs started and loaded. Shutdown cooling via RHR lost. Fourth of four events involving loss of shutdown cooling. B-RHR tripped and shutdown cooling was supplied via RWCU.

Table 2.5-8 Shutdown events occurring during 1998 and the early portion of 1999. (continued)

Initiating Event Class	Plant/ Date	Event Description/Consequences
Loss of Power	Clinton 6/29/98	Loss of 3 of 4 offsite power sources due to storm damage. Shutdown cooling B-pump tripped; restarted. Spent fuel pool cooling lost. Spent fuel cooling and one shutdown cooling bus lost. Shutdown cooling was restated without reactor coolant system (RCS) heatup. Spent fuel cooling restored.
	D.C. Cook 1&2 8/31/98	Train A reserve power supply lost due to loss of station service transformer. EDGs for train A, both units, auto-started. Operating RHR pump, each unit, briefly lost with no heatup of RCS.
	Catawba 2 9/6/98	Loss of 4160 V bus, auto start of one auxiliary feedwater (AFW) pump, and lifting of one power-operated relief valve (PORV). The plant was preparing to go water solid; therefore, little space was available in the pressurizer to accommodate the increase in RCS volume. When the charging pump discharge valve went full open, the increase in flow caused the PORV to lift about 12 to 14 times. One 1E bus lost power and was not loaded by its EDG since the EDG was down for maintenance. The fuel was not in the core.
	San Onofre 2 2/1/99	Loss of shutdown cooling due to breaker malfunction. Inadequate pre-job briefing, inadequate work plan, and inadequate controls of work in progress lead to three-phase fault with normal clearing while working on breaker and 2 °F RCS temperature rise.
Fire	Fermi 2 10/8/98	Fire in EDG panel. Damage was limited to the panel. Cause not stated.
	Fermi 2 10/10/98	Fire in a motor control center in Rad Waste. Second electrical fire in two days. This was caused by personnel error and resulted in personnel injury.
Flood	WNP 2 6/17/98	Fire header line break with subsequent flooding of ECCS pump rooms. ECCS pumps rendered inoperable'by flooding.

Table 2.5-8 Shutdown events occurring during 1998 and the early portion of 1999. (Continued)

Initiating Event Class	Plant/ Date	Event Description/Consequences
Other	WNP 2 5/30/98	Full scram and injection of LPCS, low-pressure coolant injection (LPCI) A start, start of Div I and III EDGs (accident signal response). 2600 gallons of water were injected, increasing RCS pressure and decreasing temperature. Pressure increased from 107 psig to 425 psig. Temperature decreased from 222 °F to 219 °F.
	WNP 2 5/31/98	Scram while shut down. Reactor pressure increased from 1034 psig to 1064 psig. Recurring problem. Possible cause is scram discharge volume level high.
	Salem 1 2/21/98	Operator inattention resulted in start of AFW to feed steam generator (SG). AFW ran with discharge valves closed for less than one minute. AFW was not required to be operational in the current mode, did not feed the steam generators because the feed valves were closed. Level in SGs was supposed to be maintained between 18% and 28%, but got to 9% of narrow range.
	Limerick 2 6/3/98	Standby liquid control injected into the vessel. Between 300 and 350 gallons of water bearing B4C injected. Unnecessary injection of B4C necessitated cleanup of RCS. B4C could damage carbon steel components in RCS.
	Clinton 6/10/98	Service water pump flow indications at RHR heat exchanger (HX) off-scale high. HX bypass line inadequately sized so that high flow would occur in the line should the HX be bypassed and inadequate cooling to other safety-related components could occur.

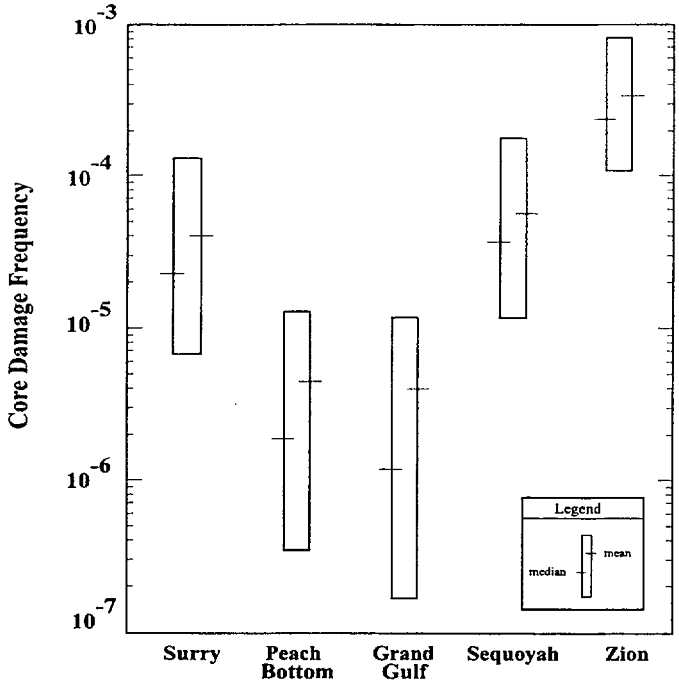


Figure 2.5-1 Internal core damage frequency ranges (5th to 95th percentiles)

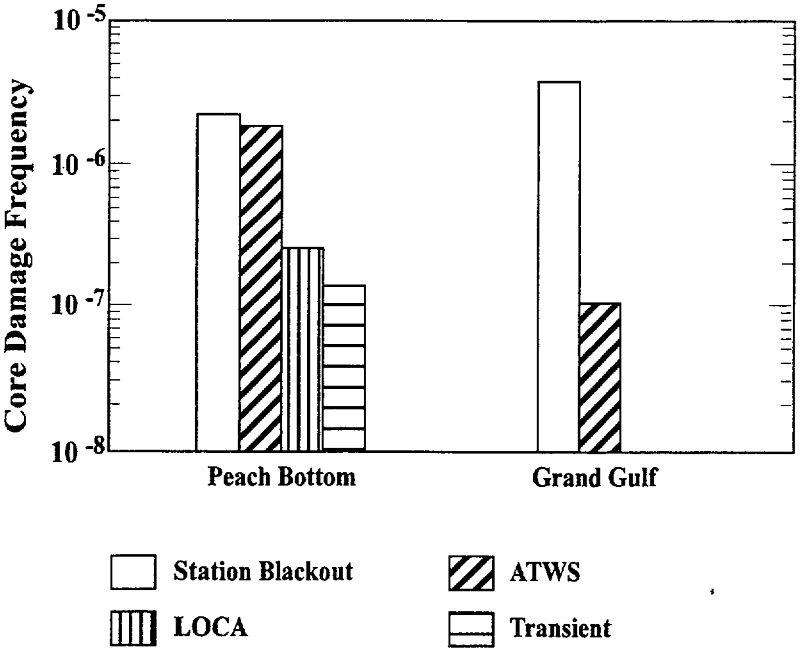


Figure 2.5-2 BWR principal contributors to internal core damage frequencies

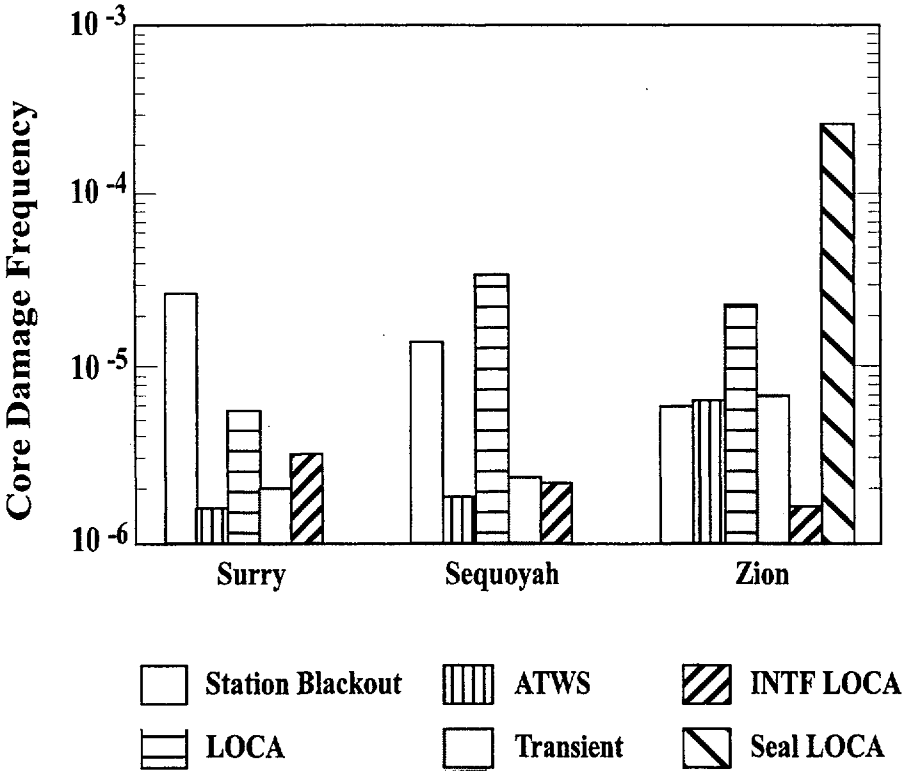


Figure 2.5-3 PWR principal contributors to internal core damage frequencies

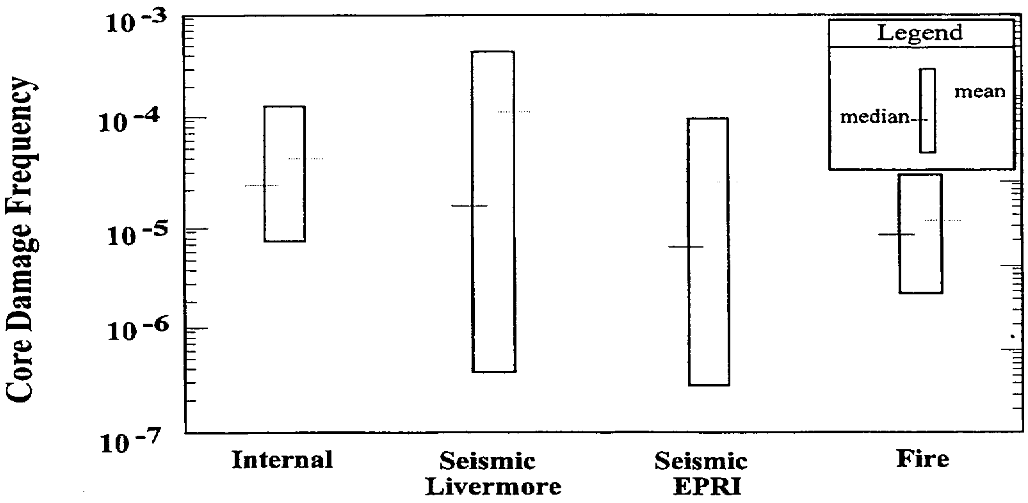


Figure 2.5-4 Surry internal and external-event core damage frequency ranges

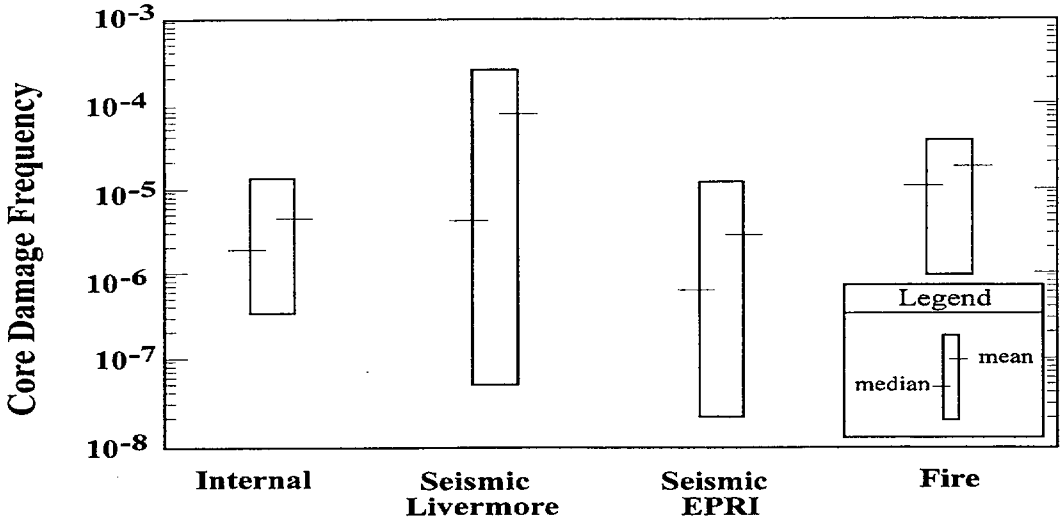


Figure 2.5-5 Peach Bottom internal- and external-event core damage frequency ranges

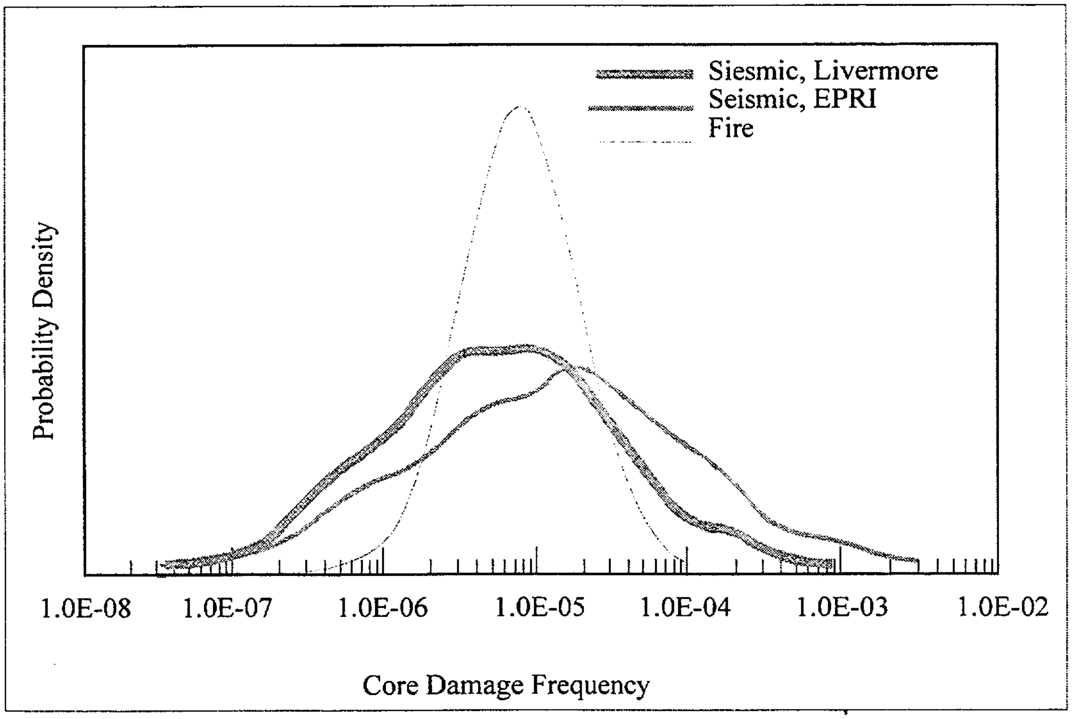


Figure 2.5-6 Surry external event core damage frequency distributions

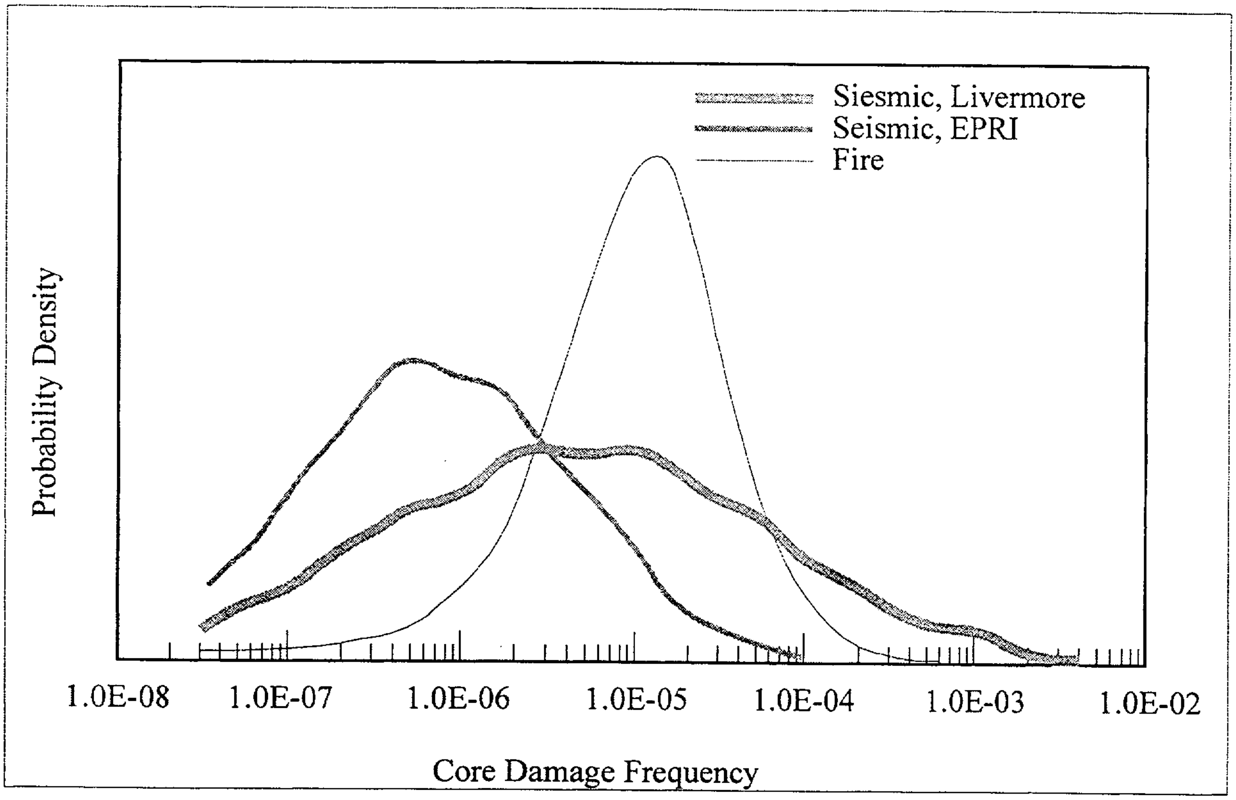


Figure 2.5-7 Peach Bottom external event core damage frequency distributions

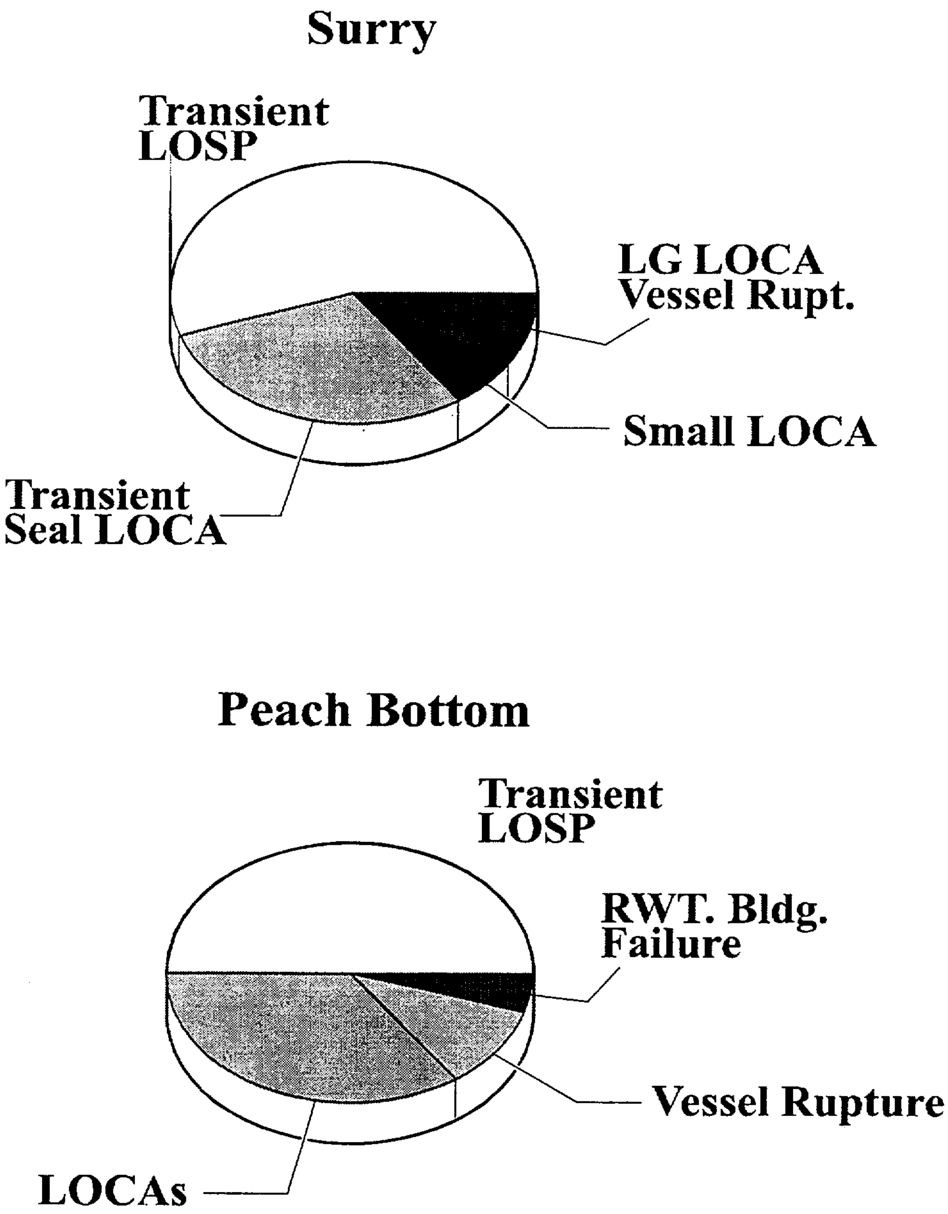


Figure 2.5-8 Principal contributors to seismic core damage frequencies

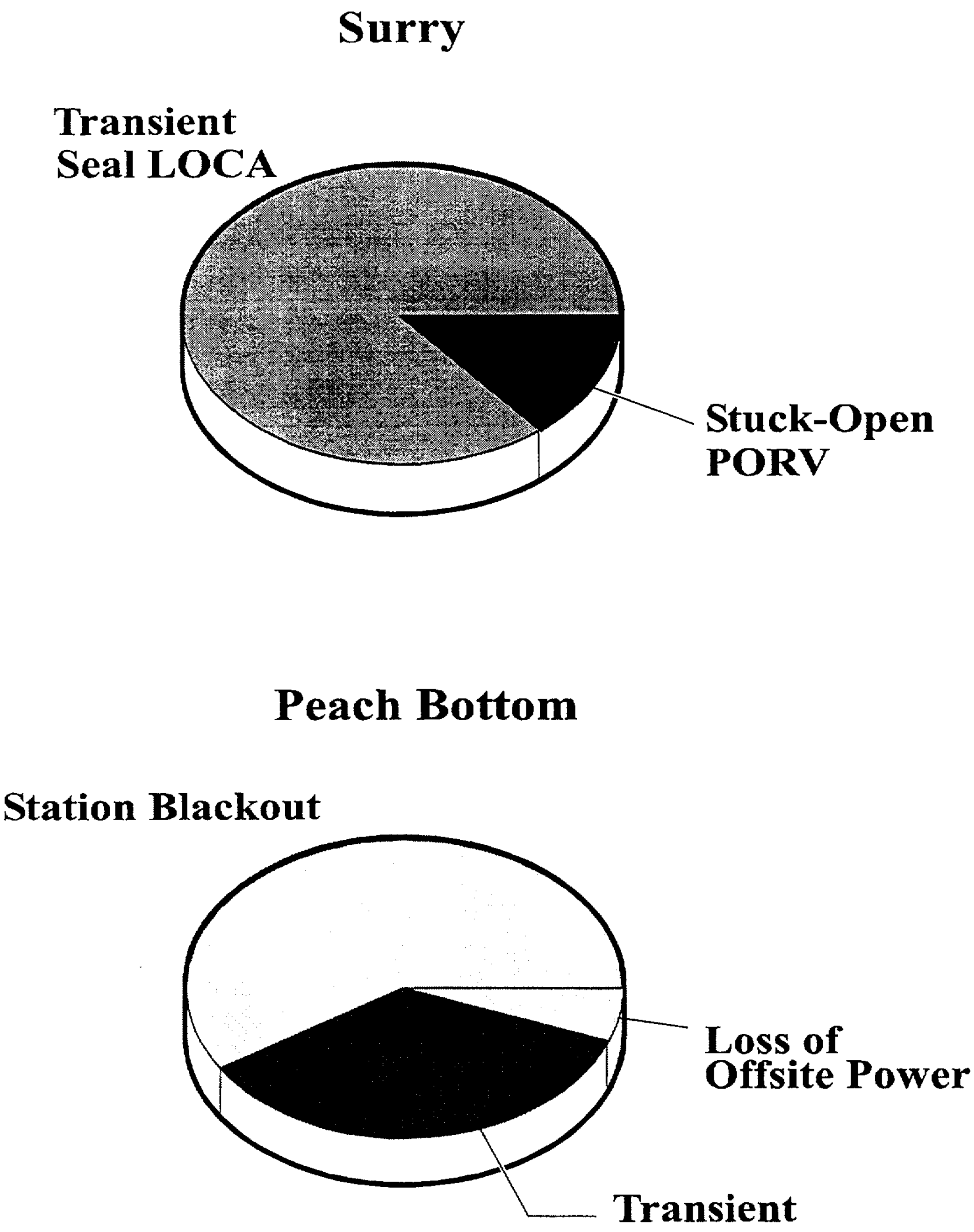


Figure 2.5-9 Principal contributors to fire core damage frequencies

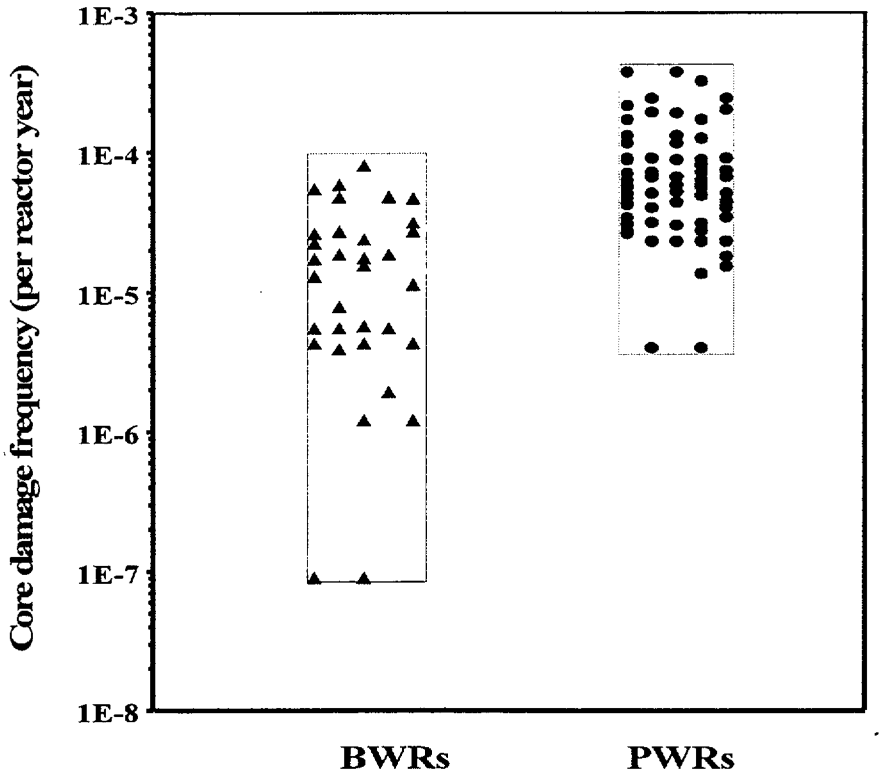


Figure 2.5-10 Reported IPE CDFs for BWRs and PWRs

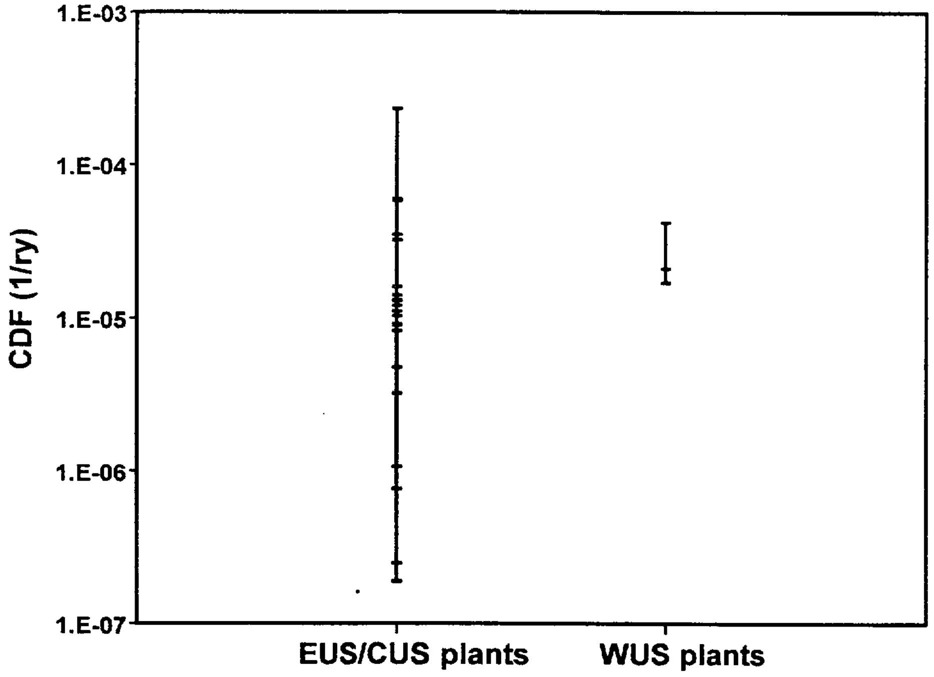


Figure 2.5-11 CDF Results

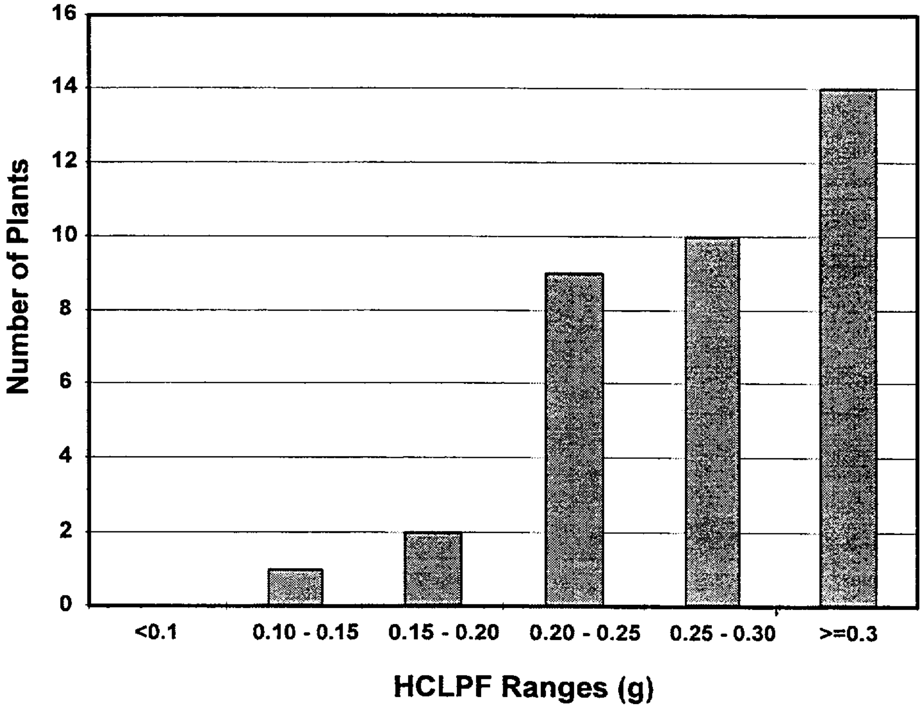


Figure 2.5-12

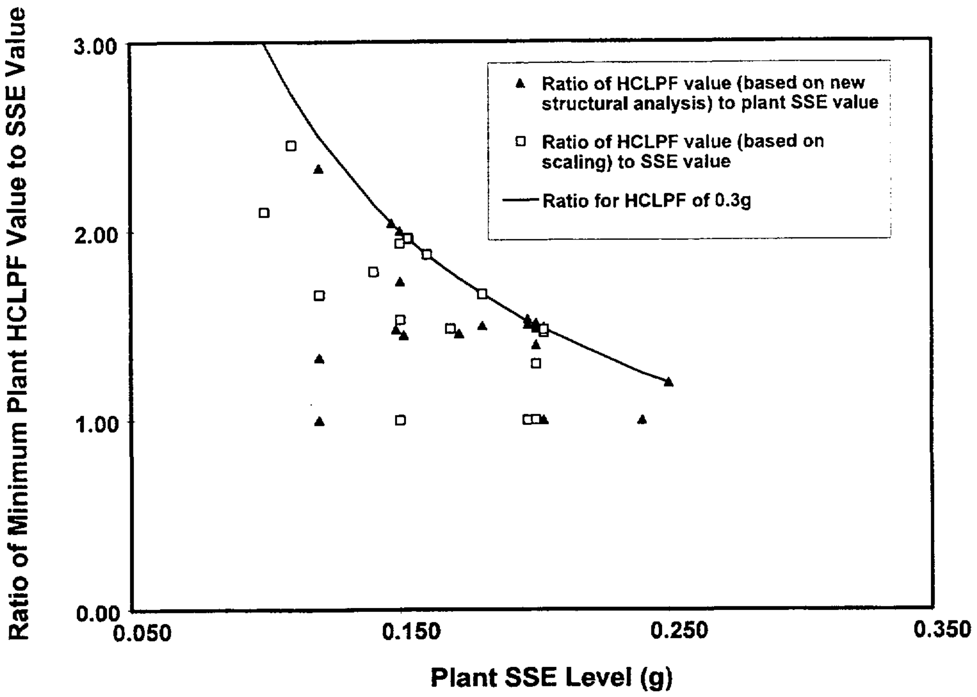

Ratio of Minimum Plant HCLPF Value to SSE Value
3.00
2.00
1.00
0.00
0.050
0.150
0.250
0.350
Plant SSE Level (g)
▲ Ratio of HCLPF value (based on new structural analysis) to plant SSE value
□ Ratio of HCLPF value (based on scaling) to SSE value
Ratio for HCLPF of 0.3g

Figure 2.5-13

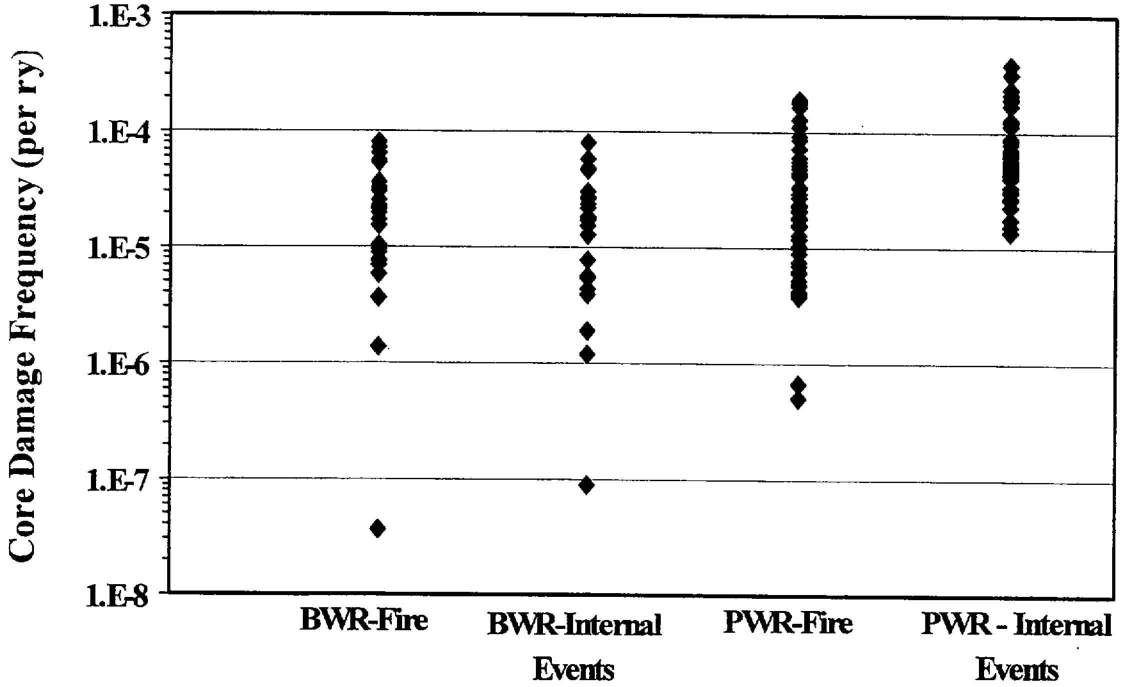


Figure 2.5-14 Fire-induced CDFs Reported by Licensees

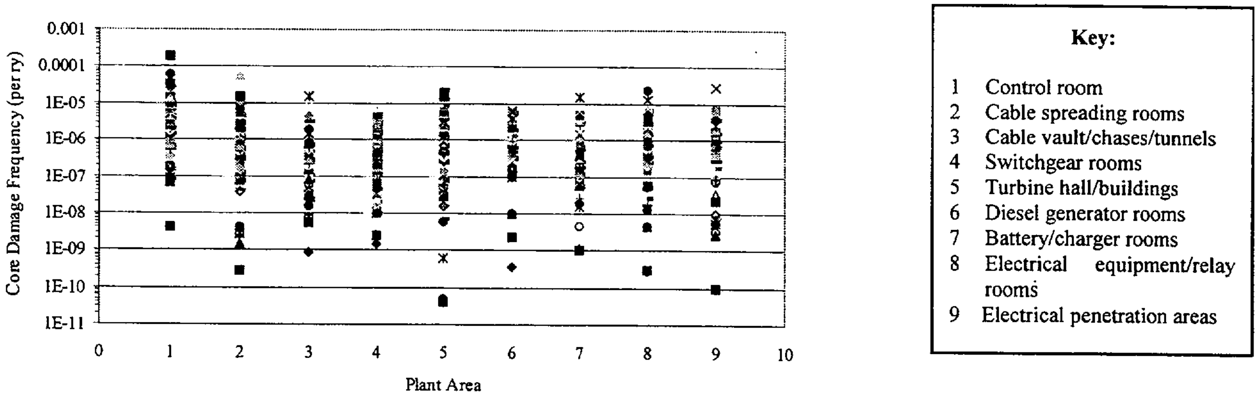


Figure 2.5-15. Reported fire-induced CDFs for commonly identified plant fire analysis zones

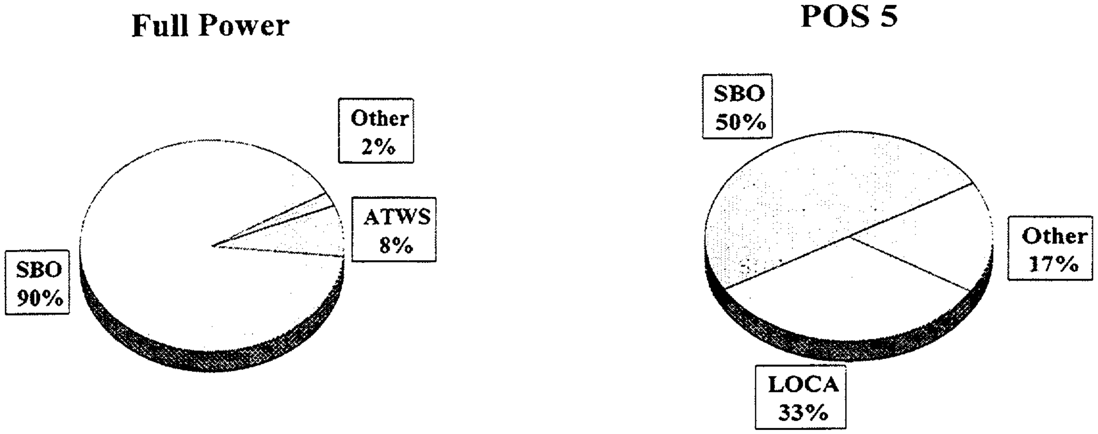


Figure 2.5-16 Grand Gulf sequence contributions for full-power and POS 5

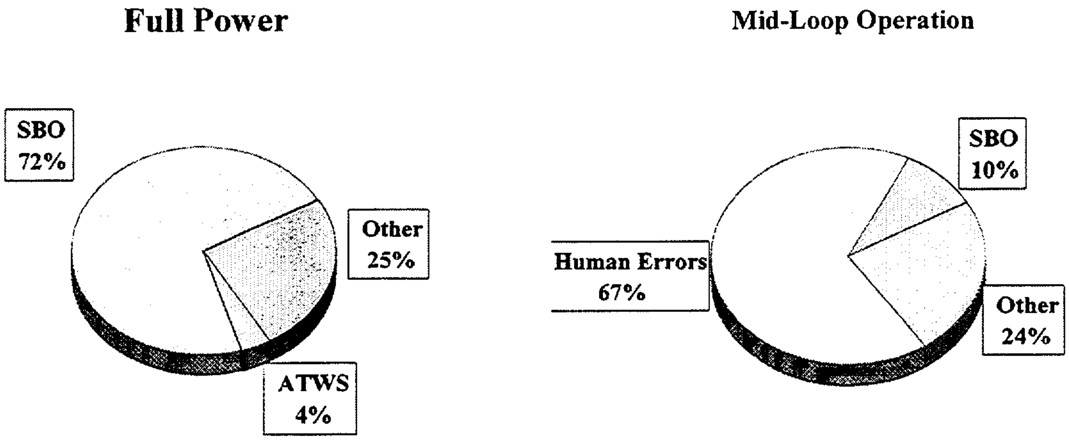


Figure 2.5-17 Surry sequence contributions for full-power and mid-loop operation

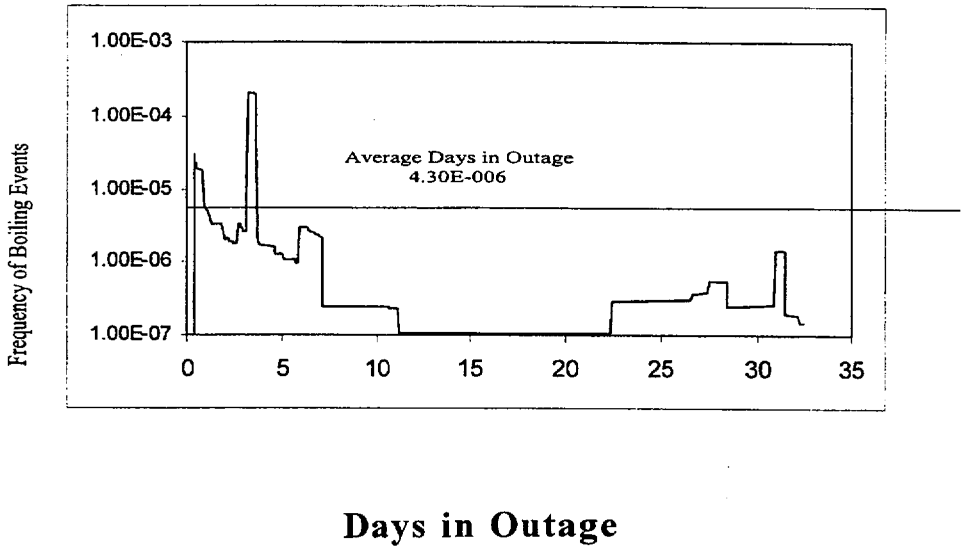


Figure 2-5.18 Example PWR Boiling Risk Profile

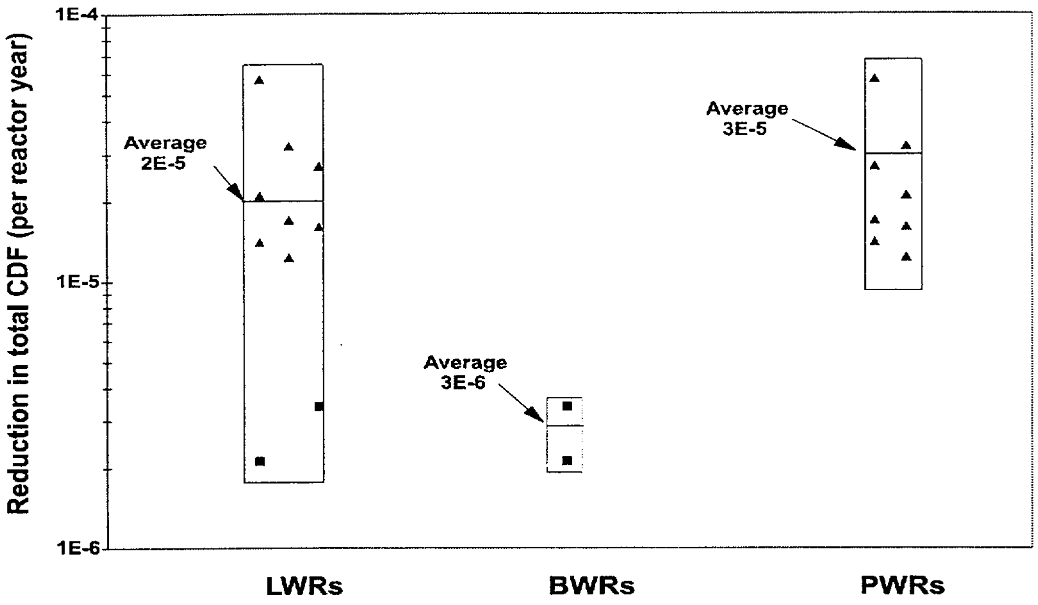


Figure 2.5-19 Reduction in CDF from implementing Station Blackout Rule

References for Section 2.5

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

2. *U.S.Code of Federal Regulations*, Title 10, Part 50.73, January 1, 1991.

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

4. U.S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 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. U.S. Nuclear Regulatory Commission, "Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts," NUREG/CR-6372 Vol. 1 & 2, April 1997.

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

9. U.S. Nuclear Regulatory Commission, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," NUREG-1560, Draft for Comment, November 1996.

10. 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," Sandia National Laboratories, NUREG/CR-6143, June, 1994.

11. T. W. Chu and W. T. Pratt, "Evaluation of Potential Severe Accidents During Low Power Shutdown Operations at Surry, Unit 1," Brookhaven National Laboratory, NUREG/CR-6144, October 1995.

2.6 Risk-Informed Regulation

2.6.1 PRA Policy Statement

Following the NUREG-1150 studies and during the implementation of the IPE program, the NRC debated the future use of PRA within the agency. NUREG-1489[1] was issued in March 1994 and provided a review of staff uses of PRA at that time. In addition, it provided information about currently available PRA methods and their strengths and weaknesses. At the same time, a commission policy statement on the use of PRA was being developed. That policy statement was issued in August 1995 and stated:[2]

> *the commission's intention to encourage the use of PRA and to expand the scope of PRA applications in all nuclear regulatory matters to the extent supported by the state-of-the-art in terms of methods and data. Implementation of the policy statement will improve the regulatory process in three areas: Foremost, through safety decision making enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees.*
>
> *Therefore, the Commission adopts the following policy statement regarding the expanded NRC use of PRA:*
>
> *(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.*
>
> *(2) PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.*
>
> *(3) PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.*
>
> *(4) The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and*

> *backfitting new generic requirements on nuclear power plant licensees.*
>
> *This policy statement affirms the Commission's belief that PRA methods can be used to derive valuable insights, perspectives, and general conclusions as a result of an integrated and comprehensive examination of the design of nuclear facilities, facility response to initiating events, the expected interactions among facility structures, systems, and components and between the facility and its operating staff.*

2.6.2 Issues Concerning the Quantitative Use of PRA

Even before the issuance of the PRA Policy Statement, the staff had begun to develop approaches for applying PRA more extensively in a regulatory setting. During this process it became clear that there were a number of key issues that needed to be addressed. The debate of these issues has been vigorous and still continues in some areas. The discussion below outlines some of the more important issues.

Do the Safety Goals provide the basis for risk targets?

The safety goals were originally developed to answer the question "how safe is safe enough?" Therefore, it is consistent with that policy to reduce risks where appropriate to ensure that the goals are met. However, if the safety goals represent "safe enough," then an ALARA approach is not warranted. On the other hand, there have been arguments that risk targets should be set that are more stringent that the quantitative health objectives (QHOs) in order to account for uncertainty and incompleteness in risk assessments. Currently, targets are being set based on the subsidiary safety goals (see Sections 2.6.5 and 2.6.6), so that the targets are tied to the QHOs, but are somewhat conservative and also more practical to implement.

Can the Safety Goals be applied on a plant-specific basis?

The safety goal policy clearly states that the safety goals are to be applied to the industry as a whole and not to individual plants. However, when implementing a risk-informed regulatory process, such an approach creates problems because it is difficult to regulate toward an industry average. For example, if we are only interested in the average, then one good plant could make up for one bad plant. Conceivably, plants could actually buy and sell risk credits to each other. Therefore, while the Commission is still interested in the collective industry behavior, implementation in a regulatory sense will be a plant-specific process. That is, if an individual plant proposes a change, decisions will be influenced by the risk at that plant and not so much by the industry average risk.

What risks are to be considered?

Until recently, many of the PRAs performed for plants included only internal events at full power. However, as discussed in Section 2.5, external events and low power/shutdown events can contribute significantly to risk. The safety goal policy does not clearly describe the risks to be included, but current thinking is that external events and low power/shutdown risks should be accounted for in some fashion. This is an extremely important question because many plants will be near or above the subsidiary safety goals if these risks are included. Thus, very little regulatory relief will be available to those plants.

Can plants with low risk be allowed to increase risk up to the Safety Goals?

Some plants are indicating very low risks in their IPE submittals. Assuming that these risk estimates are valid, plants may propose to relax safety programs to save costs. There has been much debate about this issue among the staff. Given that the Commission has indicated that the safety goals represent a state of "safe enough," increases in risk up to the safety goals would seem to be warranted. However, current thinking is that such increases should be minimized because of uncertainties in PRA numbers and skepticism about very low risk estimates. Further, while risk decisions are likely to be made on a plant-specific basis, if all of the plants with risks below the safety goals increase risk up to the goals, then the industry average will clearly be above the goals. Therefore, the current approach allows for only small increases and encourages good plants to maintain low risk levels. The downside of this approach is that it does not reward the good plants and may, in fact, force them to maintain efforts that may not be in place at plants with greater estimated risks.

To what extent can regulatory decisions be based on PRA estimates?

If PRAs were perfect, they could be used as the basis for all regulatory decisions. That is, the only requirement for plants would be to keep their risk below a set level. However, PRAs are obviously imperfect and such an approach is not practical with today's technology. Therefore, PRA will be used to some degree to influence decisions, rather than totally define the solutions. The use of PRA, then, leads to tradeoffs among risk estimates, current regulations, and defense-in-depth principles. As an extreme example, risk estimates might indicate that the CDF is so low that a containment is unnecessary to meet the safety goals; however, defense-in-depth principles would still lead to the need for such a structure. As the use of PRA is debated, the degree to which it can be used in a particular decision will continue to be controversial.

How are uncertainties to be considered?

PRAs, by their nature, produce uncertain results. As shown in Section 2.5, these uncertainties can span orders of magnitude. Further, there is debate within the PRA community as to how uncertainty analyses should be performed. In most cases the Commission and staff have indicated that mean values should be used for comparison purposes when making decisions based on quantitative risk estimates. The safety goal policy indicates that uncertainties should be accounted for, without providing much specific guidance. Various alternatives for treating uncertainties have been proposed, such as setting quantitative limits for the 95th percentile of the risk distribution or performing hypothesis testing on the decision. At this time, such prescriptive criteria for treating uncertainty are generally not being proposed. Rather, it is expected that the use of the somewhat conservative subsidiary safety goals will partially account for uncertainty and that uncertainty estimates will be considered subjectively by the staff in each particular case. The treatment of uncertainty is clearly an area that could use more research and additional guidance in the future.

In considering the answers to the above questions as well as the Commission's guidance in the PRA policy statement, it became clear that regulatory decisions should not be made entirely based on quantitative risk numbers. Other factors needed to be considered. Therefore, the decision was made to change the terminology from "risk-based" regulation to "risk-informed" regulation, reflecting the state of the art in PRA and the need to consider other factors, such as defense-in-depth. The next sections describe a number of risk-informed activities that have been implemented or are being considered.

2.6.3 Reactor Oversight Process (ROP)

The Nuclear Regulatory Commission grants licenses for individual plants based on the Final Safety Analysis Report (FSAR) for the plant and commitments made by the licensee that together constitute the licensing basis for the plant. The Commission charges the NRC staff with the responsibility of assuring that the plant is maintained and operated in accordance with the licensing basis and applicable rules and regulations. The NRC staff carries out this responsibility through its monitoring and inspection process.

The NRC staff does not have the resources to monitor all aspects of the operation and maintenance of every nuclear power plant. The staff can only hope to examine a sample of the operations etc. and from this sample infer compliance status of the plant. The compliance status of individual plants can be expected to vary, perhaps widely. The NRC staff wants, then, to apply greater regulatory attention to those plants having greater difficulty maintaining compliance with their licensing basis. There must be some process that allows the staff to optimize the utilization of its inspection and monitoring resources.

The methods of quantitative risk analyses have not advanced to the point that they can be used to make completely objective determinations about the utilization of the inspection and monitoring resources that the staff has available. Nor, is it likely that these quantitative analysis tools will ever be reliable for making such determinations completely objectively. There will, then, always be a need for a somewhat subjective method for deploying NRC resources. In the past, these determinations were made by senior NRC managers in the so-called SALP process. In the late 1990's this process was criticized by licensees. They complained that the process was not 'transparent' so that they could not readily anticipate the outcome. In some cases, they felt the process could be used to 'rachet' the regulatory requirements imposed on individual licensees. Perhaps of greater importance, the licensees felt that the combination of the SALP process and the NRC's inspection process overemphasized strict regulatory requirements in a way that did not optimize the resources available to the licensee for safety and regulatory activities. The risk significances of findings and conclusions made concerning plants were not being used in readily apparent and predictable ways to weight actions the NRC staff chose to undertake.

In response to these criticisms and the growing need to better optimize the utilization of staff resources, the Nuclear Regulatory Commission developed a revised Reactor Oversight Process. Key objectives of this process are to make greater use of quantitative risk information and, where possible, move regulation toward a more performance basis rather than a prescriptive, compliance basis. The elements of the oversight process are:

- The Cornerstones of Reactor Safety
- Performance Indicators
- Baseline Inspections
- The Significance Determination Process

- The NRC Action Matrix
- The Licensee's Corrective Action Program

Each of these elements of the oversight process is discussed in the subsections that follow.

2.6.3.1 The Cornerstones of Reactor Safety

The basis of the reactor oversight process is made of seven so-called cornerstones of reactor safety that define categories of interest to the NRC staff in the performance of a licensed nuclear power plant. The cornerstones can be considered as falling into three broad categories - Reactor Safety, Radiation Safety and Safeguards. These cornerstones are:

- Reactor Safety
    - The Initiating Events Cornerstone

      Events that cause challenges to safety systems at nuclear power plants should be prevented.
    - The Availability of Mitigating Systems Cornerstone

      Systems to mitigate initiating events at nuclear power plants should have a high availability.
    - Integrity of Barriers to the Release of Radioactivity

      The multiple barriers to the release of radioactivity designed into plants for defense in depth should be kept intact.
    - The Emergency Preparedness Cornerstone

      The system for responding to an event that cannot be mitigated completely should be in a high state of readiness.
- Radiation Safety
    - Limitation of Public Radiation Exposure

      Exposure of the public to radioactive material releases from a plant during normal operations should be kept acceptably low.
    - Limitation of Occupational Exposure to Radiation

      Occupational exposures to radiation should be kept as low as reasonably achievable (ALARA).
- Safeguards
    - Safeguarding Nuclear Materials

      Licensees should have programs to prevent the theft or misuse of nuclear materials.

These cornerstones of reactor safety can be looked upon as the things that the NRC hopes to achieve with its regulatory requirements on licensees. They can also be looked upon as performance objectives for the licensees. They contrast significantly with the categories of evaluation used in the older SALP process which included things like Engineering, Maintenance and Operations.

With performance objectives defined by the cornerstones of reactor safety, it is necessary to have some way to determine how well licensees are meeting these performance objectives. In the reactor oversight process, this is done with Performance Indicators and the Baseline Inspections that are discussed in the next two subsections.

2.6.3.2 Performance Indicators

Associated with each of the cornerstones of reactor safety are performance indicators. The definition of performance indicators is not an easy task. The performance indicators have to be objective quantities that are measurable or easily calculated. Both the licensee and the regulator must agree that the indicators are indicative of the level of performance in some continuous way. The data used for the performance indicator must be easily collected and, in the reactor oversight process, the necessary data are to be collected by the licensee. Finally, and most importantly, the performance indicator cannot be something that represents a major safety failing. That is, the frequency of large pipe breaks cannot be taken as a performance indicator for barrier integrity since such large pipe breaks failures will produce challenges to the plant's safety systems.

Performance indicators are not alien concepts to most licensees. In fact, most licensees maintain quite a large number of performance indicators for their own management purposes. In addition, INPO and WANO demand that licensees maintain performance data used in a variety of indicators. The wide availability of probabilistic risk assessments provides some guidance on appropriate performance indicators for some of the cornerstones such as safety systems availability. More subjective considerations are needed for other cornerstones such as the cornerstone for emergency preparedness.

The performance indicators that the NRC has selected for each of the cornerstones are:

- Initiating Events Cornerstone

  - Unplanned (automatic and manual) scrams per 7000 hours of critical operation
  - risk-significant scrams per 3 years
  - transients per 7000 hours of critical operations

- Availability of Mitigating Systems

  - Safety system unavailability:
    HPCI and RCIC
    HPCS
    Emergency Power
    RHR
    AFW
    HPSI

  - Safety system failures

- Integrity of Barriers to the Release of Radioactivity

  - reactor coolant system specific activity (clad integrity)
  - reactor coolant system leakage
  - containment leakage

- Emergency Preparedness

  - Emergency Response Organization (ERO) drill and exercise performance
  - percentage of Emergency Response Organization shift crews that have participated in a drill or exercise in the past 24 months
  - percentage of the time the Alert and Notification System has been available

- Limitation of Public Radiation Exposure

  - number of effluent events that are reportable per 10 CFR 20, 10 CFR 50 Appendix I, or Technical Specifications

- Limitation of Occupational Exposure to Radiation

  - the number of non-compliances with 10 CFR 20 requirements for (1) high (>1 rem/hr) and (2) very high radiation areas, and uncontrolled personnel exposures exceeding 10% of the stochastic limits or 2% of the non-stochastic limits

- Safeguarding Nuclear Materials

  - security equipment availability
  - Vital Area security equipment availability
  - personnel screening performance

There are three immediately apparent features of the performance indicators. First, the performance indicators cannot be interpreted in a way that would indicate the level of licensee compliance to NRC requirements and licensee commitments. Second, the performance indicators cannot be used either individually or collectively as measures of the risk posed by the continued operation of the plant. The indicators are truly only indicative of the need for additional attention. Third, it is not possible to make comparisons between indicators for different cornerstones. That is, changes in the availability of security equipment availability cannot be compared to changes in the availability of safety systems.

Since the indicators do not yield a measure of risk and they do not yield a measure of compliance to the regulations, it is necessary to define a scale for response to values found for the performance indicators for individual licensees. To do this the NRC has defined performance bands. These bands indicate whether the response to the values of the performance indicators should be by the licensee or by the NRC and if the response is to be by the NRC how intense this response should be. The performance bands are commonly referred to by color and are:

- Green - Licensee Response Band
- White - Increased Regulatory Response Band
- Yellow - Required Regulatory Response Band
- Red - Unacceptable Performance Band

The so-called 'threshold values' for the performance indicators that mark the boundaries of the performance bands are shown in Table 2.6-1. Details of the responses associated with each band are discussed further in connection with the NRC Action Matrix in a later subsection.

The threshold marking the boundary between the Licensee Response Band and the Increased Regulatory Response Band has been set as the 95th percentile of the industry performance. That is, 95% of the currently operating plants will have performance indicator values no worse than the green to white threshold values. This selection for the threshold has raised two questions. First, why are not the thresholds set in plant-specific manners? This question arises especially for those performance indicators that can be assessed using methods of quantitative risk assessment. It has been well-established that the risk posed by a plant is quite dependent on plant-specific features. Failure of emergency power is not of the same risk significance at all plants, for example. The second question is whether the thresholds will change as the performance of the industry as a whole changes. The NRC staff has indicated that they do not plan to change the thresholds in response to changes in the performance of the nuclear industry.

The definitions of the thresholds for bands other than the threshold between the Licensee Response band and the Increased Regulatory Attention band have been controversial especially for the performance indicators associated with Reactor Safety. The NRC staff made an attempt to use risk information to define these thresholds. Nominally the thresholds denote increases in the core damage frequency of 10^{-5} and 10^{-4}/reactor year associated with just the monitored event. Of course, the monitored event is very unlikely to produce core damage because, by assumption, other systems are available. Consequently, some remarkable numbers appear. It would be appalling if a licensee or the NRC let a plant continue to operate that had 20 or more automatic scrams in about a year of operation. These thresholds are now being reconsidered. There is also a research activity to investigate Risk Based Performance Indicators.

2.6.3.3 The Baseline Inspections

The second method for monitoring the performance of licensees is the Baseline Inspection Program. Each licensee is to be subjected to the minimal level of inspection defined by this program. This aspect of the Reactor Oversight Program contrasts with the previous SALP process in which highly rated licensees were granted some relief from routine inspection. The effect of this change is that some licensees have seen their charges for inspection hours increase after imposition of the new Reactor Oversight Program. There have apparently been no complaints from licensees that sustained a reduction in inspection as a result of the newly defined baseline inspection program.

The Baseline Inspection Program is divided into three component types of inspection which are:

- “Complementary Inspections” which deal with areas where performance indicators have not been established.

- “Supplementary Inspections” which deal with areas that performance indicators provide only limited indications of performance.

- “Verification Inspections” which deal with areas that are well treated by the performance indicators and inspection is done to verify that the performance indicator is providing the needed data.

The areas addressed by the Baseline Inspection program are indicated in Table 2.6-2. Risk has been factored into the baseline inspection program in four ways:

- inspectible areas are based on their risk importance in measuring a cornerstone objective,

- the inspection frequency, how many activities to inspect, and how much time to spend inspecting activities in each inspectible area are based on the risk information matrices,

- the selection of activities to inspect in each inspectible area is based on the use of risk information matrices modified by plant-specific information, and

- the inspectors are trained in the use of risk information.

The inspections are carried out by the NRC staff in the Regions. Note that in each of the cornerstones there is an inspectible area called "Identification and resolution of problems". This is the inspection of the licensee Corrective Action Program which is an essential element of the new Reactor Oversight Program and is discussed summarily in a subsection below.

2.6.3.4 The Significance Determination Process

Inspections will inevitably lead to findings. Furthermore, licensees themselves commonly encounter situations where they have inadvertently fallen out of compliance with their licensing basis and report these occurrences to the NRC. In the past, findings of inspectors or licensees would often result in violations of varying degrees of severity. In the new Reactor Oversight Program findings are subjected to a Significance Determination Process. The objectives of the process are:

- to characterize the significance of an inspection finding for the NRC licensee performance assessment process using risk insights as appropriate
- to provide all stakeholders an objective and common framework for communicating the potential safety significance of inspection findings, and
- to provide a basis for assessment and enforcement actions associated with an inspection finding.

The process in all cases involves first an initial characterization of the finding usually by the inspector. Then, the licensee perspective on the initial characterization of the finding significance is sought. NRC makes a final significance determination. The findings are labeled by a color code similar to that used for characterizing performance bands based on performance indicators:

- Green Finding: A finding of very low safety significance.
- White Finding: A finding of low to moderate safety significance
- Yellow Finding: A finding of substantial safety significance
- Red Finding: A finding of high safety significance.

There is, however, clearly a distinction to be made between a Green Finding and the green performance band. When there is a Green Finding, there has been a performance failure albeit one of low safety significance and the licensee is obligated to take actions to correct this failure.

There are four processes for the initial characterization of a finding. The process for characterization of a reactor inspection finding for At-Power situations does involve an assessment of the risk significance based on plant-specific work sheets. These work sheets are usually developed initially by the NRC using risk assessment models and then refined using risk assessment models developed by the specific licensee. The process for characterizing findings associated with occupation radiation safety (primarily issues of ALARA practices and accidental overexposures) and public radiation safety have quantitative elements that are based on judgement. For these findings, the color code does not include Red findings. The process for characterizing findings associated with fire protection is rather involved and includes quantifications based on judgmental inputs concerning the degradation of defense in depth as described in the fire protection regulations (notably 10CFR50 Appendix R).

2.6.3.5 The NRC Action Matrix

The combination of performance indicators and inspection findings are inputs to the NRC Action Matrix which defines escalating responses to the inputs. This Action Matrix is shown in Table 2.6-3. Note that a single white input or two white inputs for different cornerstones is still interpreted as meaning that the licensee is fully meeting the safety objectives defined by the cornerstones. Two white inputs for a particular cornerstone or a yellow input means that there is some degradation in licensee performance, but there has been minimal reduction in the safety margins. A similar conclusion is reached in the case of three white inputs to a particular class of cornerstones - Reactor Safety, Radiation Safety or Safeguards. Multiple yellow inputs or any red input implies that there has been substantial failure to meet the safety objectives and there have been significant reductions in the safety margins that merit response not only by the Regions, but also by the Agency as a whole. When the conclusion is reached that performance is unacceptable, the plant will not be permitted to operate.

2.6.3.6 Licensee Corrective Action Program

The most common response from the inputs provided by the inspections and the performance indicators is for additions to the licensee's corrective action programs. All licensee have these programs. If nothing else, they are mandated by the Maintenance Rule (10CFR50.65). They take on a very central role in the new Reactor Oversight Program. In fact, much of the routine inspection that was done in the past by the NRC at nuclear power plants has been transformed into an inspection of the licensee's corrective action program and the ability of the licensee to identify and resolve problems and issues that arise in the operation of power plants.

2.6.4 Regulatory Guide 1.174

As this document is being written, regulatory guidance for risk-informed regulation is still being developed. However, one landmark document that has been issued is Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis."[3] This document is intended for use in evaluating plant-specific changes to the licensing basis of an individual plant.

2.6.4.1 A Four-Element Approach to Integrated Decision Making

Given the principles of risk-informed decisionmaking discussed above, the staff has identified a four-element approach to evaluating proposed LB changes. This approach, which is presented graphically in Figure 2.6-1, acceptably supports the NRC's decisionmaking process. This approach is not sequential in nature; rather it is iterative.

Element 1: Define the Proposed Change

Element 1 involves three primary activities. First, the licensee should identify those aspects of the plant's licensing bases that may be affected by the proposed change, including, but not limited to, rules and regulations, final safety analysis report (FSAR), technical specifications, licensing conditions, and licensing commitments. Second, the licensee should identify all structures, systems, and components (SSCs), procedures, and activities that are covered by the LB change under evaluation and consider the original reasons for inclusion of each program requirement. Third, the licensee should identify available engineering studies, methods, codes, applicable plant-specific and industry data and operational experience, PRA findings, and research and analysis results relevant to the proposed LB change. With particular regard to the plant-specific PRA, the licensee should assess the capability to use, refine, augment, and update system models as needed to support a risk assessment of the proposed LB change.

The licensee should describe the proposed change and how it meets the objectives of the NRC's PRA Policy Statement. In addition to improvements in reactor safety, this assessment may consider benefits from the LB change such as reduced fiscal and personnel resources and radiation exposure. The licensee should affirm that the proposed LB change meets the current regulations, unless the proposed change is explicitly related to a proposed exemption or rule change.

Element 2: Perform Engineering Analysis

As part of the second element, the licensee will evaluate the proposed LB change with regard to the principles that adequate defense-in-depth is maintained, that sufficient safety margins are maintained, and that proposed increases in core damage frequency and risk are small and are consistent with the intent of the Commissions's Safety Goal Policy Statement.

Defense-in-Depth -- The engineering evaluation conducted should evaluate whether the impact of the proposed LB change (individually and cumulatively) is consistent with the defense-in-depth philosophy. Defense-in-depth is maintained if:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.

- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.

- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers).

- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.

- Independence of barriers is not degraded.

- Defenses against human errors are preserved.

- The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.

Safety Margins -- The engineering evaluation conducted should assess whether the impact of the proposed LB change is consistent with the principle that sufficient safety margins are maintained. Here also, the licensee is expected to choose the method of engineering analysis appropriate for evaluating whether sufficient safety margins would be maintained if the proposed LB change were implemented. Sufficient safety margins are maintained if:

- Codes and standards or their alternatives approved for use by the NRC are met.

- Safety analysis acceptance criteria in the LB (e.g., FSAR, supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

Evaluation of Risk Impact, Including Treatment of Uncertainties --

The licensee's risk assessment may be used to address the principle that proposed increases in CDF and risk are small and are consistent with the intent of the NRC's Safety Goal Policy Statement. For purposes of implementation, the licensee should assess the expected change in CDF and LERF. The necessary sophistication of the evaluation, including the scope of the PRA (e.g., internal events only, full power only), depends on the contribution the risk assessment makes to the integrated decisionmaking, which depends to some extent on the magnitude of the potential risk impact.

There are three parts to using the PRA results in decisiomaking:

- Assure that the quality and scope of the PRA is adequate for the intended application.

- Compare the CDF and LERF results to the acceptance guidelines. The overall baseline CDF and LERF are examined, along with the impact of the proposed change.

- Examine the uncertainties in the results and assess their potential impact on the decision.

These three items are discussed in more detail in RG 1.174. The acceptance guidelines were the subject of considerable debate and are presented below.

The risk-acceptance guidelines are structured as follows. Regions are established in the two planes generated by a measure of the baseline risk metric (CDF or LERF) along the x-axis, and the change in those metrics (CDF or LERF) along the y-axis (Figures 2.6-2 and 2.6-3), and acceptance guidelines are established for each region as discussed below. These guidelines are intended for comparison with a full-scope (including internal events, external events, full power, low power, and shutdown) assessment of the change in risk metric, and when necessary, as discussed below, the baseline value of the risk metric (CDF or LERF). However, it is recognized that many PRAs are not full scope and PRA information of less than full scope may be acceptable in some cases.

There are two sets of acceptance guidelines, one for CDF and one for LERF, and **both** sets should be used.

- If the application clearly can be shown to result in a decrease in CDF, the change will be considered to have satisfied the relevant principle of risk-informed regulation with respect to CDF. (Because Figure 2.6-3 is drawn on a log scale, this region is not explicitly indicated on the figure.)

- When the calculated increase in CDF is very small, which is taken as being less than 10^{-6} per reactor year, the change will be considered regardless of whether there is a calculation of the total CDF (Region III). While there is no requirement to calculate the total CDF, if there is an indication that the CDF may be considerably higher than 10^{-4} per reactor year, the focus should be on finding ways to decrease rather than increase it.

- When the calculated increase in CDF is in the range of 10^{-6} per reactor year to

10^{-5} per reactor year, applications will be considered only if it can be reasonably shown that the total CDF is less than 10^{-4} per reactor year (Region II).

- Applications that result in increases to CDF above 10^{-5} per reactor year (Region I) would not normally be considered.

AND

- If the application clearly can be shown to result in a decrease in LERF, the change will be considered to have satisfied the relevant principle of risk-informed regulation with respect to LERF. (Because Figure 2.6-3 is drawn with a log scale, this region is not explicitly indicated on the figure.)

- When the calculated increase in LERF is very small, which is taken as being less than 10^{-7} per reactor year, the change will be considered regardless of whether there is a calculation of the total LERF (Region III). While there is no requirement to calculate the total LERF, if there is an indication that the LERF may be considerably higher than 10^{-5} per reactor year, the focus should be on finding ways to decrease rather than increase it.

- When the calculated increase in LERF is in the range of 10^{-7} per reactor year to 10^{-6} per reactor year, applications will be considered only if it can be reasonably shown that the total LERF is less than 10^{-5} per reactor year (Region II).

- Applications that result in increases to LERF above 10^{-6} per reactor year (Region I) would not normally be considered.

These guidelines are intended to provide assurance that proposed increases in CDF and LERF are small and are consistent with the intent of the Commission's Safety Goal Policy Statement.

As indicated by the shading on the figures, the change request will be subject to an NRC technical and management review that will become more intensive when the calculated results are closer to the region boundaries.

The guidelines discussed above are applicable for full power, low power, and shutdown operations. However, during certain shutdown operations when the containment function is not maintained, the LERF guideline as defined above is not practical. In those cases, licensees may use more stringent baseline CDF guidelines (e.g., 10^{-5} per reactor year) to maintain an equivalent risk profile or may propose an alternative guideline that assures proposed increases in risk are small and are consistent with the Commission's Safety Goal Policy Statement.

Integrated Decisionmaking

The results of the different elements of the engineering analyses must be considered in an integrated manner. None of the individual analyses is sufficient in and of itself. In this way, it can be seen that the decision will not be driven solely by the numerical results of the PRA. They are one input into the decisionmaking and help in building an overall picture of the implications of the proposed change on risk. The PRA has an important role in putting the change into its proper context as it impacts the plant as a whole.

An application will be given increased NRC management attention when the calculated values of the changes in the risk metrics, and their baseline values when appropriate, approached the guidelines. Therefore, the issues in the submittal that are expected to be addressed by NRC management include:

- The cumulative impact of previous changes and the trend in CDF (the licensee's risk management approach);
- The cumulative impact of previous changes and the trend in LERF (the licensee's risk management approach);
- The impact of the proposed change on operational complexity, burden on the operating staff, and overall safety practices;
- Plant-specific performance and other factors (for example, siting factors, inspection findings, performance indicators, and operational events), and Level 3 PRA information, if available;
- The benefit of the change in relation to its CDF/LERF increase;
- The practicality of accomplishing the change with a smaller CDF/LERF impact; and
- The practicality of reducing CDF/LERF when there is reason to believe that the baseline CDF/LERF are above the guideline values (i.e., 10^{-4} and 10^{-5} per reactor year).

Element 3: Define Implementation and Monitoring Program

Careful consideration should be given to implementation and performance-monitoring strategies. The primary goal for this element is to ensure that no adverse safety degradation occurs because of the changes to the LB. The staff's principal concern is the possibility that the aggregate impact of changes that affect a large class of SSCs could lead to an unacceptable increase in the number of failures from unanticipated degradation, including possible increases in common cause mechanisms. Therefore, an implementation and monitoring plan should be developed to ensure that the engineering evaluation conducted to examine the impact of the proposed changes continues to reflect the actual reliability and availability of SSCs that have been evaluated. This will ensure that the conclusions that have been drawn from the evaluation remain valid.

The staff expects licensees to propose monitoring programs that include a means to adequately track the performance of equipment that, when degraded, can affect the conclusions of the licensee's engineering evaluation and integrated decisionmaking in support of the change to the LB. The program should be capable of trending equipment performance after a change has been implemented to demonstrate that performance is consistent with that assumed in the traditional engineering and probabilistic analyses that were conducted to justify the change. This may include monitoring associated with non-safety-related SSCs, if the analysis determines those SSCs to be risk significant. The program should be structured such that (1) SSCs are monitored commensurate with their safety importance, i.e., monitoring for SSCs categorized as having low safety significance may be less rigorous than that for SSCs of high safety significance, (2) feedback of information and corrective actions are accomplished in a timely manner, and (3) degradation in SSC performance is detected and corrected before plant safety can be compromised. The potential impact of observed SSC degradation on similar components in different systems throughout the plant should be considered.

Element 4: Submit Proposed Change

Requests for proposed change to the plant's LB typically take the form of requests for license amendments (including changes to or removal of license conditions), technical changes, changes to or withdrawals of orders, and changes to programs.

Licensees are free to decide whether to submit risk information in support of their LB change request. If the licensee's proposed change to the LB is consistent with currently approved staff positions, the staff's determination will be based solely on traditional engineering analysis without recourse to risk information (although the staff may consider any risk information which is submitted by the licensee). However, if the licensee's proposed change goes beyond currently approved staff positions, the staff will normally consider both information based upon traditional engineering analysis and information based upon risk insights.

2.6.5 Recent Regulatory Changes

2.6.5.1 Maintenance Rule (10CFR50.65)

Beginning in July, 1996, nuclear power plant licensees were required to comply with the Maintenance Rule (10 CFR 50.65):

> *Each holder of a license to operate a nuclear power plant. . . shall monitor the performance or condition of structures, systems and components, against licensee-established goals, in a manner sufficient to provide reasonable assurance that such structures, systems and components . . . are capable of fulfilling their intended functions. Such goals shall be established commensurate with safety and, where practical, take into account industry-wide operating experience. When the performance or condition of a structure, system or component does not meet established goals, appropriate corrective action shall be taken.*

The Nuclear Regulatory Commission was moved to impose this additional requirement on plants because of evidence that maintenance-related system failures were leading to unplanned plant shutdowns or other safety-related issues. The evidence suggested that it was not just the maintenance of safety-related structures, systems, and components that was of concern. Other systems not usually considered safety-related within the context of reactor regulations needed to be addressed. Consequently, the scope of the Maintenance Rule is large:

- *safety-related structures, systems, and components that are relied upon to remain functional during and following design basis events to ensure:*
    - *the integrity of the reactor coolant pressure boundary,*
    - *the capability to shutdown the reactor and maintain it in a safe shutdown condition, or*
    - *the capability to prevent or mitigate the consequences of accidents that could result in offsite exposures comparable to the guidelines in 50.34(a)(1), 50.67(b)(2), or 100.11.*

- *Nonsafety related structures, systems and components:*
    - *that are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs); or*

- *whose failure could prevent safety-related structures, systems and components from fulfilling their safety-related functions; or*
- *whose failure could cause a reactor scram or actuation of a safety-related system.*

The Maintenance Rule also applies explicitly to the safe storage of spent reactor fuel for both operating reactors and reactors that are being permanently shutdown.

The Maintenance Rule requires that licensees first decide whether structures, systems and components are within the scope of the rule. A decision tree for this first categorization is shown in Figure 2.6-4. Then, the licensees must decide if the structures, systems and components need to be monitored (so-called a(1) SSCs) or are adequately treated by the existing preventive maintenance program (a(2) SSCs). A decision 'tree' for this second categorization is shown in Figure 2.6-5.

The breadth of the concern over maintenance is sufficient that usual, generic, prescriptive regulations concerning maintenance would easily overwhelm both licensees and staff and would take tremendous effort to develop and implement. At the same time, prescriptive regulations would not take advantage of engineering creativity within the nuclear industry. Consequently, the Commission chose a more performance-based approach that allowed the industry to define maintenance goals based on safety. It is noteworthy that safety rather than risk was selected as the basis for the goals. Even in 1996, there was not the confidence in the tools for quantitative risk assessment to adopt quantitative measures of risk into the regulation nor was there a willingness to create a defacto requirement that all plants have probabilistic risk assessments (PRAs). Nevertheless, the rule states that:

- *Adjustments shall be made where necessary to ensure that the objective of preventing failures of structures, systems, and components is appropriately balanced against the objective of minimizing the unavailability of structures, systems and components due to monitoring and preventive maintenance,*

and, as originally promulgated,

- *An assessment of the total plant equipment that is out of service should be taken into account to determine the overall effect on performance of safety functions.*

This created an interest in using quantitative risk assessment methods to implement the rule.

Even when a licensee wants to use quantitative risk assessment methods in connection with the Maintenance Rule, there is a significant hurdle. Typically, a probabilistic risk assessment will address directly no more than about 2000 components or systems in a plant that may have 24,000 components and systems subject to the Maintenance Rule. The problem of setting availability goals for the systems that are not addressed in the probabilistic risk assessments then arises.

To address this difficulty NUMARC and later the Nuclear Energy Institute (NEI) developed guidance for the industry that has been endorsed by the NRC staff in Regulatory Guide 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants". This guidance defined so-called Expert Panels that actually make the classifications of structures, systems and components for the purposes of the Maintenance Rule. Where quantitative risk information is available the Expert Panel can use importance metrics such as 'risk achievement worth' (RAW) and 'risk reduction worth' (RRW) for the purposes of classification and setting availability goals. Experience and expert judgement must be used as the basis for the classification of structures, systems and components that are not treated explicitly by quantitative risk analyses. Even when quantitative risk importance measures are available, expert judgement is required to appreciate the limitations of these measures. The most limiting failing of these measures is that they do not account for the simultaneous unavailability of multiple systems and components.

The Maintenance Rule also specifies what licensees are to do in the event that the maintenance goals are not met:

> *When the performance or condition of a structure system or component does not meet established goals, appropriate corrective action shall be taken.*

This requirement of the Maintenance Rule created the licensee corrective action programs that are crucial elements of the revised reactor oversight process discussed elsewhere in this document.

The NRC staff conducted an early study of the ways licensees had implemented the Maintenance Rule, "Lessons Learned from Early Implementation of the Maintenance Rule at Nine Nuclear Power Plants"(NUREG-1526, 1995). An immediate conclusion reached in the assessment of license implementation of the Maintenance rule was that the requirement for assessment of the risk significance of removing systems from service for maintenance was being interpreted in a limited fashion. License did not sufficiently appreciate that the Maintenance Rule applied to all modes of operation including shutdown and low power modes of operation. Consequently, the Commission developed what became known as the a(4) modification to 10CFR50.65:

> *Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.*

This requirement of the Maintenance Rule has contributed to the substantial increase in attention licensees pay to the planning of outages. Most licensees now have matrices of combinations of equipment that are not permitted to be simultaneously removed from service. Many licensees have software that allows at least a semi-quantitative assessment of the risk impact of planned maintenance activities.

Other conclusions reached in the early assessment of the implementation of the Maintenance Rule included:

- Licensees had difficulty in utilizing industry experience in setting maintenance goals.

- Many licensees used too limited a set of importance measures in classifying structures, systems and components.
- Often structures were considered 'inherently safe' and not treated in accordance with the expectations from the Maintenance Rule. Monitoring of structures was criticized as not predictive and not capable of giving early warning of degradation.
- Some licensees were reluctant to categorize structures, systems and components as requiring the a(1) treatment because of concern that this might imply that their preventive maintenance programs were ineffective.
- Licensees often could not demonstrate performance criteria and goals were commensurate with the safety significance of a structure, system or component.
- Some licensees did not balance reliability and availability for high safety significant structures, systems and components.
- There can be confusion in identifying system failures as preventable by maintenance.

2.6.5.2 Risk-Informed Technical Specifications

Technical specifications (TS) are key requirements outlining the limits of acceptable operation for nuclear power plants. Section 182a of the Atomic Energy Act requires that applicants for nuclear power plant operating licenses state:

> *Such technical specifications, including information of the amount, kind, and source of special nuclear material required, the place of the use, the specific characteristics of the facility, and such other information as the Commission may, by rule or regulation, deem necessary in order to enable it to find that the utilization ...of special nuclear material will be in accord with the common defense and security and will provide adequate protection to the health and safety of the public. Such technical specifications shall be a part of any license issued.*

In Section 50.36, "Technical Specifications," of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," the Commission established its regulatory requirements related to the content of TS. In doing this, the Commission emphasized matters related to the prevention of accidents and the mitigation of accident consequences; the Commission noted that applicants were expected to incorporate into their TS "those items that are directly related to maintaining the integrity of the physical barriers designed to contain radioactivity".[4] Pursuant to 10 CFR 50.36, TS are required to contain items in the following five specific categories: (1) safety limits, limiting safety system settings, and limiting control settings, (2) limiting conditions for operation, (3) surveillance requirements, (4) design features, and (5) administrative controls.

For the most part, TS have played a major role in ensuring plant safety and maintaining safe operating conditions. However, in some cases TS have led to unnecessary burden on the plants and have even been counter to safety. Previously, it was not uncommon for plants to be required to shut down if a shutdown cooling system failed a surveillance test. Clearly, this made no sense. Further, we are now more aware of the risks associated with shutdown operations and the transitions from power operation. A risk-informed approach allows the NRC and the licensees to consider the risk tradeoffs from requiring a shutdown due to a TS violation. Allowing a plant to remain at power by extending the allowed outage time of a component may be best for both the licensee and the public, provided that a careful analysis is performed.

Some aspects of TS, particularly limiting conditions for operation and surveillance requirements are particularly amenable to PRA analysis. Changes to these items are simply reflected in the unavailabilities of the SSCs in the PRA analysis. Therefore, the risk impact of changes can be readily evaluated, provided that an adequate PRA is available (this is often not the case).

Since the mid-1980s, the NRC has been reviewing and granting improvements to TS based, at least in part, on PRA insights. Some of these improvements have been proposed by the Nuclear Steam Supply System (NSSS) owners groups to apply to an entire class of plants. Many others have been proposed by individual licensees. Typically, the proposed improvements involved a relaxation of one or more allowed outage times (AOTs) or surveillance test intervals (STIs) in the TS.

In its July 22, 1993, final policy statement on TS improvements),[5] the Commission stated that it:

> *...expects that licensees, in preparing their Technical Specification related submittals, will utilize any plant-specific PSA or risk survey and any available literature on risk insights and PSAs . . . Similarly, the NRC staff will also employ risk insights and PSAs in evaluating Technical Specifications related submittals. Further, as a part of the Commission's ongoing program of improving Technical Specifications, it will continue to consider methods to make better use of risk and reliability information for defining future generic Technical Specification requirements.*

The Commission reiterated this point when it issued the revision to 10 CFR 50.36 in July 1995).[6]

Regulatory Guide 1.177 describes an acceptable approach for making risk-informed changes to TS. The approach follows the basic four element approach from Regulatory Guide 1.174, described in the previous section.

A three-tiered approach has been identified for licensees to evaluate the risk associated with proposed TS AOT changes (part of Element 2, Engineering Evaluation). Tier 1 is an evaluation of the impact on plant risk of the proposed TS change as expressed by the change in core damage frequency(CDF), the incremental conditional core damage probability (ICCDP), and, when appropriate, the change in large early release frequency (LERF) and the incremental conditional large early release probability (ICLERP).

Tier 2 is an identification of potentially high-risk configurations that could exist if equipment in addition to that associated with the change were to be taken out of service simultaneously, or other risk-significant operational factors such as concurrent system or equipment testing were also involved. The objective of this part of the evaluation is to ensure that appropriate restrictions on dominant risk-significant configurations associated with the change are in place.

Tier 3 is the establishment of an overall configuration risk management program to ensure that other potentially lower probability, but nonetheless risk-significant, configurations resulting from maintenance and other operational activities are identified and compensated for. If the Tier 2 assessment demonstrates, with reasonable assurance, that there are no risk-significant configurations involving the subject equipment, the application of Tier 3 to the proposed AOT may not be necessary.

More details concerning the guidance for performing an acceptable PRA for TS evaluation are contained in Regulatory Guide 1.77. Other elements of the TS analysis follow closely the elements of Regulatory Guide 1.74.

2.6.5.3 Risk-Informed In-Service Testing

In-service testing (IST) of important safety equipment is required at specified intervals in order to assure operability were the equipment needed to respond to an accident situation. Such equipment is typically in a standby mode and does not operate until demanded. IST requirements are defined in 10 CFR 50.55a(f) and in Section XI of the ASME Boiler and Pressure Vessel Code.[8]

IST, while an essential part of ensuring safety, can become a problem in some situations. For example, tests can demand licensee resources, stress the equipment being tested, and result in increased worker radiation exposures. Therefore, it is appropriate to consider reducing IST requirements when the risk impact can be shown to be negligible.

Regulatory Guide 1.175 describes an approach for risk-informed IST, primarily to be applied to pumps and valves.[9] As with other risk-informed initiatives, it follows the approach outlined in Regulatory Guide 1.174. Potential changes include changing test intervals, testing methods and component groupings.

The fundamental approach of Regulatory Guide 1.175 is to group components into low safety-significant components (LSSC) and high safety-significant components (HSSC). Components in the LSSC group receive less attention, in terms of test intervals and rigorous testing, while components in the HSSC group receive the most attention.

Components are initially categorized into HSSC and LSSC groupings based on threshold values for PRA importance measures. As discussed in Regulatory Guide 1.174, while a licensee is free to choose the threshold values of importance measures, it will be necessary to demonstrate that the integrated impact of the change is such that Principle 4 is met.

PRA systematically takes credit for non-Code components as providing support, acting as alternatives, and acting as backups to those components that are within the current Code. Accordingly, to ensure that the proposed RI-IST program will provide an acceptable level of quality and safety, these additional risk-important components should be included.

Although PRAs model many of the SSCs involved in the performance of plant safety functions, other SSCs are not modeled for various reasons. However, this should not imply that unmodeled components are not important in terms of contributions to plant risk. For example, some components are not modeled because certain initiating events may not be modeled (e.g., low power and shutdown events, or some external events); in other cases, components may not be directly modeled because they are grouped together with events that are modeled (e.g., initiating events, operator recovery events, or within other system or function boundaries); and in some cases, components are screened out from the analysis because of their assumed inherent reliability; or failure modes are screened out because of their insignificant contribution to risk (e.g., spurious closure of a valve). When feasible, adding missing components or missing initiators or plant operating states to the PRA should be considered by the licensee. When this is not feasible, information based on traditional engineering analyses and judgment is used to determine whether a component should be treated as an LSSC or HSSC. One approach to combining these different pieces of information is to use what has been referred to as an expert panel.

In classifying a component not modeled in the PRA as LSSC, the expert panel should have determined that:

- The component does not perform a safety function, or does not perform a support function to a safety function, or does not complement a safety function.
- The component does not support operator actions credited in the PRA for either procedural or recovery actions.
- The failure of the component will not result in the eventual occurrence of a PRA initiating event.
- The component is not a part of a system that acts as a barrier to fission product release during severe accidents.
- The failure of the component will not result in unintentional releases of radioactive material even in the absence of severe accident conditions.

For acceptance guidelines, when using risk importance measures to identify components that are low risk contributors, the potential limitations of these measures have to be addressed. Therefore, information to be provided to the licensee's integrated decisionmaking process (e.g., expert panel) must include evaluations that demonstrate the sensitivity of the risk importance results to the important PRA modeling techniques, assumptions, and data. Issues that the licensee should consider and address when determining low risk contributors include truncation limit used, different risk metrics (i.e., CDF and LERF), different component failure modes, different maintenance states and plant configurations, multiple component considerations, defense in depth, and analysis of uncertainties (including sensitivity studies to component data uncertainties, common- cause failures, and recovery actions).

While the categorization process can be used to highlight areas in which testing strategy can be improved and areas in which sufficient safety margins exist to the point that testing strategy can be relaxed, it is the determination of the change in risk from the overall changes in the IST program that is of concern in demonstrating that Principle 4 has been met. Therefore, no generically applicable acceptance guidelines for the threshold values of importance measures used to categorize components as HSSC or LSSC are given here. Instead, the licensee should demonstrate that the overall impact of the change on plant risk is small.

As part of the categorization process, licensees must also address the initiating events and plant operating modes missing from the PRA evaluation. The licensee can do this either by providing qualitative arguments that the proposed change to the IST program does not result in an increase on risk, or by demonstrating that the components significant to risk in these missing contributors are maintained as HSSC.

2.6.6 NRC Initiatives for Regulatory Change

RG 1.174 described a process for making plant-specific changes. The NRC is also considering broader risk-informed changes to 10CFR50 that could be applied to groups of plants or the industry as a whole. In SECY 98-300, (SECY-98-300, "Options For Risk Informed Revisions to 10CFR Part 50 - 'Domestic Licensing of Production and Utilization Facilities,'", December 23, 1998) the staff identified three options for addressing 10CFR50:

(1) continue with current activities, but make no changes to the current Part 50,

(2) make changes to the overall scope of systems, structures, and components (SSCs) covered by those sections of Part 50 requiring special treatment (such as quality assurance, technical specifications, environmental qualification, and 50.59 by formulating new definitions of safety-related and important-to-safety SSCs)(2), and

(3) make changes to specific requirements in the body of regulations, including general design criteria (GDCs).

The Commission directed the ·staff to undertake Option 2 in the short-term and Option 3 as a longer-term activity. Work on both options is currently in progress.

Option 2

The information below is taken from SECY-99-256, "Rulemaking Plan for Risk-Informing Special Treatment Requirements", USNRC, October 29, 1999.)

The purpose of this rulemaking is to develop an alternative regulatory framework that enables licensees, using a risk-informed process for categorizing SSCs according to their safety significance (i.e., a decision that considers both traditional deterministic insights and risk insights), to reduce unnecessary regulatory burden for SSCs of low safety significance by removing these SSCs from the scope of special treatment requirements. In the process, both the NRC staff and industry should be able to better focus their resources on regulatory issues of greater safety significance. This framework should improve regulatory effectiveness and efficiency, and contribute to enhanced plant safety. To accomplish this goal, it is necessary to amend the governing regulations. The current regulations use terms such as "safety-related," "important to safety," and "basic component" to identify the groups of SSCs and associated activities that require "special treatment." This rulemaking will build into the regulations an alternative that offers licensees the flexibility of utilizing a risk-informed process to evaluate the need for special treatment.

This risk-informed process will ensure that risk insights will be used in a manner that complements the NRC's traditional deterministic approach. The risk-informed approach will be consistent with the defense-in-depth philosophy, will maintain sufficient safety margins, will ensure that any increase in core damage frequency or risk is small and consistent with the safety goal policy statement, and will include a performance measurement strategy. The risk-informed framework will also be aligned to the NRC Reactor Inspection Oversight process by incorporating the cornerstones from the reactor safety and radiation protection safety areas into the SSC categorization process.

A graphical depiction of the changes that are expected to result from a risk-informed re-categorization of SSCs is illustrated in Figure 2.6-6. The figure is only intended to provide a conceptual understanding of the new SSC categorization process. The staff's thinking is continuing to evolve on this matter. The figure depicts the current safety-related versus nonsafety-related SSC categorization scheme with an overlay of the new risk-informed categorization. The risk-informed categorization would group SSCs into one of the four boxes in Figure 2.6-7.

Box 1 of Figure 2.6-7 contains safety-related SSCs that a risk-informed categorization process concludes are significant contributors to plant safety. These SSCs are termed risk-informed safety class 1 (RISC-1) SSCs. SSCs in this box would continue to be subject to the current special treatment requirements. In addition, it is possible that some of these SSCs may have additional requirements concerning reliability and availability, if attributes which cause an SSC to be safety significant are not sufficiently controlled by current special treatment requirements. However, the staff is not currently aware of any examples of this situation.

Box 2 depicts the SSCs that are nonsafety-related, and that the risk-informed categorization concludes make a significant contribution to plant safety. These SSCs are termed RISC-2 SSCs. Examples of RISC-2 SSCs could include the station blackout emergency diesel, startup feedwater pumps, or SSCs that function for pressurized water reactor (PWR) "feed and bleed" capability. For RISC-2 SSCs, there will probably need to be requirements to maintain the reliability and availability of the SSCs consistent with the probabilistic risk assessment (PRA). As discussed below, it is currently envisioned that 10 CFR 50.69 (i.e., the new rule) would contain the regulatory treatment requirement for RISC-1 and RISC-2 SSCs regarding the reliability and availability of these SSCs.

Box 3 depicts the currently safety-related SSCs that a risk-informed categorization process determines are not significant contributors to plant safety. These SSCs are termed RISC-3 SSCs. The rulemaking would revise Part 50 to contain alternative requirements (per §50.69) such that RISC-3 SSCs would no longer be subject to the current special treatment requirements. For RISC-3 SSCs, it is not the intent of this rulemaking to allow such SSCs to be removed from the facility, or to have their functional capability lost. Instead, the RISC-3 SSCs will need to receive sufficient regulatory treatment such that these SSCs are still expected to meet functional requirements, albeit at a reduced level of assurance. The staff may determine that this level of assurance can be provided by licensee's commercial grade programs. As discussed below, it is currently envisioned that §50.69 would contain the regulatory treatment requirements for RISC-3 SSCs.

Box 4 depicts SSCs that are non safety-related and continue to be categorized as not being significant contributors to plant safety. These SSCs are out of scope of both current special treatment and any future regulatory controls of §50.69. The functional performance of these SSCs is controlled under the licensee's commercial grade program (no change from the current requirements).

Debate is ongoing about the implementation of this approach. Most of the concern revolves around Box 3 and the degree of regulation needed for these SSCs.

There are literally thousands of SSCs that may fall into Box 3 at a given plant; therefore, the stakes are high. South Texas has submitted an exemption request that is similar in nature to what Option 2 would allow. It does not follow exactly the same process, however, and is based on a licensee PRA that is better than the industry average.

Option 3

In SECY-98-300, the staff delineated the following broad objectives for its work to risk-inform 10 CFR Part 50:

- Enhance safety by focusing NRC and licensee resources in areas commensurate with their importance to health and safety,
- Provide NRC with the framework to use to risk information to take action in reactor regulatory matters, and
- Allow use of risk information to provide flexibility in plant operation and design, which can result in burden reduction without compromising safety.

SECY 00-198[7] describes staff progress on more comprehensive changes to 10CFR50. A framework for guiding these changes has been developed and is presented below, although it continues to evolve.

Option 3 Framework Overview

Figure 2.6-8 illustrates the key elements of the framework. The primary goal is to protect the public health and safety. The framework constitutes a risk-informed, defense-in-depth approach. It will be used by the NRC staff to analyze the effectiveness of existing regulations in supporting the primary goal. When the staff determines that the effectiveness of an existing regulation can be improved, an alternative risk-informed regulation, which is consistent with the framework, is formulated and recommended to the Commission.

As indicated in Figure 2.6-8, this approach is consistent with cornerstones of safe nuclear power plant operations, which were identified in the NRC Reactor Inspection and Oversight Program. Specific strategies and related elements of the framework are used to implement the cornerstones as discussed below along with quantitative guidelines for implementation.

Defense-in-Depth Approach

The term defense-in-depth is used to describe applications of multiple measures to prevent or mitigate accidents. The measures can be embodied in SSCs or in procedures (including emergency plans). Defense-in-depth can be applied in various ways. Redundant or diverse means may be used to accomplish a function, the classic example being the use of multiple barriers (fuel, cladding, reactor coolant pressure boundary, spray or scrubbing systems, and containment) to limit the release of core radionuclides. Alternatively, redundant or diverse functional lines of defense may be used to accomplish a goal.

To illustrate, consider the primary goal of protecting the public from nuclear power plant accidents. As indicated in Figure 2.6-8, the first line of defense is to eliminate initiators that could conceivably lead to core damage. However, it is not possible to eliminate all initiators. The frequency of initiators, although significantly less than before the accident at Three Mile Island Unit 2 (TMI-2), is about 1 per plant year. As a second line of defense, systems such as the Emergency Core Cooling System (ECCS) are provided to prevent core damage should postulated initiators occur. Although such systems are designed for a wide spectrum of initiators and compounding equipment failures, no prevention system is perfect. As a third line of defense, barriers including containment and associated heat and fission product removal systems are required. These barriers would prevent large radionuclide releases for many severe accidents, but scenarios exist in which containment would be breached or bypassed. A fourth line of defense, offsite emergency preparedness, is therefore required.

Defense-in-depth has evolved since the first research reactors were designed in the 1940s. The approach adopted herein requires accident prevention and mitigation strategies and supporting elements. Probabilistic insights are used in implementing the required strategies and elements. The approach used in Option 3 is summarized in the following working definition:

Defense-in-depth is the approach taken to protect the public by applying the following strategies in a risk-informed manner:

1. limit the frequency of accident initiating events

2. limit the probability of core damage given accident initiation

3. limit radionuclide releases during core damage accidents

4. limit public health effects due to core damage accident

The strategies consider the following defense-in-depth elements:

- reasonable balance is provided among the strategies (as shown in Figure 2.6-8).

- over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.

- independence of barriers is not degraded.

- safety function success probabilities commensurate with accident frequencies, consequences, and uncertainties are achieved via appropriate:

  - redundancy, independence, and diversity,
  - defenses against common cause failure mechanisms,
  - defenses against human errors, and
  - safety margins

- the defense-in-depth objectives of the current General Design Criteria (GDCs) in Appendix A to 10 CFR 50 are maintained.

The four strategies emphasizes defense against core damage accidents, which dominate the risk to public health and safety posed by existing plants. Quantitative guidelines are developed to characterize a reasonable balance among the preventive and mitigative strategies. For risk significant accidents in which one or more of the four strategies are precluded (e.g., containment bypass accidents), the remaining strategies may be more tightly regulated; that is, regulations should provide a very high confidence in the remaining strategies.

Similarly, more stringent requirements may be imposed in the presence of large uncertainties regarding the effectiveness of one of the strategies.

Cornerstones and Strategies

The cornerstones for safe nuclear power plant operation were discussed in Section 2.6.3.1. The four reactor safety cornerstones are directly addressed in PRAs and are, therefore, most relevant to the initial Option 3 efforts. As illustrated in Figure 2.6-8, the four reactor safety cornerstones are reflected in the framework by the four defense-in-depth strategies. The strategies seek both to prevent core damage accidents and to mitigate the public impact should a core damage accident occur. The two preventive strategies are:

- limit the frequency of accident initiating events (initiators), and
- limit the probability of core damage given accident initiation.

The two mitigative strategies are:

- limit radionuclide releases during core damage accidents, and
- limit public health effects due to core damage accidents.

Except for the implied emphasis on core damage accidents, Strategy 1 is identical to Reactor Safety Cornerstone 1. Similarly, for core damage accidents, Strategy 4 is equivalent to Reactor Safety Cornerstone 4, and Strategies 2 and 3 are functionally equivalent to Reactor Safety Cornerstones 2 and 3.

The four defense-in-depth strategies are intentionally more focused than the reactor safety cornerstones. The cornerstones also apply to accidents that can not lead to core damage (for example fuel-handling, fuel-storage, and radwaste storage tank rupture accidents). The strategy statements may in the future be modified to address non-core-damage accidents; however, emphasis on core damage accidents is appropriate for the initial efforts to risk-inform existing regulatory requirements.

In describing the cornerstones and strategies, the words “limit,” “prevent,” and “contain” are relative rather than absolute. Cutting a failure rate in half "prevents" half the failures that would otherwise occur in a given time period, and some fixes last for the life of a plant. However, it is not possible to prevent all accident initiators or to eliminate the possibility of core damage or containment failure for all conceivable accidents. All four strategies are applied to compensate for the limitations of the individual strategies; issues related to PRA scope, level of detail, and technical adequacy; and uncertainty, in particular completeness uncertainty.

Other Framework Elements

As indicated in Figure 2.6-8, other elements are applied to support the cornerstones and related strategies. These elements are referred to as tactics to distinguish them from the four defense-in-depth strategies. Existing regulatory requirements apply a wide variety of tactics. Some tactics such as quality assurance are broadly applicable to all four strategies. Safety margin is often applied to provide a high degree of confidence that a design or process will provide a needed function. Other tactics may only be applicable to specific strategies or accident types. The primary responsibility for implementing tactics, whether required by regulations or not, resides with the licensee.

Quantitative Guidelines for the Framework

Quantitative guidelines for the preventive and mitigative defense-in-depth strategies are applied by the NRC staff to assess the effectiveness of existing regulations, to formulate and compare risk-informed options to existing regulatory requirements, and to develop risk-informed alternative regulations. In the context of integrated decisionmaking, the acceptance guidelines should not be interpreted as being overly prescriptive. The quantitative guidelines are not proposed regulatory requirements. They reflect a desired level of safety against which to compare industry-averaged risk measures; a level that is "safe enough" based on the Commission's Safety Goal Policy Statement while providing reasonable balance among the defense-in-depth strategies.

The starting point for developing quantitative guidelines is the Quantitative Health Objectives (QHOs), which were originally set to as a measure of "safe enough."

Unfortunately, the QHOs are difficult to apply in making risk-informed changes to the existing regulations. PRAs often do not proceed to Level 3, that is, to the quantification of public health risks and even if they did, their calculation is dependent upon many factor outside the licensee's control (e.g., weather, topography, and population density).

In addition, simply replacing existing regulations with the QHOs would not be risk-informed. It would not assure reasonably balanced defense-in-depth approach. To illustrate, consider the following example. Even at a densely populated U.S. site, if a plant's core damage frequency is 10^{-4} per year or less, the latent cancer QHO is generally met with no credit taken for containment. The early fatality QHO is more restrictive than the latent cancer QHO. If a plant's large early release frequency is 10^{-5}/yr or less, the early fatality QHO is generally met. Conceivably, both QHOs could be met by reducing a plant's CDF to 10^{-5}/yr or less with no containment and no preplanned offsite protection actions. This would not constitute a risk-informed approach.

What is required for a risk-informed approach are quantitative measures and guidelines that can be used to describe and indicate the effectiveness of the defense-in-depth strategies. The measures and guidelines proposed for this purpose are summarized in Figure 2.6-9.

Two methods of quantitatively assessing the level of protection against accidents at a given nuclear power plant are also depicted in Figure 2.6-9:

- a prevention-mitigation assessment considers the strategies in pairs,
- an initiator-defense assessment considers the strategies individually.

In the context of these two assessment methods, mean risk measures quantified in full-scope, plant-specific PRAs would ideally be compared to the quantitative guidelines. Full scope PRAs address internal and external initiating events as well as accidents initiated in all operating modes. The frequencies in Figure 2.6-9 are, accordingly, stated per calender year rather than per year of reactor operation.

Details regarding the use of Figure 2.6-9 and the Option 3 framework are still being worked out. 10 CFR 44 (hydrogen rule) and10 CFR 50.46 (ECCS Rule) are currently being evaluated by the staff for risk-informed changes. It is unlikely that licensees will see dramatic changes in these and other regulations as a result of the

Option 3 efforts. The treatment of defense-in depth and PRA uncertainties are among the issues leading the staff to move rather slowly in these areas.

PRA quality is another issue that is being debated. While the IPEs and IPEEs appear to have successfully met their intended purpose, they are very uneven in quality and scope. It is extremely unfortunate that the NRC did not provide better guidance to the industry in the 1980s regarding the preparation of the IPEs and IPEEEs so that they would be more useful in the context of risk-informed regulation. Over the next few years many important decisions regarding the implementation of risk-informed regulation are expected and the reader should stay tuned. In any case it is clear that regulatory thought processes within the NRC have profoundly changed over the last ten years.

Table 2.6-1 Thresholds for Performance Bands

Cornerstone	Indicator	Thresholds		
		Increased Regulatory Response Band (green/white)	Required Regulatory Response Band (white/yellow)	Unacceptable Performance Band (yellow/red)
Initiating Events	Unplanned scrams per 7000 critical hours	>3	>6	>25
	Risk-significant scrams per 3 years	>4	>10	>20
	Transients per 7000 critical hours	>8	N/A	N/A
Mitigating Systems	Safety System unavailability			
	HPCI and RCIC	>0.04	>0.12	>0.5
	HPCS	>0.015	>0.04	>0.2
	Emergency Power	>0.025	>0.05*	>0.1**
	RHR	>0.015	>0.05	
	AFW	>0.02	>0.06	>0.12
	HPSI	>0.015	>0.05	
	Safety System Failures previous 4 quarters	>5	N/A	N/A
Barrier Integrity	Reactor Coolant System specific activity	>50% TS limit	>100% TS limit	N/A
	Reactor Coolant System leakage	>50% TS limit	>100% TS limit	N/A
	Containment Leakage	>100% L_A	N/A	N/A
Emergency Preparedness	Emergency Response Organization drill/exercise performance	<75% prior 6 months; or <90% prior 2 years	<55% prior 6 months; or <70% prior 2 years	N/A
	Percentage of Emergency Response Organization shift crews that have participated in a drill or exercise in the past 24 months	<80% prior 2 years: or <70% prior 3 years	<60% prior 2 years: or <70% prior 3 years	N/A
	Percentage of time Alert and Notification System available	<94% per year	<90% per year	N/A

*for plants with more than 2 diesel generators threshold is >0.1

**for plants with more than 2 diesel generators threshold is >0.2

Table 2.6-1 Thresholds for performance bands (cont.)

Cornerstone	Indicator	Thresholds		
Public Radiation Safety	Reportable effluent events	>6 in 3 years or >3 in one year	>13 in 3 years or >7 in 1 year	N/A
Occupation Radiation Safety	Number of non-compliances with 10 CFR 20 requirements for (1) high (>1 rem/hr) and (2) very high radiation areas, and uncontrolled personnel exposures exceeding 10% of the stochastic or 2% of the non-stochastic limits	>5 occurrences in 3 years or >2 occurrences in 1 year	>11 occurrences in 3 years or >5 occurrences in 1 year	N/A
Safeguards	Availability of security equipment	<95% per year	<85% per year	N/A
	Vital Area security equipment availability	<95% per year	<85% per year	N/A
	Personnel screening process performance	>2 reportable events	>6 reportable events	N/A

* for plants with more than 2 diesel generators threshold is >0.1
** for plants with more than 2 diesel generators threshold is >0.2

Table 2.6-2 Inspectible Areas Associated with Each Cornerstone of Reactor Safety

Cornerstone	Inspectible Areas	Type
Initiating Events	Adverse weather preparations	complementary
	Equipment alignment	supplementary
	Emergent work	complementary
	Fire protection	complementary
	Flood protection measures	complementary
	Heat sink performance	complementary
	Identification and resolution of problems	complementary
	In-service inspection activities	complementary
	Maintenance rule implementation	supplementary
	Maintenance work prioritization/control	supplementary
	Non-routine plant evolutions	supplementary
	Piping system erosion and corrosion	complementary
	Refueling and outage activities	complementary
Mitigating Systems	Adverse weather preparations	complementary
	Changes to license conditions and SAR	complementary
	Emergent work	complementary
	Equipment alignment	supplementary
	Fire protection	complementary
	Flood protection measures	complementary
	Heat sink performance	complementary
	Identification and resolution of problems	complementary
	In-service testing of pumps and valves	complementary
	Licensed operator requalification	complementary
	Maintenance rule implementation	supplementary
	Maintenance work prioritization/control	supplementary
	Non-routine plant evolutions	supplementary
	Operability evaluations	complementary
	Operator workloads	complementary
	Permanent plant modification	complementary
	Post maintenance testing	supplementary
	Refueling and outage activities	complementary
	Safety system design and performance	complementary
	Surveillance testing	supplementary
	Temporary plant modifications	complementary

Table 2.6-2 Inspectible Areas Associated with Each Cornerstone of Reactor Safety (Cont.)

Cornerstone	Inspectible Area	Type
Barrier Integrity	Changes to license conditions and SAR	complementary
	Equipment alignment	supplementary
	Fuel barrier performance	verification
	Identification and resolution of problems	complementary
	In-service inspection activities	complementary
	Containment leak rate and isolation valve	verification
	Licensed operator requalification	complementary
	Maintenance rule implementation	supplementary
	Maintenance work prioritization	supplementary
	Non-routine plant evolutions	supplementary
	Permanent plant modifications	complementary
	Refueling and outage activities	complementary
	Surveillance testing	supplementary
	Temporary plant modifications	complementary
Emergency Preparedness	Alert and notification system testing	verification
	Drill and exercise inspection	verification
	Emergency action level changes	complementary
	Emergency response organization testing	complementary
	Training program	verification
	Identification and resolution of problems	complementary
Public Radiation Exposure	Gaseous and liquid effluent treatment systems	supplementary
	Identification and resolution of problems	complementary
	Radioactive material processing and shipping	complementary
	Environmental monitoring program	complementary
Occupational Radiation Exposure	Access control to radiologically significant areas	supplementary
	ALARA planning and controls	complementary
	Identification and resolution of problems	complementary
	Radiation monitoring instrumentation	complementary
	Radiation worker performance	complementary

Table 2.6-2 Inspectible Areas Associated with Each Cornerstone of Reactor Safety (cont.)

Cornerstone	Inspectible Area	Type
Safeguard		
	Access authorization	supplementary
	Access control	complementary
	Changes to license conditions and SAR	complementary
	Identification and resolution of problems	complementary
	Physical protection system	verification
	Response to contingency events	complementary

Table 2.6-3. NRC Action Matrix

RESULTS		Cornerstones fully met; all inputs are green	One or two inputs white in different cornerstones	One degraded cornerstone	Repetitive degraded Cornerstones or Multiple degraded cornerstones	Overall unacceptable performance
RESPONSE	**Regulatory Conference**	Routine Senior Resident Inspector interaction	Branch Chief or Division Director meets with Licensee	Division Director or Regional Administrator Meet with Licensee	EDO or Commission Meet with Senior Licensee Management	Commission meeting with Senior Licensee Management
	Licensee Action	Licensee Corrective Action Program	Licensee Corrective Action Program with NRC Oversight	Licensee Self Assessment with NRC Oversight	Licensee Performance Improvement Plan with NRC Oversight	
	NRC Inspection	Risk Informed Base line Inspection Program	Baseline and Inspection Follow-up	Baseline and inspection focused on cause of degradation	Baseline and Team Inspection focused on cause of degradation	
	Regulatory Action	none	Document response to degrading area in inspection report	Docket response to degrading condition	10CFR2.20404 DFI 10CFR 50.54(f) letter Confirmatory action letter/order	Order to modify, suspend or revoke licensed activities

Table 2.6-3. NRC Action Matrix (Cont.)

COMMUNICATION	**Assessment Report**	Division director reviews and signs assessment report with inspection plan	Division Director review and signs assessment report with inspection plan	Regional Administrator reviews and signs assessment report with inspection plan	Regional Administrator reviews and signs assessment report Commission informed	
	Public Assessment Report	Senior Resident Inspector or Branch Chief meets with licensee	Branch Chief or Division Director meets with licensee	Regional Administrator discusses performance with licensee	Executive Director of Operations or Commission discuss performance with senior licensee management	Commission meeting with senior licensee management

Table 2.6-4 Examples Illustrating the Concept of Maintenance Preventable Functional Failures

Maintenance Preventable Functional Failures:

- Failures due to the implementation of incorrect maintenance procedures
- Failures due to incorrect implementation of correct maintenance procedures
- Failures due to incorrect implementation of maintenance performed with procedures and considered within the skill of the craft
- Failures of the same kind occurring at a utility that have occurred in industry that could have been precluded by an appropriate and timely maintenance activity
- Failures that occur due to the failure to perform maintenance activities that are normal and appropriate to the equipment function and importance such as failure to lubricate with appropriate material or the failure to rotate equipment that is in a standby mode for long periods.

Not Maintenance Preventable Functional Failures:

- Initial failures due to original equipment manufacturer design
- Initial failures due to design inadequacies in selecting or applying commercial or 'off-the-shelf" equipment
- Initial failures due to inherent material defects
- Failures due to operational errors
- Failures due to external events
- Intentional runs to failure
- Recurrence of a failure during post maintenance testing but before returning the system to service.
- Often structures were considered 'inherently safe' and not treated in accordance with the expectations from the Maintenance Rule. Monitoring of structures was criticized as not predictive and not capable of giving early warning of degradation.
- Some licensees were reluctant to categorize structures, systems and components as requirieing the a(1) treatment because of concern that this might imply that their preventative maintenance programs were ineffective.
- Licensees often could not demonstrate performance criteria and goals were commensurate with the safety significance of a structure, system or component.
- Some licensees did not balance reliability and availability for high safety significant structures, systems and components.
- There can be confusion in identifying system failures as preventable by maintenance.

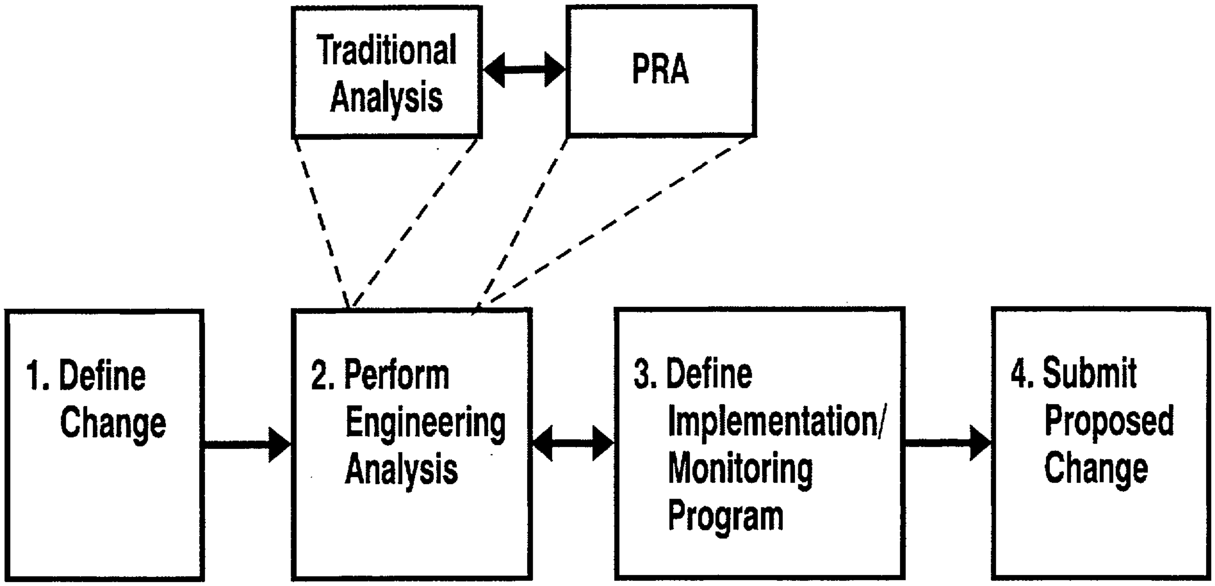

Traditional Analysis
PRA
1. Define Change
2. Perform Engineering Analysis
3. Define Implementation/ Monitoring Program
4. Submit Proposed Change

Figure 2.6-1 Elements of risk-informed process

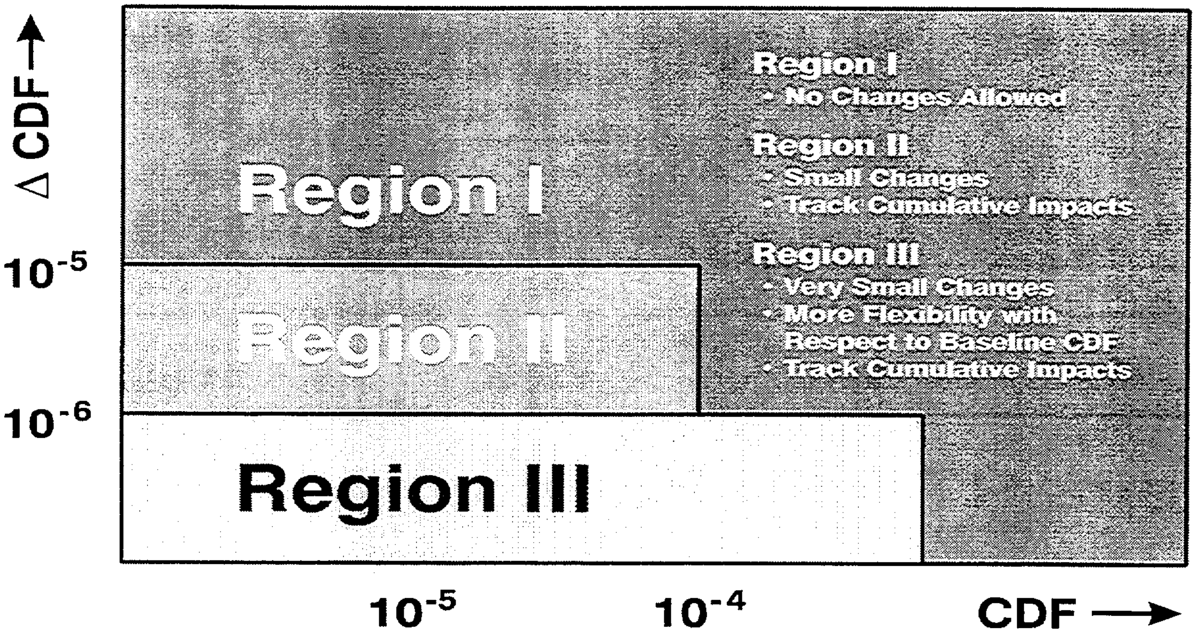


Figure 2.6-2 CDF acceptance guidelines

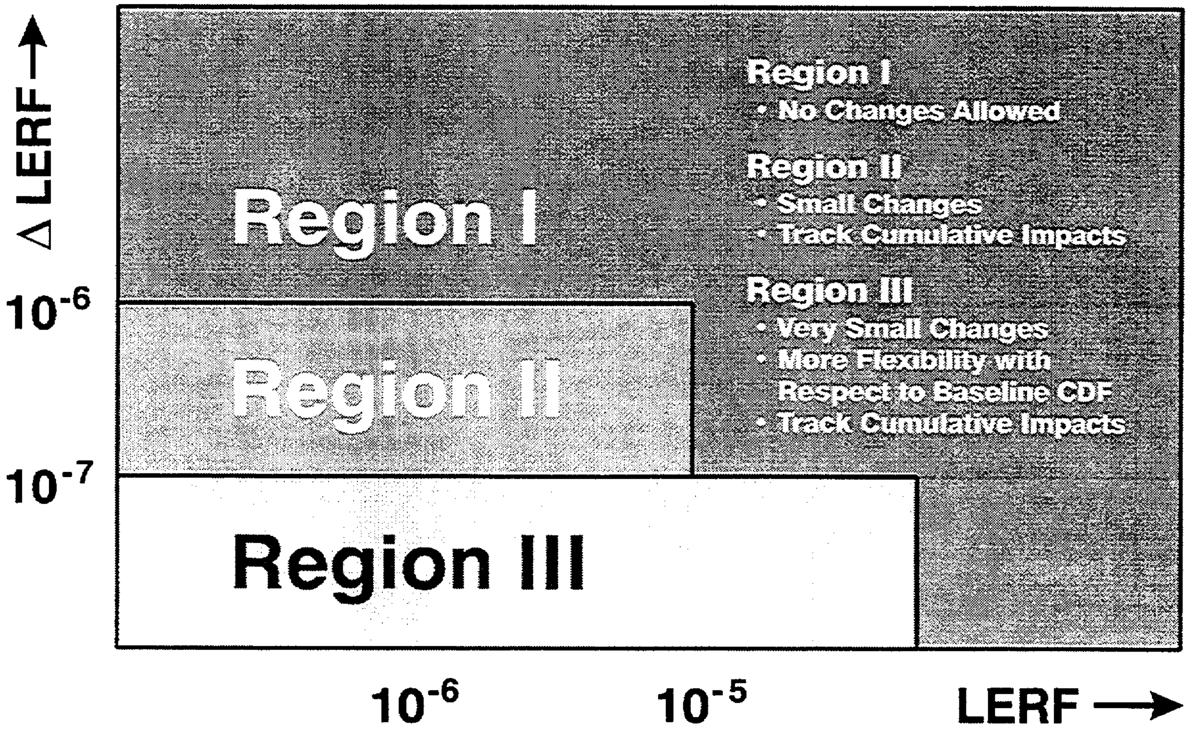


Figure 2.6-3 LERF acceptance guidelines

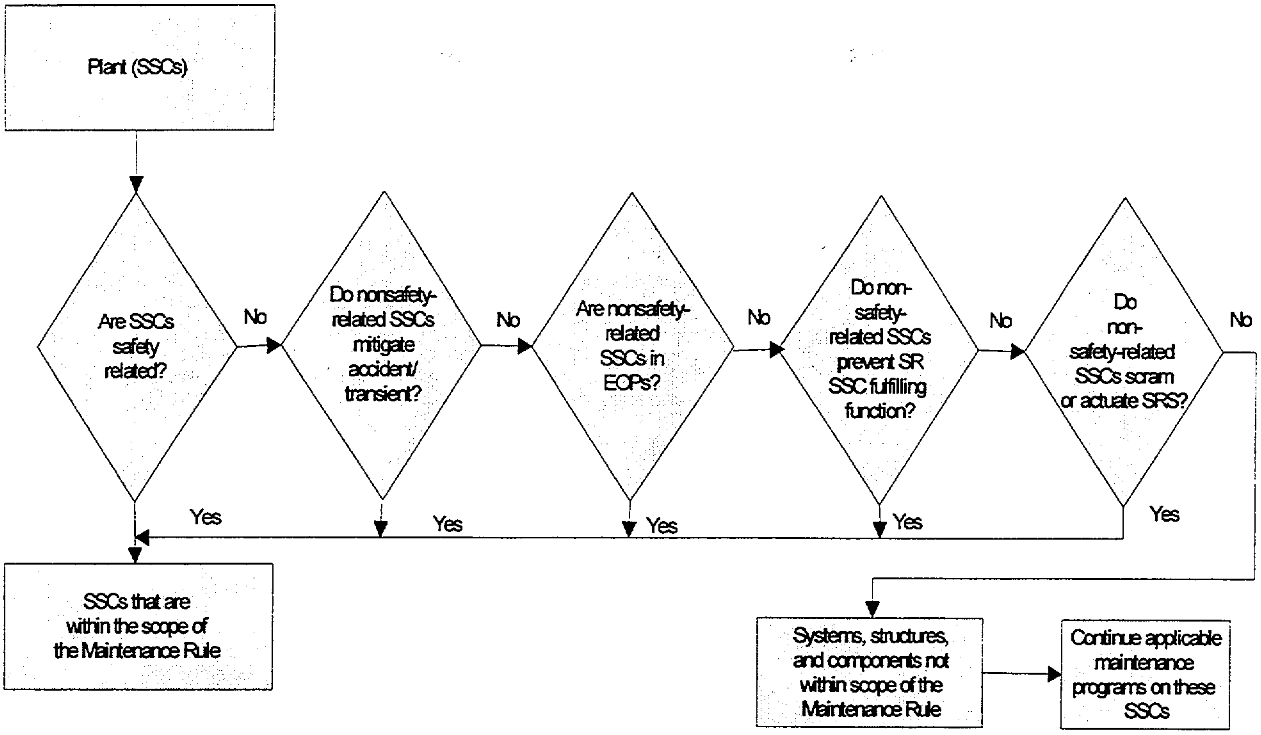

Plant (SSCs)
Are SSCs safety related?
No
Do nonsafety-related SSCs mitigate accident/ transient?
No
Are nonsafety-related SSCs in EOPs?
No
Do non-safety-related SSCs prevent SR SSC fulfilling function?
No
Do non-safety-related SSCs scram or actuate SRS?
No
Yes
Yes
Yes
Yes
Yes
SSCs that are within the scope of the Maintenance Rule
Systems, structures, and components not within scope of the Maintenance Rule
Continue applicable maintenance programs on these SSCs

Figure 2.6-4 Decision tree for the categorization of structures, systems and components for the purposes of the Maintenance Rule.

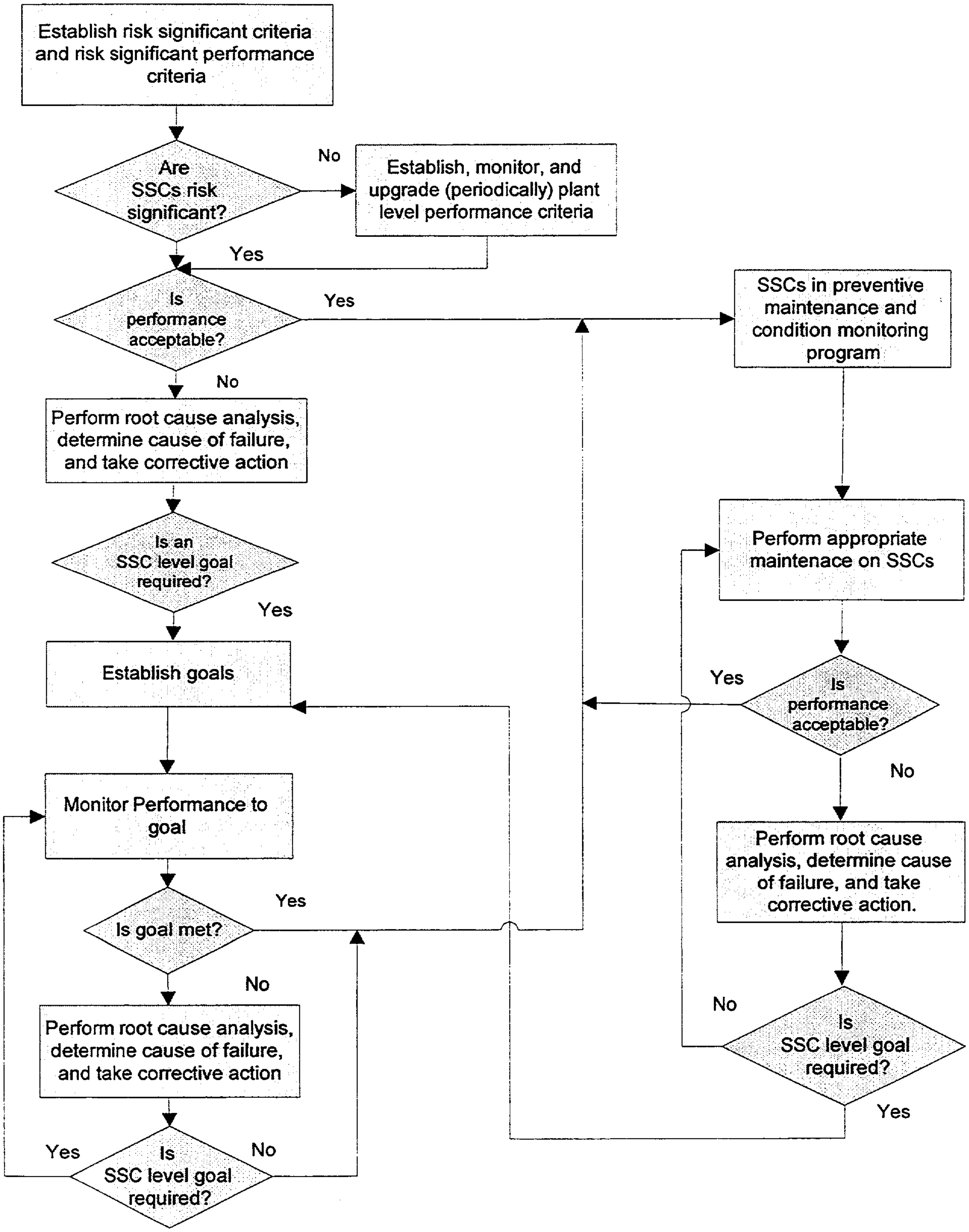

Establish risk significant criteria and risk significant performance criteria
Are SSCs risk significant?
No
Establish, monitor, and upgrade (periodically) plant level performance criteria
Yes
Is performance acceptable?
Yes
SSCs in preventive maintenance and condition monitoring program
No
Perform root cause analysis, determine cause of failure, and take corrective action
Is an SSC level goal required?
Yes
Establish goals
Perform appropriate maintenace on SSCs
Yes
Is performance acceptable?
No
Monitor Performance to goal
Perform root cause analysis, determine cause of failure, and take corrective action.
Yes
Is goal met?
No
Perform root cause analysis, determine cause of failure, and take corrective action
No
Is SSC level goal required?
Yes
Yes
Is SSC level goal required?
No

Figure 2.6-5 Decision tree for the categorization of structures, systems and components for the purposes of the Maintenance Rule

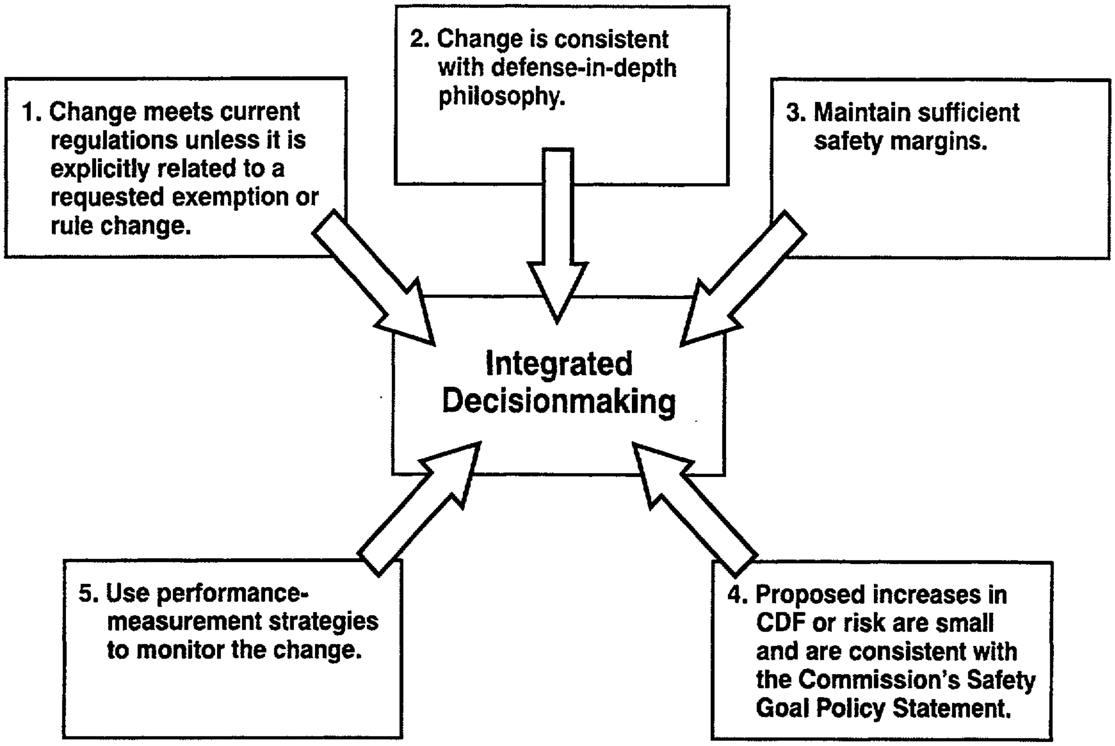
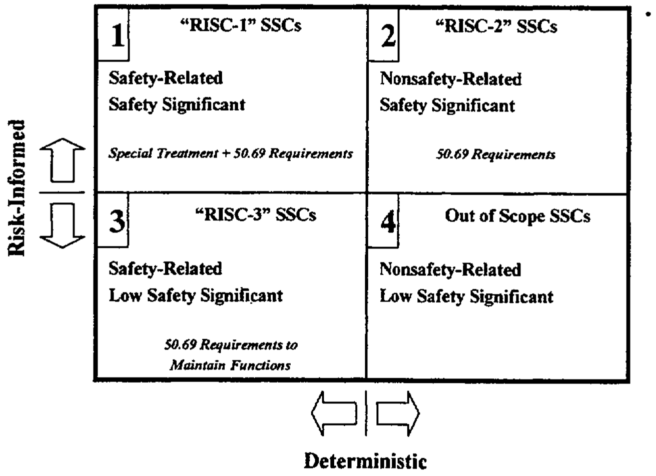

1. Change meets current regulations unless it is explicitly related to a requested exemption or rule change.
2. Change is consistent with defense-in-depth philosophy.
3. Maintain sufficient safety margins.
Integrated Decisionmaking
5. Use performance-measurement strategies to monitor the change.
4. Proposed increases in CDF or risk are small and are consistent with the Commission's Safety Goal Policy Statement.

Figure 2.6-6 Integrated decision process for risk-informed regulation



1 "RISC-1" SSCs Safety-Related Safety Significant *Special Treatment + 50.69 Requirements*	2 "RISC-2" SSCs Nonsafety-Related Safety Significant *50.69 Requirements*
3 "RISC-3" SSCs Safety-Related Low Safety Significant *50.69 Requirements to Maintain Functions*	4 Out of Scope SSCs Nonsafety-Related Low Safety Significant

Figure 2.6-7. Diagram of Categorization and Treatment

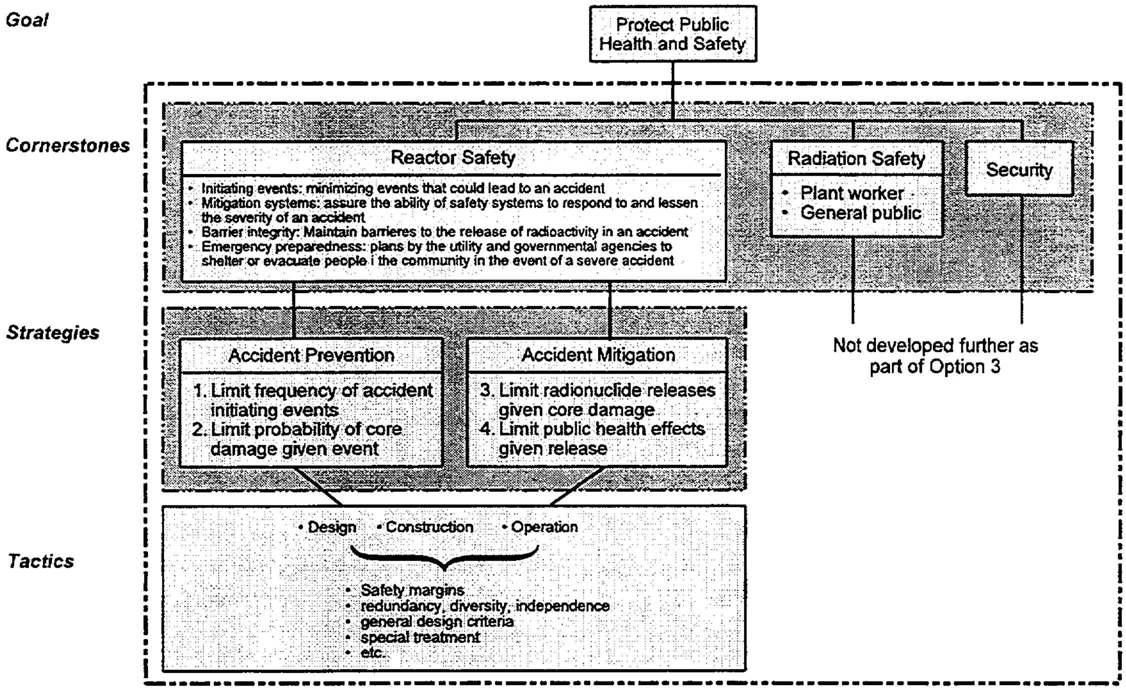

Goal
Protect Public Health and Safety
Cornerstones
Reactor Safety
• Initiating events: minimizing events that could lead to an accident
• Mitigation systems: assure the ability of safety systems to respond to and lessen the severity of an accident
• Barrier integrity: Maintain barrieres to the release of radioactivity in an accident
• Emergency preparedness: plans by the utility and governmental agencies to shelter or evacuate people i the community in the event of a severe accident
Radiation Safety
• Plant worker
• General public
Security
Strategies
Accident Prevention
1. Limit frequency of accident initiating events
2. Limit probability of core damage given event
Accident Mitigation
3. Limit radionuclide releases given core damage
4. Limit public health effects given release
Not developed further as part of Option 3
Tactics
• Design • Construction • Operation
• Safety margins
• redundancy, diversity, independence
• general design criteria
• special treatment
• etc.

Figure 2.6-8 Elements of risk-informed framework

	Accident Prevention		**Accident Mitigation**	
	Core Damage Frequency **≤10^{-4}/year**		**Conditional Large Early Release Probability** **≤10^{-1}** (Note 5)	
	Limit frequency of accident initiating events	Limit probability of core damage given event	Limit radionuclide releases given core damage	Limit public health effects given release
	Initiator Frequency	Conditional core damage probability	Conditional large early release probability	Conditional individual fatality probability
Frequent initiators	≥1/year	≤10-4	≤10-1	Note 3
Infrequent initiators	≤10-2/year	≤10-2	≤10-1	Note 3
Rare initiators	≤10-5/year	Note 4	Note 4	Note 3

Notes:
1. The product across each row gives a large early release frequency of <10^{-5}/year.
2. It is preferable that no single type of initiator cause a large fraction of any frequency guideline.
3. No quantitative guideline is proposed for the fourth strategy, the LERF guideline is used as a surrogate.
4. For rare initiators, emphasis is placed on Strategy 1, limit initiator frequency.
5. Measures to mitigate late large releases are also appropriate. A conditional probability of a late large release (up to 24 hours after the onset of core damage) of ≤10^{-1} is proposed.

Figure 2.6-9 Quantitative guidelines for risk-informed framework

References for Section 2.6

1. U.S. Nuclear Regulatory Commission, PRA Working Group, "A Review of NRC Staff Uses of Probabilistic Risk Assessment, "NUREG-1489, March 1994.

2. U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement,"*Federal Register*, 60FR42622, August 16, 1995.

3. U.S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174.

4. USNRC, Statement of Considerations, "Technical Specifications for Facility Licensees; Safety Analysis Reports," *Federal Register*, 33 FR 18612, December 17, 1968.

5. USNRC, "Final Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors," Federal Register, 58 FR 39132, July 22, 1993.

6. USNRC, 10 CFR 50.36, "Technical Specifications," *Federal Register*, 60 FR 36953, July 19, 1995.

7. Letter from William D. Travers, Executive Director for Operations, to The Commissioners, dated September 14, 2000.

8. ASME Boiler and Pressure Vessel Code: An International Code, Section XI, "Rules for Inservice Inspection of Nuclear Power Plant Components", 2001 Edition, New York, NY, July 1, 2001.

9. USNRC, "An Approach for Plant-Specific Risk-Informed Decisionmaking: Inservice Testing," Regulatory Guide 1.175, 1998.

Appendix 2A Davis-Besse Loss Of Feedwater

The one-unit Davis-Besse nuclear power plant is located in Oak Harbor, Ohio. The plant is operated by the First Energy Nuclear Operating Co.. The plant consists of one Babcock & Wilcox PWR designed for a maximum operational power of 874 MWe. The Davis-Besse plant has been in operation since July 1978. Key systems of the Davis-Besse plant are depicted in Figures 2A-1 through 2A-6.

The following sections describe a loss-of-feedwater incident that occurred at the Davis-Besse plant. In view of the importance of the operator actions in this event, the description is a narrative based upon a composite of the operator interviews performed by an NRC review team following the incident (NUREG-1154),. The review team decided that this would best convey the effects of stress, training, experience, teamwork, and impediments on operator performance.

The following text is extracted directly from NUREG-1154.

2A.1 Initiating Events

On June 9, 1985, the midnight shift of operators assumed control of the Davis-Besse nuclear power plant. The oncoming shift included four licensed operators, four equipment operators, an auxiliary operator, and an administrative assistant. The shift supervisor and the assistant shift supervisor are licensed senior reactor operators and the most experienced members of the operating crew. Both were at the plant before it was issued an operating license in April 1977. The reactor operators, who were responsible for the control room, had decided between themselves who would be responsible for the primary-side and who would take the secondary-side work stations. The secondary-side operator had been a licensed reactor operator for about two years. The primary-side operator was licensed in January 1985; he had previous nuclear Navy experience and was an equipment operator before being licensed. Prior to the morning of June 9, neither reactor operator had been at the controls during a reactor trip at Davis-Besse.

The four equipment operators are a close-knit group, three of whom had been operators in the nuclear Navy. Their experience at the plant ranges from three to nine years, averaging six-and-one-half years per operator. Equipment operators receive directions from the control room operators to manipulate and troubleshoot equipment in the reactor auxiliary building and the turbine building. Generally, equipment operators occupy this position temporarily as they participate in a development program leading to the position of licensed operator. However, two equipment operators did not intend to become licensed operators.

The shift turnover of June 9 was easy; there were no ongoing tests or planned changes to plant status. The plant was operating at 90% of the full power authorized in the license granted by the NRC in April 1977, to minimize the potential for an inadvertent reactor trip due to noise on primary coolant flow instrumentation. All the major equipment control stations were running on automatic except the No. 2 main feedwater pump. As a result, the integrated control system instruments were monitoring and controlling the balance between the plant's reactor coolant system and the secondary coolant system.

Since April 1985, there had been control problems with both main feedwater pumps. Troubleshooting had not identified or resolved the problems. In fact, a week earlier, on June 2, 1985, both feedwater pumps tripped unexpectedly after a reactor trip. After some additional troubleshooting, the decision was made to not delay startup any longer, but to put instrumentation on the pumps to help diagnose the cause of a pump trip, if it occurred again. As a precaution, the number two main feedwater pump was operating in manual control to prevent it from tripping and to ensure that all main feedwater would not be lost should the reactor trip. Some operators were uneasy about going up to power with problems in the feedwater pumps, but they complied with the decisions made by their management.

During the first hour of the shift, the operators' attention and thoughts were directed to examining the control panels and alarm panels, and performing instrument checks and routine surveillance associated with shift turnover. Thus, at 1:35 in the morning, the plant generator was providing electricity to the Ohio countryside. The secondary-side operator had gone to the kitchen where he joined an equipment operator for a snack. The other reactor operator was at the operator's desk studying procedures for requalification examinations. The assistant shift supervisor had just left the kitchen on his way back to the control room after a break. The shift supervisor was in his office outside the control room performing administrative duties.

2A.2 Reactor Trip - Turbine Trip

The assistant shift supervisor entered the control room and was examining one of the consoles when he noticed that main feedwater flow was decreasing and that the No. 1 main feedwater pump had tripped. Since the No. 2 feedwater pump was in manual control, it could not respond to the integrated control system demand automatically to increase feedwater flow.

The "winding down" sound of the feedwater pump turbine was heard by the reactor operator in the kitchen, and by the administrative assistant and the shift supervisor, both of whom were in their respective offices immediately outside the control room. They headed immediately for the control room -- the event had begun.

The secondary-side reactor operator ran to his station and immediately increased the speed of the No. 2 main feedwater pump to compensate for the decrease of feedwater flow from the No. 1 pump. The primary-side operator had already opened the pressurizer spray valve in an attempt to reduce the pressure surge resulting from the heatup of the reactor coolant system due to a decrease in feedwater flow.

The plant's integrated control system attempted automatically to reduce reactor/turbine power in accordance with the reduced feedwater flow. The control rods were being inserted into the core and reactor power had been reduced to about 80%. At the same time the primary-side reactor operator held open the pressurizer spray valve in an attempt to keep the reactor coolant pressure below the high pressure reactor trip set point of 2300 psig (normal pressure is 2150 psig). However, the reduction of feedwater and subsequent degradation of heat removal from the primary coolant system caused the reactor to trip on high reactor coolant pressure. The operators had done all they could do to prevent the trip, but the safety systems had acted automatically to shut down the nuclear reaction.

The primary-side operator acted in accordance with the immediate post-trip actions specified in the emergency procedure that he had memorized. Among other things, he checked that all control rod bottom lights were on, hit the reactor trip (shutdown) button, isolated letdown from the reactor coolant system, and started a second makeup pump to anticipate a reduced pressurizer inventory after a normal reactor trip. Then he waited, and watched the reactor coolant pressure to see how it behaved.

The secondary-side operator heard the turbine stop valves slamming shut and knew the reactor had tripped. This "thud" was heard by most of the equipment operators who also recognized its meaning and two of them headed for the control room. Almost simultaneously, the secondary-side operator heard the loud roar of main steam safety valves opening, a sound providing further proof that the reactor had tripped. The lifting of safety valves after a high-power reactor trip was normal. Everything was going as expected as he waited and watched the steam generator water levels boil down -each should reach the normal post-trip low level limit of 35 inches on the startup level instrumentation and hold steady.

The shift supervisor joined the operator at the secondary-side control console and watched the rapid decrease of the steam generator levels. The rapid feedwater reduction system (a subsystem of the integrated control system) had closed the startup feedwater valves, but as the level approached the low level limits, the startup valves opened to hold the level steady. The main steam safety valves closed as expected. The system response was looking "real good" to the shift supervisor.

The assistant shift supervisor in the meantime opened the plant's looseleaf emergency procedure book. (It is about two inches thick, with tabs for quick reference. The operators refer to it as emergency procedure 1202:01; the NRC refers to it as the ATOG procedure -Abnormal Transient Operating Guidelines) As he read aloud the immediate actions specified, the reactor operators were responding in the affirmative. After phoning the shift technical advisor (STA) to come to the control room, the administrative assistant began writing down what the operators were saying, although they were speaking faster than she could write.

The STA was working a 24-hour shift and was asleep when awakened by a telephone call from the shift supervisor, which was followed immediately by the call from the administrative assistant. (The STAs are provided an apartment-type room in the administrative building, which is outside the protected area about one-half mile from the plant. According to procedures, they must be able to get to the control room within 10 minutes of being called.) He had detected a sense of urgency in the telephone calls and so he ran out of the building to his car for the drive to the site. He was anxious himself -- this was his first reactor trip since becoming a shift technical advisor in January 1985.

2A.3 Loss of Main Feedwater

Although the assistant shift supervisor was loudly reading the supplementary actions from the emergency procedure book, the shift supervisor heard the main steam safety valves open again. He knew from experience that something was unusual and instinctively surveyed the control console and panel for a clue. He discovered that both main steam isolation valves (MSIVs) had closed -- the first and second of a list of unexpected equipment performances and failures that occurred during the event.

The secondary-side operator was also aware that something was wrong because he noticed that the speed of the only operating main feedwater pump was decreasing. After verifying that the status of the main feedwater pump turbine was normal, he concluded that the turbine was losing steam pressure at about the same time that the shift supervisor shouted that the MSIVs were closed. All eyes then turned up to the annunciators at the top of the back panel. They saw nothing abnormal in the kind or number of annunciators lit after the reactor trip. The operators expected to find an alarm indicating that the Steam Feedwater Rupture Control System (SFRCS, pronounced S-FARSE) had activated. Based on their knowledge of previous events at the plant, they believed that either a partial or full actuation of the SFRCS had closed the MSIVs. However, the SFRCS annunciator lights were dark. The MSIVs had closed at 1:36 a.m. and they were going to stay closed. It normally takes at least one-half hour to prepare the steam system for reopening the valves.

The No. 2 main feedwater pump turbine, deprived of steam, was slowly winding down. Since the MSIVs were closed and there was limited steam inventory in the moisture separator reheaters, there was inadequate motive power to pump feedwater to the steam generators. At about 1:40 a.m., the discharge pressure of the pump had dropped below the steam pressure which terminated main feedwater flow.

2A.4 Loss of Emergency Feedwater

The secondary-side operator watched the levels in both steam generators boil down; he had also heard the main steam safety valves lifting. Without feedwater, he knew that an SFRCS actuation on low steam generator level was imminent. The SFRCS should actuate the auxiliary feedwater system (AFWS) which in turn should provide emergency feedwater to the steam generators. He was trained to trip manually any system that he felt was going to trip automatically. He requested and received permission from the shift supervisor to trip the SFRCS on low level to conserve steam generator inventory, i.e., the AFWS would be initiated before the steam generator low-level setpoint was reached.

He went to the manual initiation switches at the back panel and pushed two buttons to trip the SFRCS. He inadvertently pushed the wrong two buttons and, as a result, both steam generators were isolated from the emergency feedwater supply. He had activated the SFRCS on low pressure for each steam generator instead of on low level. By manually actuating the SFRCS on low pressure, the SFRCS was signaled that both generators had experienced a steamline break or leak and the system responded, as designed, to isolate both steam generators. The operator's anticipatory action defeated the safety function of the auxiliary feedwater system -- a common-mode failure and the third abnormality to occur within 6 minutes after the reactor trip.

The operator returned to the auxiliary feedwater station expecting the AFWS to actuate and provide the much-needed feedwater to the steam generators that were boiling dry. Instead, he first saw the No. 1 AFW pump, followed by the No. 2 AFW pump trip on overspeed –a second common-mode failure of the auxiliary feedwater system and abnormalities four and five. He returned to the SFRCS panel to find that he had pushed the wrong two buttons.

The operator knew what he was supposed to do. In fact, most knowledgeable people in the nuclear power industry, even control room designers, know that the once-through steam generators in Babcock & Wilcox-designed plants can boil dry in as little as 5 minutes; consequently, it is vital for an operator to be able to quickly start the AFWS. There could have been a button labeled simply "AFWS--Push to start." But instead, the operator had to do a mental exercise to first identify a signal in the SFRCS that could indirectly start the AFW system, find the correct set of buttons from a selection of five identical sets located knee-high from the floor on the back panel, and then push them without being distracted by the numerous alarms and loud exchanges of information between operators.

The shift supervisor quickly determined that the valves in the AFWS were improperly aligned. He reset the SFRCS, tripped it on low level, and corrected the operator's error about one minute after it occurred. This action commanded the SFRCS to realign itself such that each AFW pump delivered flow to its associated steam generator. Thus, had both systems (the AFWS and SFRCS) operated properly, the operator's mistake would have had no significant consequences on plant safety.

The assistant shift supervisor, meanwhile, continued reading aloud from the emergency procedure. He had reached the point in the supplementary actions that require verification that feedwater flow was available. However, there was no feedwater, not even from the AFWS, a safety system designed to provide feedwater in the situation that existed. (The Davis-Besse emergency plan identifies such a situation as a Site Area Emergency.) Given this condition, the procedure directs the operator to the section entitled, "Lack of Heat Transfer." He opened the procedure at the tab corresponding to this condition, but left the desk and the procedure at this point to diagnose why the AFWS had failed. He performed a valve alignment verification and found that the isolation valve in each AFW train had closed. Both valves (AF-599 and AF-608) had failed to reopen automatically after the shift supervisor had reset the SFRCS. He tried unsuccessfully to open the valves by pressing the buttons on the back panel. He went to the SFRCS cabinets in the back of the control panel to clear any trips in the system and block them so that the isolation valves could open. However, there were no signals keeping the valves closed. He concluded that the torque switches in the valve operators must have tripped. The AFW system had now suffered its third common-mode failure, thus increasing the number of malfunctions to seven within 7 minutes after the reactor trip (1:42 a.m.).

2A.5 Reactor Coolant System Heatup

Meanwhile, about 1:40 a.m., the levels in both steam generators began to decrease below the normal post-reactor-trip limits (about 35 inches on the startup range). The feedwater flow provided by the No. 1 main feedwater pump had terminated. The flow from the No. 2 main feedwater pump was decreasing because the MSIVs were closed, which isolated the main steam supply to the pump. With decreasing feedwater flow, the effectiveness of the steam generators as a heat sink for removing decay (i.e., residual) heat from the reactor coolant system rapidly decreased. As the levels boiled down through the low level setpoints (the auxiliary feedwater should automatically initiate at about 27 inches), the average temperature of the reactor coolant system began to increase, indicating a lack of heat transfer from the primary to the secondary coolant systems.

When the operator incorrectly initiated SFRCS on low pressure, all feedwater was isolated to both steam generators. The reactor coolant system began to heat up because heat transfer to the steam generators was essentially lost due to loss of steam generator water level.

The average reactor coolant temperature increased at the rate of about 4°F/minute for about 12 minutes. The system pressure also increased steadily until the operator fully opened the pressurizer spray valve (at about 1:42 a.m.). The spray reduced the steam volume in the pressurizer and temporarily interrupted the pressure increase. The pressurizer level increased rapidly but the pressurizer did not completely fill with water. As the indicated level exceeded the normal value of 200 inches, the control valve for makeup flow automatically closed.

At this point, things in the control room were hectic. The plant had lost all feedwater; reactor pressure and temperature were increasing; and a number of unexpected equipment problems had occurred. The seriousness of the situation was fully appreciated.

2A.6 Operator Actions

By 1:44 a.m., the licensed operators had exhausted every option available in the control room to restore feedwater to the steam generators. The main feedwater pumps no longer had a steam supply. Even if the MSIVs could be opened, the steam generators had essentially boiled dry, and sufficient steam for the main feedwater pump turbines would likely not have been available. The turbines for the AFW pumps had tripped on overspeed, and the trip throttle valves could not be reset from the control room. Even if the AFW pumps had been operable, the isolation valves between the pumps and steam generators could not be opened from the control room, which also inhibited the AFWS from performing its safety function. The likelihood of providing emergency feedwater was not certain, even if the AFW pump overspeed trips could be reset and the flow path established. For example there was a question as to whether there was enough steam remaining in the steam generators to start the steam driven pumps. Unknown to the operators, the steam inventory was further decreased because of problems controlling main steam pressure. The number of malfunctions had now reached eight.

Three equipment operators had been in the control room since shortly after the reactor tripped. They had come to the control room to receive directions and to assist the licensed operators as necessary. They were on the sidelines watching their fellow operators trying to gain control of the situation.

The safety-related AFW equipment needed to restore water to the steam generators had failed in a manner that could only be remedied at the equipment location and not from the control room. The affected pumps and valves are located in locked compartments deep in the plant.

The primary-side reactor operator directed two of the equipment operators to go to the auxiliary feedwater pump room to determine what was wrong -- and to hurry.

The pump room, located three levels below the control room, has only one entrance: a sliding grate hatch that is locked with a safety padlock. One of the operators carried the key ring with the padlock key in his hand as they left the control room. They violated the company's "no running" policy as they raced down the stairs. The first operator was about 10 feet ahead of the other operator who tossed him the keys so as not to delay unlocking the auxiliary feedwater pump room. The operator ran as fast as he could and had unlocked the padlock by the time the other operator arrived to help slide the hatch open.

The operators descended the steep stairs resembling a ladder into the No. 2 AFW pump room. They recognized immediately that the trip throttle valve had tripped. One operator started to remove the lock wire on the handwheel while the other operator opened the water-tight door to the No. 1 AFW pump. He also found the trip throttle valve tripped and began to remove the lock wire from the handwheel.

The shift supervisor had just dispatched a third equipment operator to open AFW isolation valves AF-599 and AF-608. These are chained and locked valves, and the shift supervisor gave the lock-valve key to the operator before he left the control room. He paged a fourth equipment operator over the plant communications systems and directed him also to open valves AF-599 and AF-608. Although the operators had to go to different rooms for each valve, they opened both valves in about 3 1/2 minutes. They were then directed to the AFW pump room.

As operators ran to the equipment, a variety of troubling thoughts ran through their minds. One operator was uncertain if he would be able to carry out the task that he had been directed to do. He knew that the valves he had to open were locked valves, and they could not be operated manually without a key. He did not have a key and that concerned him. As he moved through the turbine building, he knew there were numerous locked doors that he would have to go through to reach the valves. He had a plastic card to get through the card readers, but they had been known to break and fail. He did not have a set of door keys and he would not gain access if his key card broke and that concerned him too.

The assistant shift supervisor came back into the control console area after having cleared the logic for the SFRCS and he tried again, unsuccessfully, to open the AFWS isolation valves. At this point, the assistant shift supervisor made the important decision to attempt to place the startup feedwater pump (SUFP) in service to supply feedwater to the steam generators. He went to the key locker for the key required to perform one of the five operations required to get the pump running.

The SUFP is a motor-driven pump, usually more reliable than a turbine-driven pump, and more importantly, it does not require steam from the steam generators to operate. The SUFP is located in the same compartment as the No. 2 AFW pump. But since the refueling outage in January 1985, the SUFP had been isolated by closing four manual valves and its fuses were removed from the motor control circuit. This isolation was believed necessary because of the consequences of a high energy break of the non-seismic grade piping which passes through the two seismic-qualified AFW pump rooms. Prior to January 1985, the SUFP could be initiated from the control room by the operation of a single switch.

The assistant shift supervisor headed for the turbine building where he opened the four valves and placed fuses in the pump electrical switchgear. This equipment is located at four different places; in fact, other operators had walked through the procedure of placing the SUFP in operation and required 15 to 20 minutes to do it. The assistant shift supervisor took about 4 minutes to perform these activities. He then paged the control room form the AFW pump room and instructed the secondary-side operator to start the pump and align it with the No. 1 steam generator.

The two equipment operators in the AFW pump rooms had been working about 5 minutes to reset the trip throttle valves when the assistant shift supervisor entered the room to check the SUFP. The equipment operators thought that they had latched and opened the valves. However, neither operator was initially successful in getting the pumps operational. Finally, after one equipment operator had tried everything that he knew to get the No. 1 AFW pump operating, he left it and went to the No. 2 AFW pump where the other operator was having the same problem of getting steam to the turbine. Neither operator had previously performed the task that he was attempting.

The assistant shift supervisor went over to assist the equipment operators and noticed immediately that the trip throttle valves were still closed. Apparently, the equipment operators had only removed the slack in attempting to open the valve. The valve was still closed and the differential pressure on the wedge disk made it difficult to turn the handwheel after the slack was removed, thus necessitating the use of the valve wrench. A third, more experienced operator had entered the pump room and used a valve wrench to open the trip throttle valve on AFW pump No. 2. Without the benefit of such assistance the equipment operators may well have failed to open the trip throttle valves to admit steam to the pump turbines.

The third equipment operator then proceeded to the No. 1 AFW pump trip throttle valve. The valve had not been reset properly and he experienced great difficulty in relatching and opening it because he had to hold the trip mechanism in the latched position and open the valve with the valve wrench. Because the trip mechanism was not reset properly, the valve shut twice before he finally opened the valve and got the pump operating.

2A.7 PORV Failure

Prior to being informed by the assistant shift supervisor that the SUFP was available, the secondary-side operator requested the primary-side operator to reset the isolation signal to the startup feedwater valves in preparation for starting the SUFP. In order to perform this task, the operator left the control console and went to the SFRCS cabinets in back of the control room. As he re-entered the control panel area, he was requested to reset the atmospheric vent valves. As a result of these activities the primary side operator estimated that he was away from his station for 20 to 30 seconds. (In fact, he was away for about two minutes.)

While the operator was away from the primary-side control station, the pressurizer PORV opened and closed twice without his knowledge. The pressure had increased because of the continued heatup of the reactor coolant system that resulted when both steam generators had essentially boiled dry.

According to the emergency procedure, a steam generator is considered "dry" when its pressure falls below 960 psig and is decreasing, or when its level is below 8 inches on the startup range (normal post-trip pressure is 1010 psig and post-trip level is 35 inches). The instrumentation in the control room is inadequate for the operator to determine with certainty if these conditions exist in a steam generator. The lack of a trend recorder for steam generator pressure makes it difficult to determine if the steam pressure is 960 psig and decreasing. The range of the steam generator level indicator in the control room is 0-250 inches, a scale which makes determining the 8-inch level difficult. The safety parameter display system (SPDS) was intended to provide the operators with these critical data, but both channels of the SPDS were inoperable prior to and during this event. Thus, the operators did not know that the conditions in the steam generators beginning at about 1:47 a.m. were indicative of a "dry" steam generator, or subsequently, that both steam generators were essentially dry.

When both steam generators are dry, the procedure requires the initiation of make-up/high pressure injection (MU/HPI) cooling, or what is called the "feed-and-bleed" method for decay heat removal. Even before conditions in the steam generators met these criteria, the shift supervisor was fully aware that MU/HPI cooling might be necessary. When the hot-leg temperature reached 591°F (normal post-trip temperature is about 550°F), the secondary-side operator recommended to the shift supervisor that MU/HPI cooling be initiated. At about the same time, the operations superintendent told the shift supervisor in a telephone discussion that if an auxiliary feedwater pump was not providing cooling to one steam generator within one minute, to prepare for MU/HPI cooling. However, the shift supervisor did not initiate MU/HPI cooling. He waited for the equipment operators to recover the auxiliary feedwater system.

The shift supervisor appreciated the economic consequences of initiating MU/HPI cooling. One operator described it as a drastic action. During MU/HPI, the PORV and the high point vents on the reactor coolant system are locked open, which breaches one of the plant's radiological barriers. Consequently, radioactive reactor coolant is released inside the containment building. The plant would have to be shut down for days for cleanup even if MU/HPI cooling was successful. In addition, achieving cold shutdown could be delayed. Despite his delay, the shift supervisor acknowledged having confidence in this mode of core cooling based on his simulator training; he would have initiated MU/HPI cooling if "it comes to that."

The primary-side operator returned to his station and began monitoring the pressure in the pressurizer, which was near the PORV set point of 2425 psig. The PORV then opened and he watched the pressure decrease. The indicator in front of him signaled that there was a closed signal to the PORV and that it should be closed. The acoustic monitor installed after the TMI accident was available to him to verify that the PORV was closed, but he did not look at it. Instead, he looked at the indicated pressurizer level, which appeared steady, and based on simulator training, he concluded that the PORV was closed. In fact, the PORV had not completely closed and, as a result, the pressure decreased at a rapid rate for about 30 seconds.

The operator did not know that the PORV had failed. He believed the RCS depressurization was due either to the fully open pressurizer spray valve or to the feedwater flow to the steam generators. He closed the spray valve and the PORV block valve as precautionary measures. But subsequent analyses showed that the failed PORV was responsible for the rapid RCS depressurization. Two minutes later, the reactor operator opened the PORV block valve to ensure that the PORV was available. Fortunately, the PORV had closed by itself during the time the block valve was closed. The failed PORV was the ninth abnormality that had occurred within 15 minutes after reactor trip.

2A.8 Steam Generator Refill

At about 1:50 a.m. the No. 1 atmospheric vent valve opened and depressurized the No. 1 steam generator to about 750 psig when the SFRCS signal was reset by the primary-side operator. The vent valve for the No. 2 steam generator had been closed by the secondary-side operator before the SFRCS signal was reset. The indicated No. 1 steam generator level was less than 8 inches. The corresponding pressure and indicated level in No. 2 steam generator were about 928 psig and 10 inches, respectively. The indicated levels continued to decrease until the secondary-side operator started the SUFP after being informed by the assistant shift supervisor that it was available and after the other operator had reset the isolation signal to startup feedwater valves.

Although the flow capacity of the SUFP is somewhat greater, approximately 150 gallons per minute were fed to the steam generators because the startup valves were not fully opened. Essentially all the feedwater from the SUFP was directed to the No. 1 steam generator. At about 1:52 a.m., the pressure in the No. 1 steam generator increased sharply while the indicated water level stopped decreasing and began slowly to increase. Since there was little feedwater sent to the No. 2 steam generator, its condition did not change significantly.

The trip throttle valve for No. 2 AFW pump was opened by the equipment operators at about 1:53 a.m. After the SFRCS was reset and tripped on low level by the shift supervisor, the AFWS aligned itself so that each AFW pump would feed only its associated steam generator, i.e., the No. 2 AFW pump would feed the No. 2 steam generator. Thus, the No. 2 AFW pump refilled the No. 2 steam generator and its pressure increased abruptly to the atmospheric vent valve relief set point. The turbine governor valve was fully open when the trip throttle valve was opened and the pump delivered full flow for about 30 seconds until the operator throttled the flow down.

The No. 1 trip throttle valve was opened by the equipment operator about 1:55 a.m. and feedwater from the AFWS flowed to the No. 1 steam generator. However, the No. 1 AFW pump was not controlled from the control room but controlled locally by the equipment operators.

The equipment operators controlled the pump locally using the trip throttle valve. One operator manipulated the valve based on hand signals from the operator who was outside the No. 1 AFW pump room communicating with the control room operator. For two hours the AFW pump was controlled in this manner by the operators. Their task was made more difficult from the time they first entered the AFW pump room by the intermittent failures of the plant communication station in the room.

With feedwater flow to the steam generators, the heatup of the reactor coolant system ended. At about 1:53 a.m. the average reactor coolant temperature peaked at about 592oF and then decreased sharply to 540°F in approximately 6 minutes (normal post-trip average temperature is 550°F). Thus, the reactor coolant system experienced an overcooling transient caused by an excessive AFW flow from the condensate storage tank. The overfill of the steam generators caused the reactor coolant system pressure to decrease towards the safety features actuation system (SFAS) setpoint of 1650 psig. To compensate for the pressure decrease, and to avoid an automatic SFAS actuation, at approximately 1:58 a.m., the primary-side operator aligned one train of the emergency core cooling system (ECCS) in the piggyback configuration. In this configuration the discharge of the low pressure injection pump is aligned to the suction of the high pressure injection pump to increase its shutoff head pressure to about 1830 psig. At about the time the train was actuated, the combination of pressurizer heaters, makeup flow, and reduction of the AFW flow increased the reactor coolant pressure above 1830 psig. As a result, only a limited amount (an estimated 50 gallons) of borated water was injected into the primary system from the ECCS.

At 1:59 a.m., the No. 1 AFW pump suction transferred spuriously from the condensate storage tank to the service water system (malfunction number 10). This action was not significant, but it had occurred before and had not been corrected. Similarly, a source range nuclear instrument became inoperable after the reactor trip (malfunction number 11) and the operators initiated emergency boration pursuant to procedures. (Note: One channel had been inoperable prior to the event.) The source range instrumentation had malfunctioned previously and apparently had not been properly repaired. Also, the control room ventilation system tripped into its emergency recirculation mode (malfunction number 12), which had also occurred prior to this event.

The steam generator water levels soon exceeded the normal post-trip level and the operator terminated AFW flow to the steam generators. The subcooling margin remained adequate throughout this event. The event ended at about 2 o'clock in the morning, twelve malfunctions and approximately 30 minutes after it began.

2A.9 NRC Findings and Conclusions

The NRC review team concluded that the underlying cause of the Davis-Besse loss-of-feedwater incident was the licensee's lack of attention to detail in the care of plant equipment. The licensee had a history of performing troubleshooting, maintenance and testing of equipment, and of evaluating operating experience related to equipment in a superficial manner and, as a result, the root causes of problems were not always found and corrected. Engineering design and analysis effort to address equipment problems had frequently either not been utilized or had not been effective. Furthermore, operator interviews made clear that equipment problems were not aggressively addressed and resolved beyond compliance with NRC regulatory requirements.

In addition to this major conclusion on the underlying cause of the event, the NRC Review Team findings and conclusions included:

- The key safety significance of the event is that multiple equipment failures occurred resulting in a transient beyond the design basis of the plant. These failures included several common-mode failures affecting redundant safety-related equipment.

- The operators' understanding of procedures, plant system designs, and specific equipment operation, and operator training all played a crucial role in their success in mitigating the consequences of the event.

- If the manual initiation features of the SFRCS had originally been properly designed with regard to human factors considerations, such as labeling and placement, it is likely that no operator error in auxiliary feedwater initiation would have occurred.

- The post-TMI improvements: Temperature-saturation meters, additional training on transient behavior, and ATOG emergency procedures had a positive contribution to the mitigation of the event. Of these, training on transient behavior was the most important.

- For plant events involving conditions outside the plant design basis, operator training and operator understanding of system and equipment are key to the success of mitigating actions taken by the operators. It is not practical to rely on detailed step-by-step procedures for such events.

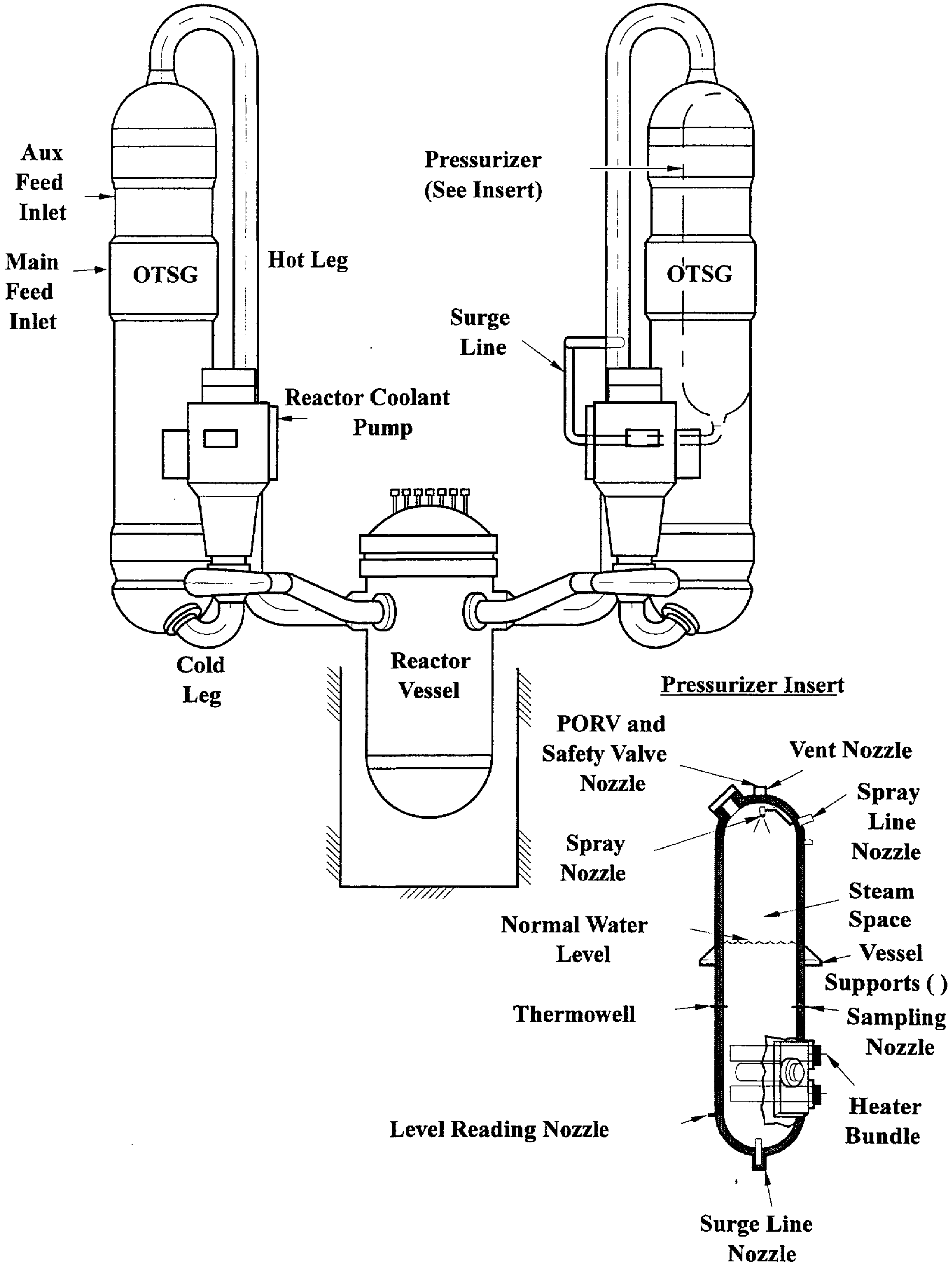


Figure 2A-1 Davis-Besse nuclear steam supply system

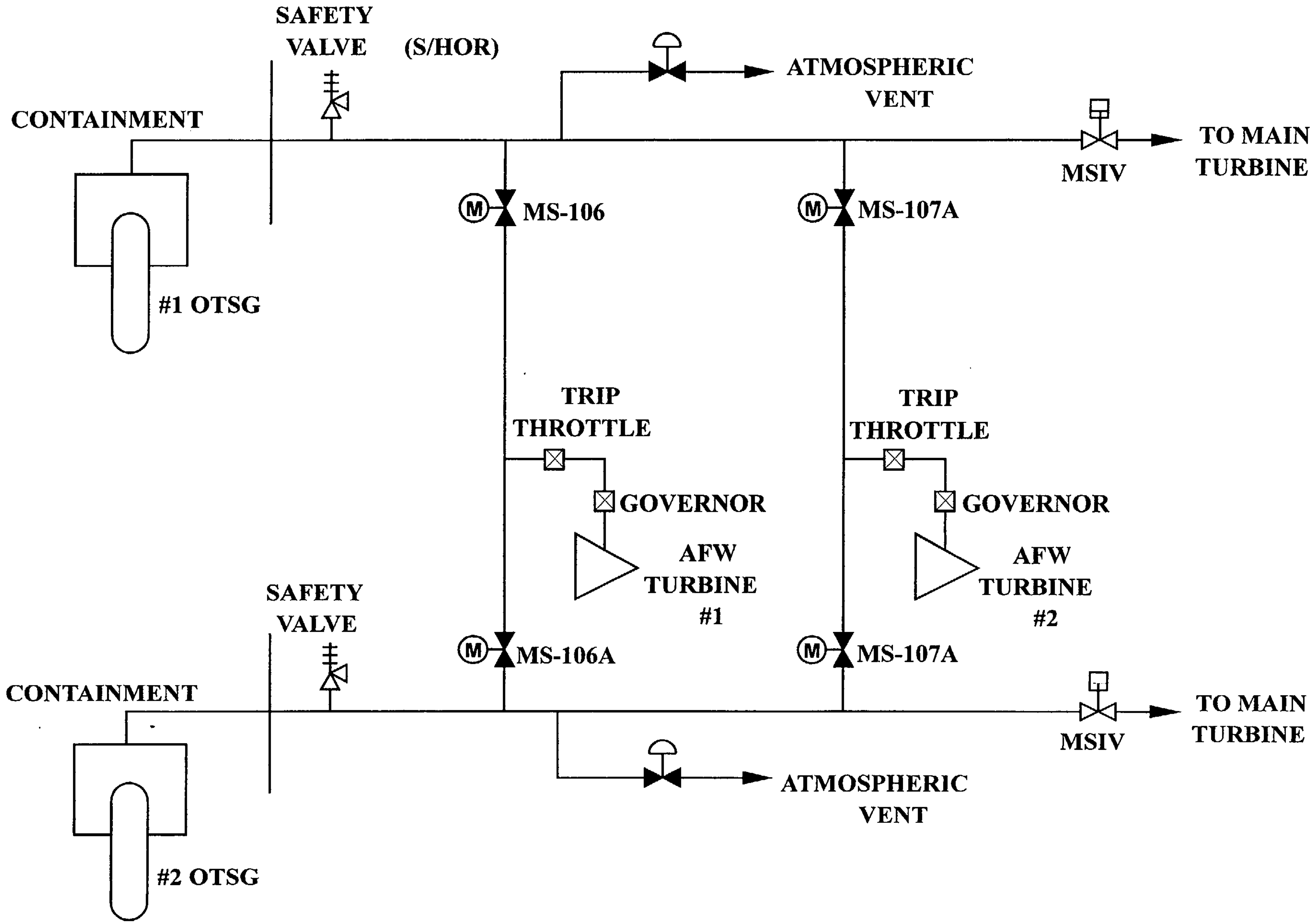
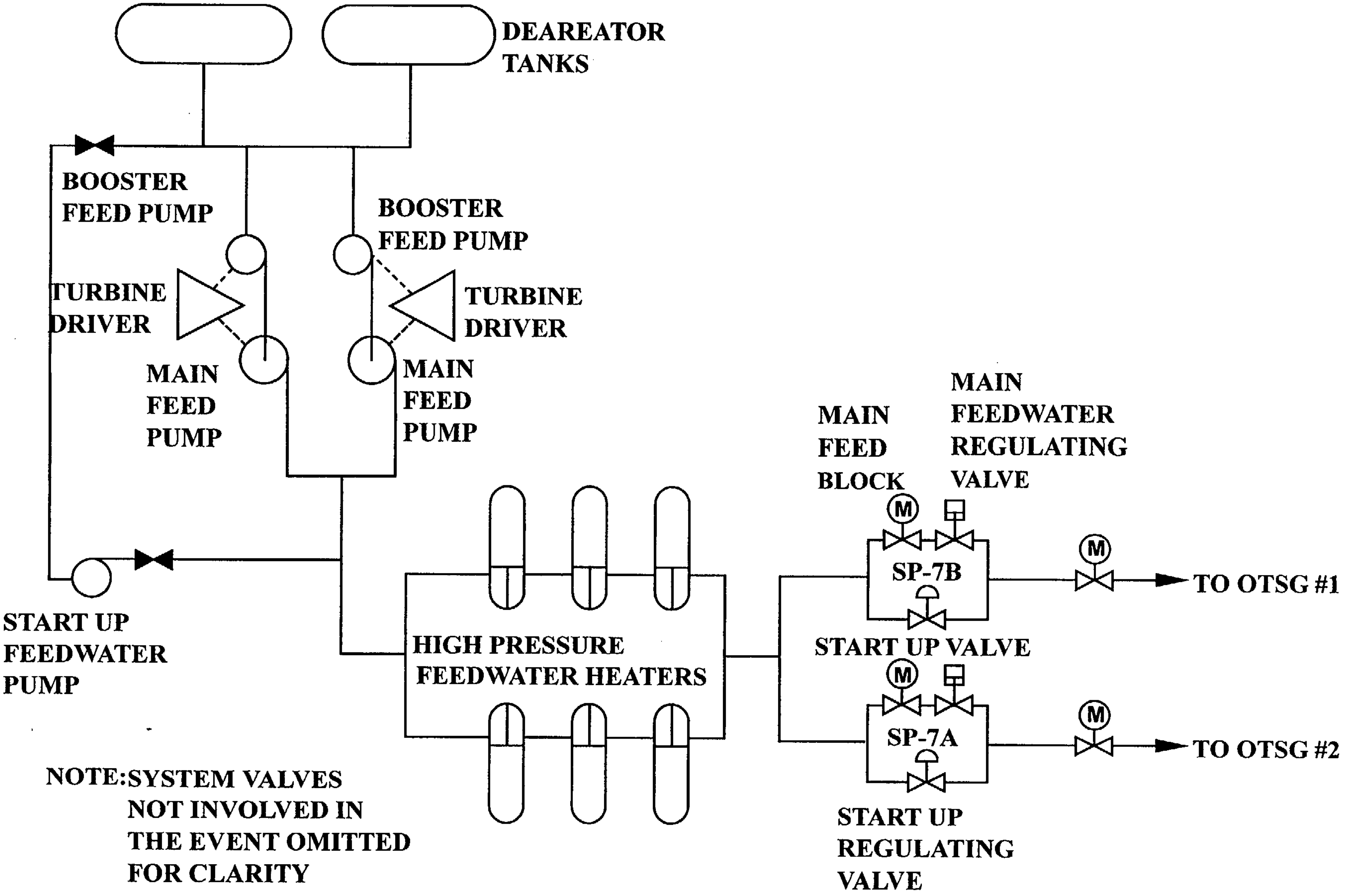


Figure 2A-2 Main steam system



NOTE: SYSTEM VALVES
NOT INVOLVED IN
THE EVENT OMITTED
FOR CLARITY

Figure 2A-3 Main feedwater system

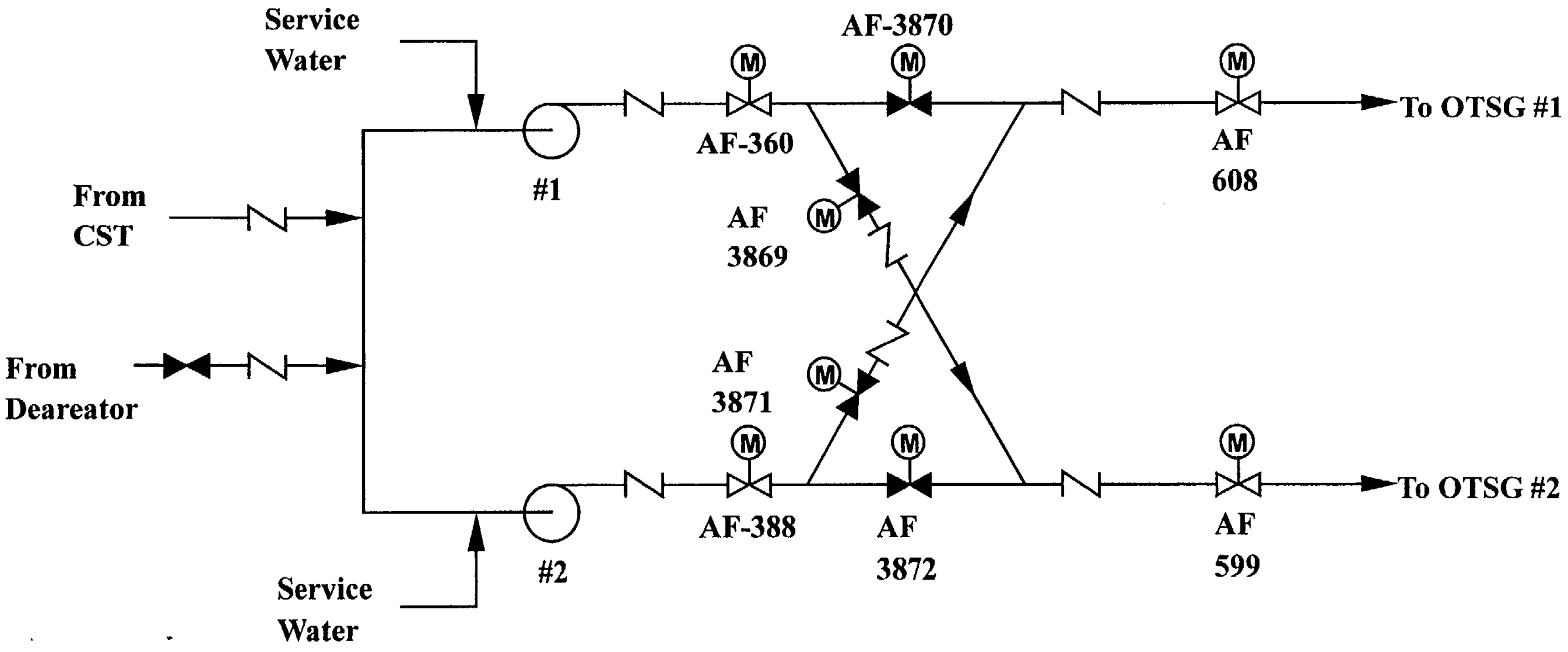


Figure 2A-4 Schematic of auxiliary feedwater system

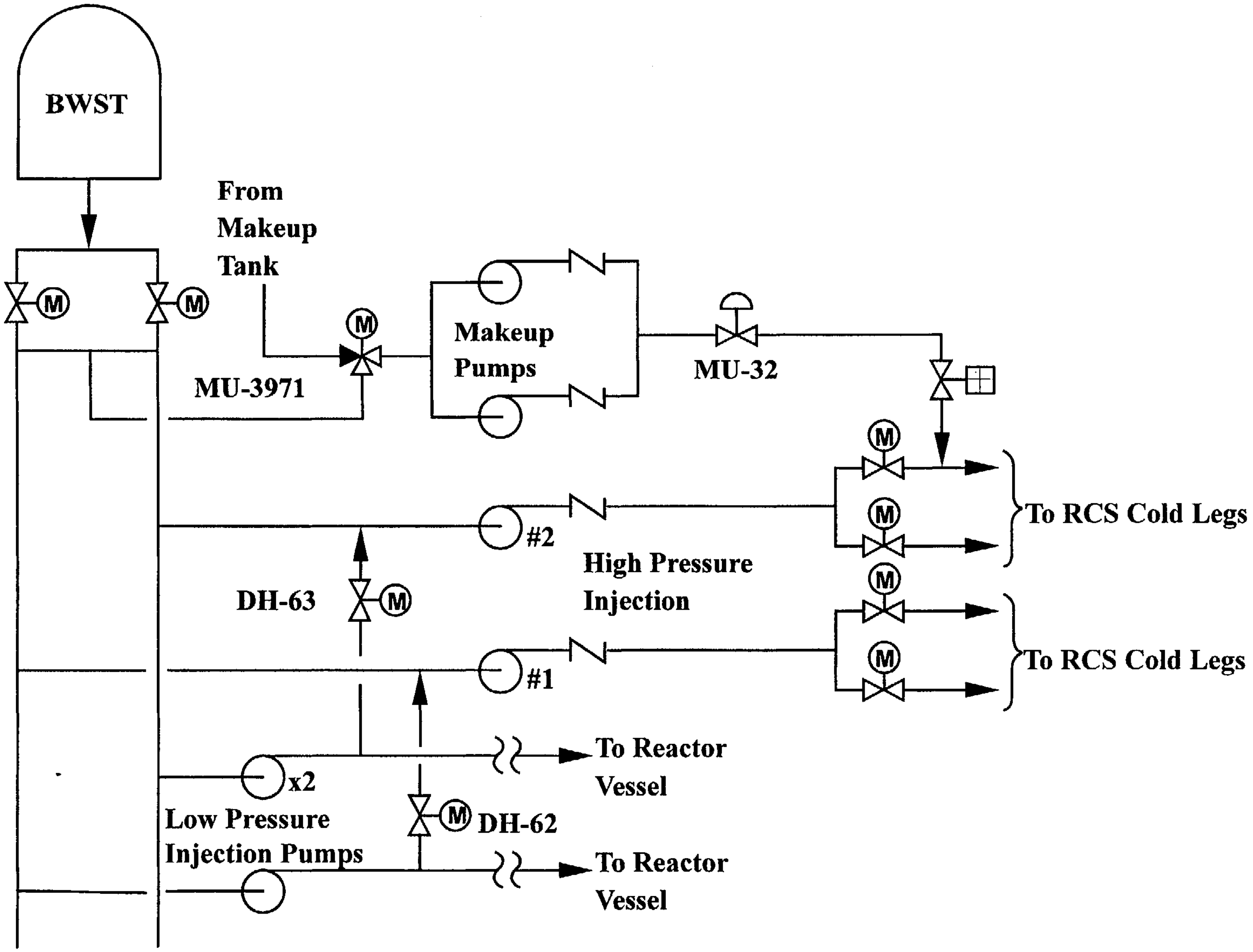


Figure 2A-5 Makeup / HPI cooling system

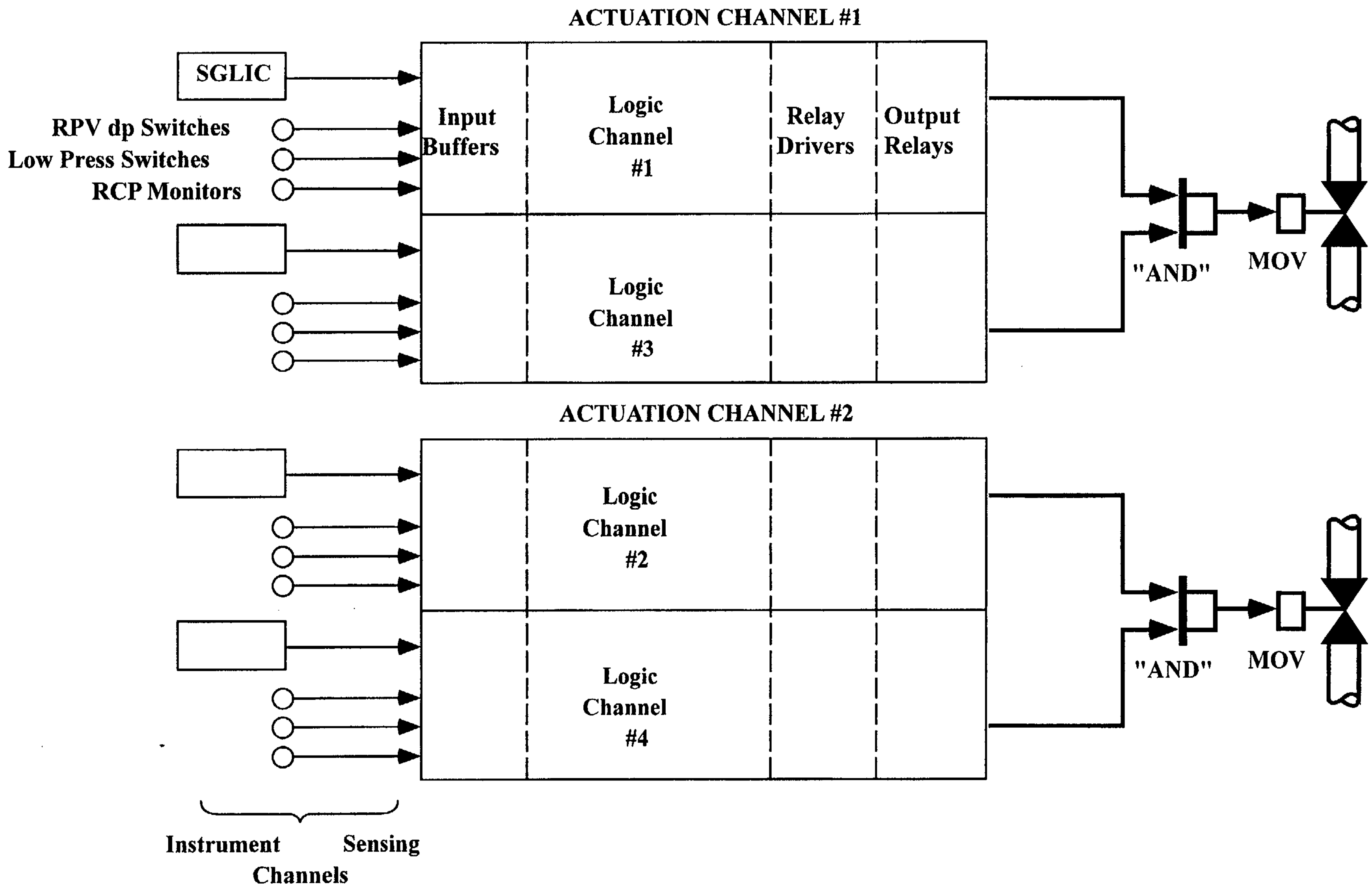


Figure 2A-6 Steam feedwater rupture control system (SFRCS) block diagram

Appendix 2B Information on ATWS

In September 1973 the regulatory staff issued a report, WASH-1270, called "Technical Report on Anticipated Transients without Scram for Water-Cooled Power Reactors,"[1] in which they publicly adopted a position on ATWS. Significant WASH-1270 insights regarding reactor protection systems and plant responses to ATWS events are presented in the next two subsections. Subsections 2B.3 and 2B.4 discuss the Browns Ferry partial failure to scram, and the Salem 1 ATWS event respectively. The final ATWS rule is reproduced as Subsection 2B.5, and Subsection 2B.6. These sections discuss the changes considered in formulating the final rule.

2B.1 Protection Systems Designs and Failure Analyses

The reactor protection system (RPS) is a safety-related system that is designed to monitor key operating plant variables; and to cause alarms, control rod insertions, or scram, as the occasion may require when off-normal conditions occur. The reactor trip system (RTS) is part of the RPS and includes those power sources, sensors, initiation circuits, logic matrices, bypasses, interlocks, racks, panels, control boards, actuation devices, and actuated devices, that are required to initiate reactor shutdown. The RTS automatically initiates control rod insertion when required to assure that acceptable fuel design limits are not exceeded. It is designed to fail safe for most internal component failures. The RTS can also be actuated manually by operator action.

The essential RTS design bases are that no single failure can negate a reactor scram when one is needed, and all instrument channels and associated trip logic must be capable of being calibrated, tested, and maintained while the plant operates. These features are implemented in protection system designs by providing for each variable that is to be measured several redundant instrument channels. In most cases, four such redundant channels are provided for each monitored variable. The output responses of the redundant channels are collected and an appropriate alarm, control rod insertion, or scram is initiated when two of the redundant channels agree that action is needed.

Just as the system designer is concerned that no failure in a subsystem should render the protective feature of a group of redundant channels inoperative, he also is concerned that the occurrence of spurious scrams be minimized. This is the reason that two concurrent trip signals are required in the normal protection system arrangement.

The kinds of single failures for which protection systems are designed to be resistant include a wide range of possible occurrences. Component malfunctions and failures are some of the kinds of single failures considered. Both a simple failure to function and an improper function, from whatever cause, are considered on the component, channel, and subsystem levels. Accidental electrical grounds at any point in the system are considered as single failure events, as are short circuits from whatever higher voltage circuits may exist in the vicinity of a given section of the protection system. An additional feature of the single failure design basis is that any damage or other consequence that follows from a hypothesized failure is included in determining the effects of that single failure. Thus, if a hypothesized hot short at some point in a protection system circuit might cause failure of several components, or spurious signals to other channels, then all of these effects are taken into account in determining the vulnerability of the overall system to the single initiating event.

Full scram tests in which the rods are actually driven into the core are carried out during shutdowns for refueling and maintenance, or on other occasions when the plant may have been shut down. During operating periods, control rods are moved periodically to adjust reactivity and power distribution in the core. This operation of the rods gives some assurance of operability, although it does not completely guarantee that the rods will scram if called upon to do so. All plants are designed to be shut down safely with the most effective control rod malfunctioning such that it does not enter the core. This "stuck rod" criterion gives assurance of the ability of the system to surmount a limited degree of operational failure.

The results of the designer's failure analyses of protection systems for random independent failures show that the systems are generally resistant to such failures. The probability of scram failure can be demonstrated to be quite low (less than 10^{-7} per demand) if only these random failure events are considered. This is due to the highly redundant nature of the protection systems and the testability provided in their designs.

As discussed in Section 2.2.4.4, common cause failures could be a result of: environmental conditions; design, manufacturing, operating or maintenance errors; or functional deficiencies such as an unrecognized deficiency in sensing instrumentation or a misunderstanding of the behavior of process variables in the design of a system. For common cause failures, the analysis of protection systems is more difficult. Techniques to analyze a system for common cause failures are not as well-developed as techniques to analyze a system for random failures. However, the fault tree models used for random failure analysis are helpful in making qualitative judgments as to the effects of common cause failures.

Defenses against common cause failures all involve "diversity" of one kind or another. One form, called equipment diversity, involves use of instruments operating on different principles to measure the same reactor variable. Use of different kinds of components in the amplifying and scram logic systems leading from the sensing instruments is also a form of equipment diversity, as in the use of different kinds of trip breakers and control rod drive mechanisms. A second form is called functional diversity, which involves instrument systems responding to different variables to provide trip action for the same transient or accident. The value of diversity of one sort or another in defending against common cause failures is that with systems of different principle and with different kinds of components, the likelihood of a common failure affecting all the elements that are significant for a given transient or accident is much diminished.

In making analyses of the effects of common cause failures on reactor protection systems, each transient is examined on the assumption that all the instrument channels pertaining to a given reactor variable (e.g., neutron flux) fail in such a way as to not give any protective action signal. All other portions of the protection system are assumed to be operative. In general, the results of these analyses show that protection systems have a reasonable degree of functional diversity in the sensor portions of the systems. If a required protective action signal is not generated by the several redundant channels for a given variable, then, in most cases, another variable is driven off-normal and the necessary signal is generated from that source. The functional diversity of protection system designs, however, often applies mainly to the sensing elements. The transmitters, amplifiers, and circuitry leading into the scram logic matrices for various reactor variables that are monitored, as well as the logic matrix relays and switches or solid-state devices, the scram breakers or pilot valves, control rod drive mechanisms, and control rods often have much less diversity.

2B.2 Plant Response to ATWS Events

For pressurized water reactor plants the transients with the greatest potential for damage in the event of a failure to scram are the loss of feedwater and certain loss of load transients occurring with the reactor at full power. Loss of feedwater flow could occur as the result of malfunctions of the interlock and supervisory circuitry controlling the feedwater or condensate pumps or valves. The sequence of events for a typical pressurized water reactor plant given a loss of feedwater transient without reactor scram may be summarized as follows:

a. An accidental trip of the feedwater or condensate pumps or valves would cause a rapid reduction of feedwater flow. Low feedwater flow compared to steam flow, in coincidence with low steam generator water level, would initiate a reactor scram signal.

b. This scram signal is ignored in the ATWS analysis, as are three or more subsequent reactor scram signals generated as the transient proceeds. The loss of feedwater flow to the steam generator secondary side would result in a drop in water level in the steam generator.

c. A falling water level in the steam generator results in reduced heat transfer from the primary system. The primary coolant temperature would begin to increase since reactor power would remain high, and this, in turn, would cause the primary pressure to increase.

d. The auxiliary feedwater pumps would be started automatically after the main feedwater pumps or condensate pumps were tripped. However, the auxiliary feedwater pump capacity is not large enough to remove all the heat being generated in the core;

e. consequently, the steam generator would boil dry.

f. The primary system temperature and pressure would continue to increase and the primary safety valves in the surge volume of the pressurizer vessel would open and discharge steam.

g. The increasing temperature of the primary coolant would cause expansion of the coolant and the water level would rise in the pressurizer.

h. When the pressurizer vessel became filled completely with water, the safety valves would discharge water instead of steam, but at a rate less than required to keep the primary system pressure from rising sharply.

i. The reactor power would decrease throughout the transient because of the negative reactivity feedback arising from increased water temperature and reduced density. This effect, combined with heat removal by the auxiliary feedwater system and with the discharge of water through the pressurizer safety valves, would reduce the pressure.

j. The pressurizer safety valves would then close and steam would reappear in the pressurizer dome. If the primary system survived the pressure peak, which was estimated in early analyses to reach values between 3000 and 7000 psi, heat generation in the core would be reduced and the heat removal capacity of the auxiliary feedwater system on the secondary side of the plant would cool the core and prevent further pressure increase.

k. Lower pressure in the primary system would allow boron solution injection into the primary system initiated by a safety injection signal generated by low pressure in the secondary steam line or by manual actuation.

l. When the boron solution reached the core, enough negative reactivity would be provided to shut the plant down.

A loss of electrical load transient could occur from a generator trip, a turbine trip, or a loss of main condenser vacuum. Generally, the most severe transient would be caused by the loss of condenser vacuum. The main feedwater pumps in many plants are steam turbine-driven and exhaust to the main condenser. Thus, loss of condenser vacuum also could cause a loss of the main feedwater pumps. In this case the sequence of events would be similar to the loss of feedwater transient. The most severe effect of the transient, the peak pressure in the primary system, would be of about the same magnitude as in the loss of feedwater flow transient.

For boiling water reactor plants, the transients having the greatest potential for significant damage are those leading to a reactor coolant system pressure increase. The most severe of these are the loss of condenser vacuum and the closure of all main steam isolation valves. A loss of condenser vacuum causes automatic closure of the turbine stop valves and the turbine bypass valves. The turbine stop valves are fast-acting valves, so there is an abrupt interruption of steam flow from the reactor. The main steam isolation valves are slower in closing, but in this case the large steam line volume is not available to buffer the pressure rise. The result in either case would be an increase in reactor coolant pressure and temperature. The pressure increase would decrease the volume of steam bubbles in the reactor core and this, in turn, would increase the reactivity and cause an increase in reactor power. The power increase would cause a further increase in system temperature and pressure. The other transients that lead to primary system pressure increase are less severe.

Generator or turbine trips are less severe because the turbine bypass valves can be assumed to open and the condenser to be operative. Although the transient proceeds more slowly in these cases, the result still would be a high reactor coolant system pressure. More details about BWR ATWS events are contained in Section 2B.7

2B.3 Failure of Control Rods to Fully Insert at Browns Ferry 3

On June 28, 1980, Browns Ferry Unit 3, a BWR, reported that 76 of 185 control rods failed to insert fully into the core when a manual scram was initiated by the reactor operator. Fortunately, this occurred during a routine shutdown from about 35% power, rather than during the kind of reactor transient in which complete and rapid scram of all the rods might have been important.

The partially inserted rods were all (with one exception) on the east side of the core where reactor power level was indicated to be 2% or less. The west side of the core was subcritical. A second manual scram was initiated 6 minutes later and all partially inserted rods were observed to drive inward, but 59 remained partially withdrawn. A third manual scram was initiated 2 minutes later, and 47 rods remained partially withdrawn. Six minutes later, an automatic scram occurred and all the rods inserted fully when the scram discharge level bypass switch was returned from "bypass" to "normal" and there was a high water level in the scram discharge instrument volume. It appears that this was a coincidence in that a manual scram would probably have produced the same result. Core coolant flow, temperature, and pressure remained normal for the existing plant conditions.

The problem was determined to be hydraulic in nature rather than electrical or mechanical. The control rod drives (CRDs), which insert and withdraw the attached control rods in a General Electric BWR, are essentially water-driven hydraulic pistons. On a scram, a relatively high water pressure is applied to the bottom side of the piston by opening a scram inlet valve. A scram outlet valve opens to relieve water and pressure above the piston and the rods are rapidly driven up into the reactor core. Water discharged from the 185 individual CRDs during scram insertion is collected in two separate headers consisting of a series of interconnected 6-inch-diameter pipes (four on each side of the reactor) called the scram discharge volume (SDV). During normal operation, both SDVs are designed to remain empty by being continuously drained to a separate scram discharge instrument volume (SDIV) tank. The SDVs are therefore normally ready to receive the scram discharge water when a scram occurs. This instrumented tank is monitored for water level and initiates an automatic scram on high level, in anticipation of too much water in the SDV preventing a scram.

The control rod drives at Browns Ferry Unit 3 are grouped in such a manner that the east and west sides of the reactor core are connected to separate SDVs. Later tests, inspections, and analyses resulted in the conclusion that the east SDV was substantially full of water at the time of the event, leaving insufficient room for the discharge water. Accordingly, upon scram actuation, the CRDs rapidly drove the control rods partially into the core but rod motion prematurely ceased when pressure quickly equalized on each side of the pistons. Following each scram actuation, the scram signal was reset by the operator, allowing some water to drain from the SDV, permitting the rods to insert further with each scram attempt. Sufficient water was finally drained from the SDV to allow the rods to insert fully on the fourth scram signal. It is believed that the east SDV water accumulation problem resulted from improper drainage into the SDIV from the SDV due to inadequate SDV venting, an obstruction in the line between the SDV and SDIV, or a combination of these problems.

The unit remained shut down while a series of tests was performed in an attempt to determine the cause of the water accumulation in the SDV. Ultrasonic probes were installed on the SDVs to continuously monitor the water level in the SDVs. A Preliminary Notification was issued to inform other NRC offices promptly. On July 3, 1980, IE Bulletin No. 80-17 was issued to all licensees operating BWRs and required them to conduct prompt and periodic inspections of the SDV; perform two reactor scrams within 20 days while monitoring pertinent variables to further confirm operability; review emergency procedures to assure pertinent requirements are included; and conduct additional training to acquaint operating personnel with this type of problem.

On July 18, 1980, Supplement 1 to Bulletin 80-17 was issued to all licensees operating BWRs. This supplement required an analysis of the "as built" SDV; revised procedures on initiation of the standby liquid control system (SLCS); specifying in operating procedures action to be taken if water is found in the SDV; daily monitoring of the SDV until a continuous monitor can be installed; and studying of designs to improve the venting of the SDV. During testing required by IE Bulletin 80-17, additional SDV anomalies were found at seven other BWRs. As a result, Supplement 2 to IE Bulletin 80-17 was issued on July 22, 1980. This required the BWR licensees to provide a vent path from the SDV directly to the building atmosphere without any intervening component except for the vent valve itself. These modifications had to be completed within 48 hours for plants operating or prior to startup for plants shut down.

Browns Ferry Unit 3 was authorized to restart on July 13, 1980, following completion of the actions required by IE Bulletin 80-17 and other extensive tests.

Continuing NRC review of this event identified a potential for unacceptable interaction between the control rod drive system and the nonessential control air system; therefore, IE Bulletin 80-17 Supplement 3 was issued on August 22, 1980. This Supplement required affected BWR licensees to implement operating procedures within five days, which required an immediate manual scram on low control air pressure, or in the event of multiple rod drift-in alarms, or in the event of a marked change in the number of control rods with high temperature alarms. In addition, the licensees were requested to implement procedures, which require a functional test using water for the instrument volume level alarm, rod block, and scram switches after each scram event.

On October 2, 1980 the NRC issued Confirmatory Orders to the licensees of 16 BWR plants requiring the installation of equipment to continuously monitor water levels in all SDVs and provisions for water level indication and alarm for each SDV in the control room. This equipment permits the reactor operators to take timely action if water accumulates in the SDV. The equipment was required to be operable by December 1980 or prior to restart for those reactors in refueling. In the interim, the licensees were required to increase their surveillance of the SDV water level.

The NRC prepared two detailed reports: "Report on the Browns Ferry 3 Partial Failure to Scram Event on June 28, 1980," dated July 30, 1980, and "Report on the Interim Equipment and Procedures at Browns Ferry to Detect Water in the Scram Discharge Volume," dated September 1980. The various aspects of the BWR scram systems were studied further by the NRC, the BWR licensees, and General Electric.

2B.4 ATWS Event at Salem 1

Salem 1, like other Westinghouse PWRs, uses two redundant reactor trip breakers (RTBs) in series in the RTS. For Salem 1, each RTB includes an under-voltage (UV) trip attachment and a shunt trip attachment to actuate (open) the trip breaker. The UV device initiates a breaker trip when de-energized, while the shunt device initiates a breaker trip when energized. For an automatic trip, only the UV device is actuated; initiation of the UV devices in either or both RTBs will actuate the control rods. A manual trip signal operates both the UV device and the separate shunt device. Either device is designed to cause the RTBs to open. Salem Unit 1 uses Westinghouse DB-50 type RTBs.

At 12:21 a.m. on February 25, 1983 a low-low water level condition in one of the four steam generators at Salem 1 initiated a reactor trip signal in the RPS. At the time, the reactor was at 12% rated thermal power in preparation for power escalation after a recently completed refueling outage. Upon receipt of the valid reactor trip signal, both of the redundant RTBs failed to open (opening of either RTB would have caused the reactor to trip). About 25 seconds later, operators manually initiated a reactor trip from the control room. The RTBs opened as a result of the manual trip signal and this resulted in insertion of all control rods and shutdown of the reactor. Following the manual trip, the plant was stabilized in the hot standby condition. All other systems functioned as designed. Approximately two hours after the Salem 1 event, the cause of the failure to trip was determined by licensee instrumentation technicians to be failure of the UV trip device in both RTBs to function as designed. The plant was placed in cold shutdown at the request of the NRC.

During investigation of this incident on February 26, 1983 by the NRC, it was found that a similar failure had occurred on February 22, 1983 at Salem 1. At 9:55 p.m. on February 22, with the reactor at 20% power, operators were attempting to transfer the 4160 volt group electrical busses from the station power transformers to the auxiliary power transformers, a routine evolution during power escalation. During the transfer attempt, one of the 4160 busses failed to transfer and deenergized, resulting in the loss of one reactor coolant pump and power for the operating main feed pump control and indication. At 9:56 p.m., a low-low level condition occurred in one steam generator (due to the loss of the main feed pump), initiating a reactor trip signal. Due to the abnormal conditions created by the loss of the 4160 volt bus and in anticipation of loss of steam generator water levels, the operator was directed at about the same time to manually initiate a reactor trip. It was understood by plant personnel and was reported to the NRC that the automatic reactor trip signal due to the low-low level in one steam generator had, in fact, caused the reactor to trip. On February 26, 1983, as a result of NRC queries, the sequence of events computer printout for February 22 was reviewed in detail and it revealed that the RTBs actually opened in response to the operator's manual trip signal. Consequently, it became evident that on February 22 (as on February 25) the two RTBs failed to open upon receipt of an automatic trip signal from the RPS. The operators initiated a manual trip even though they were unaware that the automatic trip had failed.

Since the operators initiated a manual reactor trip shortly after receipt of the automatic trip signals on both February 22 and February 25, no adverse consequences occurred and the reactor was in a safe condition. However, as the first actual ATWS events, the Salem 1 events were of major safety concern.

With few exceptions, all PWR plants designed by the three nuclear steam system suppliers (Westinghouse, Babcock & Wilcox, and Combustion Engineering) use an RTS design requiring circuit breakers to open to trip the reactor. Although the basic designs of the RTSs and the number of RTBs per plant differ considerably among the plant designers, each RTB generally includes a UV trip attachment and a shunt trip attachment to actuate the circuit breaker. Westinghouse designed plants use a Westinghouse breaker (DB type for older plants, DS type for newer plants) while the other two PWR designers use General Electric breakers (AK type).

Other pressurized water reactors (PWRs) have experienced RTB failures, both before and after the February 1983 Salem 1 events.

None of them however, involved an ATWS event. The RTB failures prior to the February 1983 events at Salem 1 had been the subject of several actions taken since 1971 by the AEC/NRC, Westinghouse, and General Electric.

Due to the serious nature of Salem 1 failure of both redundant RTBs on February 25, 1983, the NRC issued Inspection and Enforcement Bulletin No. 83-01[2] on the same day to all pressurized water nuclear power reactor facilities holding an operating license for action and to other nuclear power reactor facilities for information. The Bulletin informed the licensees of the Salem 1 February 25, 1983 event (the similarity of the February 22, 1983 event had not yet been ascertained) and mentioned that failures involving only one of the two breakers had previously occurred at Salem Unit 2, Robinson Unit 2, Connecticut Yankee, and St. Lucie. The Bulletin referenced two previously issued NRC notifications of RTB problems and Westinghouse-issued technical information on their breakers. Action items required of licensees using Westinghouse DB type breakers by Bulletin No. 83-01 included, (a) testing of the DB type breakers, (b) assuring maintenance is in accord with the recommended Westinghouse program, © notifying licensed operators of the Salem 1 events, (d) reviewing with the operators the procedures to follow in the event of failure of trip, and (e) reporting the results to the NRC.

On February 28, 1983 the NRC Executive Director for Operations (EDO) directed that NRC Region I was to develop a detailed report of the Salem 1 events. This report was subsequently issued as NUREG-0977.[3] The EDO further directed that a special NRC task force be formed to evaluate the generic implications of the events.

Possible contributors to failures of UV trip devices include: (1) dust and dirt; (2) lack of lubrication; (3) wear; (4) more frequent operation than intended by design; and (5) nicking of latch surfaces caused from repeated operation of the breakers. Based on an independent evaluation of the failed UV trip devices identified by the licensee, the NRC staff concluded that, while the Salem 1 breaker failures occurred as a result of several possible contributors, the predominant cause was excessive wear accelerated by lack of lubrication and improper maintenance.

During the testing required by Bulletin No. 83-01, no further failures of Westinghouse DB type RTBs occurred. However, even though not required to do so by Bulletin No. 83-01, Southern California Edison decided to test the General Electric type AK-2 breakers on their Combustion Engineering designed San Onofre Units 2 and 3. On March 1, 1983, one of eight RTBs in Unit 3 failed to trip on undervoltage. On March 8, 1983, three of eight RTBs in Unit 2 failed to trip on UV. (Note: Contrary to the Salem design in which an automatic trip signal is fed only to the UV trip devices, the signal is fed to both the UV and shunt trip devices for the San Onofre Units 2 and 3 design. The shunt devices were satisfactorily tested; therefore, the RTBs would have tripped from an automatic trip signal during operations.) During the investigations of these events, it was found that previous failures had occurred at these units during 1982 but had not been reported to the NRC.

Accordingly, Inspection and Enforcement Bulletin No. 83-04[4] was issued on March 11, 1983 to all pressurized water nuclear power reactor facilities holding an operating license except those with Westinghouse DB type breakers for action and to other nuclear power reactor facilities for information. The Bulletin described the San Onofre events and mentioned that similar events involving the General Electric AK-2 type breakers had previously occurred at Arkansas Unit 1, Crystal River Unit 3, Oconee Units 1 and 3, Three Mile Island Unit 1, St. Lucie Unit 1, and Rancho Seco Unit 1. Licensees were to (a) take actions similar to those required by Bulletin No. 83-01, (b) provide a description of all RPS breaker malfunctions not previously reported to the NRC, and © verify that procurement, testing, and maintenance activities treat the RTBs and associated UV devices as safety related.

In response to Bulletin No. 83-04, additional cases of past RTB failures were reported to the NRC. In addition, other failures occurred after the testing required by Bulletin Nos. 83-01 and 83-04. In all cases, the NRC closely monitored the corrective actions taken by the licensees to assure that the plants were safe for continued operation.

In parallel with the NRC initiated actions, Westinghouse formed an intercompany task force to conduct an internal review of their procedures for dissemination of technical information to utilities. In addition, they reviewed the testing program for the breakers. Since there were generic implications associated with the Salem 1 ATWS event, Westinghouse worked with the Owners Group (licensees of Westinghouse designed plants) to review operating and emergency procedures, to look for similar failures in other plant systems, and to assure that the owners had current Westinghouse technical information. Westinghouse also identified potential deficiencies with their DS type breakers, which were being used in five operating plants, and 24 plants under construction. Westinghouse developed updated maintenance procedures for both DB and DS type RTBs. Combustion Engineering and Babcock & Wilcox made similar reviews, and in cooperation with General Electric, developed updated maintenance procedures for the licensees with AK-2 type breakers.

As noted previously, the Salem 1 licensee failed to recognize on February 22, 1983 that an ATWS event had occurred. This was due to the lack of a thorough and systematic review to achieve the necessary understanding of the event. This, and previously identified problems at Salem, indicated the need for both a number of corrective actions and some significant management improvements. The NRC did not permit the Salem plants to restart until both technical and management corrective actions were satisfactory addressed. On April 26, 1983 the Commission agreed that the plants could be returned to service, after the NRC staff was satisfied with the licensee's commitment to meet certain restart conditions. On May 5, 1983 the NRC forwarded to the Salem licensee a Notice of Violation and Proposed Imposition of Civil Penalties (for $850,000).[5] Violations included operation of the reactor even though the RPS could not be considered operable, and several significant deficiencies which contributed to the inoperability of the RTBs. Region I instituted an augmented inspection program at Salem to monitor the licensee's progress towards completion of longer term corrective actions, including independent management consultants' recommendations.

The special NRC task force prepared a two-volume report, NUREG-1000.[6] The first volume dealt with the generic implications of the Salem events. The second volume documented the NRC actions to be taken based on the work of the task force. The results of the task force were considered in deliberations regarding the ATWS position and rule, which was being developed by the NRC.

2B.5 10 CFR 50.62, The ATWS Rule

50.62 Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants.

(a) *Applicability.* The requirements of this section apply to all commercial light-water-cooled nuclear power plants.

(b) *Definition.* For purposes of this section, "Anticipated Transient Without Scram" (ATWS) means an anticipated operational occurrence as defined in Appendix A of this part followed by the failure of the reactor trip portion of the protection system specified in General Design Criterion 20 of Appendix A of this part.

(c) *Requirements.*

(1) Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions' indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

(2) Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods).

(3) Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.

(4) Each boiling water reactor must have a standby liquid control system (SLCS) with a minimum flow capacity and boron content equivalent in control capacity to 86 gallons per minute of 13 weight percent sodium pentaborate solution. The SLCS and its injection location must be designed to perform its function in a reliable manner. The SLCS initiation must be automatic and must be designed to perform its function in a reliable manner for plants granted a construction permit after July 26, 1984 and for plants granted a construction permit prior to July 26, 1984 that have already been designed and built to include this feature.

(5) Each boiling water reactor must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.

(6) Information sufficient to demonstrate to the Commission the adequacy of items in paragraphs (c)(1) through (c)(5) of this section shall be submitted to the Commission as specified in 10 CFR 50.4.

(d) *Implementation.* By 180 days after the issuance of the QA guidance for nonsafety related components, each licensee shall develop and submit to the Commission, as specified in 10 CFR 50.4, a proposed schedule for meeting the requirements of paragraphs (c)(1) through (c)(5) of this section. Each shall include an explanation of the schedule along with a justification if the schedule calls for final implementation later than the second refueling outage after July 26, 1984, or the date of issuance of a license authorizing operation above 5 percent of full power. A final schedule shall then be mutually agreed upon by the Commission and licensee.

[49 FR 26044, June 26, 1984; 49 FR 27736, July 6, 1984, as amended at 51 FR 40310, Nov. 6,1986]

2B.6 Changes Considered for ATWS Rule

10 CFR 50.62 (c)(1)
<u>Diverse and Independent Auxiliary Feedwater Initiation and Turbine Trip for PWRs</u>

This was proposed by the Utility Group on ATWS. It consists of equipment to trip the turbine and initiate auxiliary feedwater independent of the reactor trip system. It has the acronym AMSAC, which stands for Auxiliary (or ATWS) Mitigating Systems Actuation Circuitry. It showed a highly favorable value/impact for Westinghouse plants and a marginally favorable value/impact for CE and B&W plants. It should be designed to minimize the potential for causing a spurious reactor trip.

10 CFR 50.62 (c)(2) and (c)(3)
<u>Diverse Scram System</u>

This was proposed by the Utility Group on ATWS for CE, B&W and GE plants. The NRC staff analysis showed a favorable value/impact. However, the principal reasons for requiring the feature are to assure emphasis on accident prevention and to obtain the resultant decrease in potential common cause failure paths in the RTS. It should be designed to minimize the potential for causing a spurious trip of the reactor. A diverse scram system for Westinghouse plants was not a recommendation of the Utility Group on ATWS and was not a clear requirement of the Staff Rule or the Hendrie Rule. NRC staff analyses indicated a marginally favorable value/impact for Westinghouse plants; however, a diverse scram was ultimately not required for Westinghouse plants.

10 CFR 50.62 (c)(4)
<u>Increased Standby Liquid Control System (SLCS) Capacity</u>

The SLCS is a system for injecting borated water into the reactor primary coolant system. The neutron absorption by the boron causes shutdown of the reactor. Addition of this system was proposed by the Utility Group on ATWS for new plants (those receiving an operating license three years after the effective date of the final rule). Because of the vulnerability of BWR containments to ATWS sequences, the NRC determined that increased SLCS capacity was warranted. The preferred location for SLCS injection was into HPCS or HPCI lines, which provides significant improvement in mixing of borated water when compared to SLCS injection into the standpipe at the core inlet plenum. The HPCS/HPCI injection location is also preferred, since it could prevent local power increases and possible power excursions during the recovery phase of an ATWS when cold unborated ECCS water could be added above the core. Some BWR/5 and BWR/6 licensees already had this injection location.

10 CFR 50.62 (c)(4)

Automatic Initiation of Standby Liquid Control System

One of the alternatives considered by the Task Force was an automatically initiated standby liquid control system with a capacity of greater than 86 gpm (such as 150-200 gpm). This would have resulted in a considerable ATWS risk reduction (about a factor of seven) for operating plants. Unfortunately, the cost to do this (based on information supplied by the Utility Group on ATWS) would have been on the order of $24 million per plant. This cost is significantly impacted by the costs of downtime for installation in existing plants and by an allowance for potential downtime from an inadvertent trip that would inject boron into the reactor vessel. The value/impact did not favor this alternate for existing plants. New plants (those receiving construction permits after the effective date of the ATWS rule) are required to have automatic SLCS initiation. The equipment for automatic SLCS actuation should be designed to perform its function in a reliable manner while minimizing the potential for spurious actuation.

10 CFR 50.62 (c)(5)
Automatic Recirculation Pump Trip for BWRs

Recirculation pump trip (RPT) results in a reduction of reactor power from 100 percent to about 30 percent within a minute or so of an ATWS. This requirement had already been implemented on all operational BWRs in response to a show cause order dated February 21, 1980. The BWR owners generally agreed that this was a necessary requirement. It was included in the final rule for completeness.

Adding Extra Safety Valves or Burnable Poisons

One of the alternatives considered by the NRC Task Force was adding more safety valves to plants manufactured by CE and B&W. This would reduce the peak pressure in the reactor vessel and yield a higher probability of the plant surviving an ATWS with no core damage. The peak overpressure could also be reduced by modifying the core behavior (the fraction of the time the moderator temperature coefficient is unfavorable) by adding burnable poisons. The Utility Group on ATWS estimated that installing larger valve capacity could cost up to $10 million per plant. A large fraction of this is the cost of downtime for installation of the valves. The NRC found the value/impact of this option to be unfavorable for existing plants. Thus, the ATWS rule does not cover enhanced pressure relief capacity for new CE and B&W plants. However, the NRC expects this issue to be addressed during licensing reviews of any specific new or standard plant application.

2B.7 BWR ATWS Behavior and Mitigation Measures

Anticipated Transient Without Scram (ATWS) is the set of accident sequences initiated by a failure of control rod insertion following a transient event for which the plant protection system normally provides a scram. These sequences involve failure of the scram function and, if not successfully brought under control, can lead to a severe accident situation. BWR ATWS has several unique features, particularly with respect to mitigation measures such as reactor vessel water level control. It is characterized by an early threat to containment integrity, because the energy release from the reactor vessel into the pressure suppression pool can greatly exceed the capacity of the pool cooling equipment.

For the ATWS accident sequences, as for all other BWR accident sequences, core degradation can occur only after failure of adequate reactor vessel injection. If sufficient water is injected during ATWS to maintain a lower portion of the core critical, then sufficient steam will be generated to provide adequate steam cooling of the uncovered (subcritical) upper region of the core. Structural degradation and melting would occur in an ATWS severe accident only after reactor vessel injection had been lost, with the subsequent heatup of the uncovered core under the impetus of decay heating.

2B.7.1 Categories of BWR ATWS

This set of accident sequences includes many variations, but the chief distinction lies between ATWS accident sequences where the main steam isolation valves (MSIVs) remain open (but the main turbine is tripped so that steam flow into the main condenser is via the turbine bypass valves) and ATWS sequences with the reactor vessel isolated.

2B.7.1.1 Turbine Trip With Bypass

The ATWS accident sequence for which main turbine trip is the initiating transient is illustrated in Figure 2B-1. The calculated flows shown in this example are based upon the Browns Ferry Nuclear Plant. Here the feedwater pumps continue to function and are automatically adjusted (by the feedwater control system) so as to maintain the reactor vessel water level in its normal operating range. Thus, vessel water level is approximately constant initially and does not play a role in causing variation of core power.

The central assumption for the steady-state balance of flows shown in Figure 2B-1 is that the core power would be 30% under natural circulation conditions (recirculation pumps tripped), as has been determined by many analyses.[7,8] Most of the steam generated within the reactor vessel is passed to the main condensers, but the capacity of the turbine bypass valves is limited, and some must escape via a single cycling safety/relief valve (SRV). Makeup water to the reactor vessel to replace the mass lost by steam relief into the pressure suppression pool is provided by a combination of vacuum drag into the main condenser hotwell from the condensate storage tank (CST) and control rod drive hydraulic system (CRDHS) injection.

Because the core remains covered, the turbine trip-initiated ATWS accident sequence has less severe consequences than does the MSIV closure case, discussed in the next Section. Nevertheless, many studies (such as Reference 2) have shown that unstable pressure fluctuations are expected to eventually develop between the reactor vessel and the main turbine bypass valve control system, which in turn would cause large swings of core void collapse and power increase. As these instabilities eventually induce large fluctuations in the vessel water level, the condition for MSIV tripping on low level would be approached.

2B.7.1.2 MSIV Closure

The ATWS initiated by a transient event that causes closure of the MSIVs is the most threatening of this class of accident sequences. An example, based upon the Browns Ferry Nuclear Plant, of the flows associated with the MSIV closure ATWS is provided as Figure 2B-2. With the MSIVs closed, almost all of the steam exiting the reactor vessel would be passed through the SRVs into the pressure suppression pool.

[The remainder would be used to drive the high pressure coolant injection (HPCI) or reactor core isolation cooling (RCIC) turbines during their periods of operation and then would enter the pressure suppression pool as turbine exhaust.] Because the rate of energy deposition into the pool can greatly exceed the capacity of the pool cooling equipment, excessive pool temperature leading to primary containment failure by overpressurization is of major concern.

The dominant ATWS sequences identified by the severe accident risk assessment (NUREG-1150[9]) study all include MSIV closure as an initiating event. Specifically, this study identifies two variations of MSIV closure ATWS as among the more probable combinations of failures leading to core damage for Peach Bottom. For Grand Gulf, one MSIV closure case is described as "the most probable combination of failures leading to core damage" within the general class of ATWS sequences. In general, ATWS sequences initiated by MSIV closure are found by probabilistic risk assessments to be second in core melt frequency (behind station blackout) for BWRs. Examples of calculated values are 42% of the overall calculated risk for Peach Bottom[9], 3% for Grand Gulf [9], 28% for Limerick[10], and 32% for Susquehanna [11].

2B.7.2 Mitigation Measures

The discussions that follow are based upon the assumption of MSIV closure with complete failure of the scram function, so that the control blades remain in the withdrawal pattern that existed before the inception of the transient. Total failure of blade movement constitutes the most severe ATWS case, but is also the most improbable of the possible scram system failures. Where specific setpoints are given, the values appropriate to the Browns Ferry Nuclear Plant[12] are used for the purpose of illustration.

2B.7.2.1 Recirculation Pump Trip

As in all reactor designs, the criticality of the BWR depends upon a complicated set of factors that simultaneously introduce positive or negative reactivity. Whether power is increasing, constant, or decreasing at a given point in time depends upon the particular reactivity balance at that instant. In BWR studies, it is necessary to recognize the importance of the void coefficient of reactivity. "Voids" are created by the steam bubbles formed by boiling within the core. The moderation or slowing down of neutrons is much less in steam than in liquid water, so increased voiding has the effect of reducing the supply of thermal neutrons. Therefore, an increase in voids introduces negative reactivity and a decrease in voids introduces positive reactivity. Because the BWR operates with the water moderator at saturation condition within the core, negative or positive reactivity insertions caused by the creation or elimination of voids are a natural, important, and immediate result of reactor vessel pressure changes.

When successfully inserted, the BWR control blades introduce enough negative reactivity to ensure that the reactor is maintained subcritical even with the moderator at room temperature and with zero voids in the core. (This is true even with as many as five control blades stuck in the fully withdrawn position.) It is easy to imagine that there must be many dangerous situations that might arise during reactor power operation that would require instantaneous shutdown by reactor scram. However, careful review reveals that only one set of initiating conditions might actually require control blade scram as the only means to prevent the occurrence of a severe accident. This is a closure of all MSIVs compounded by failure of recirculation pump trip (RPT), which is an "unanticipated transient," meaning that it is not expected to occur during the lifetime of the plant. Before considering the ramifications of failure of RPT, it is instructive to examine the progression of events without scram but *with* RPT.

During the 3- to 5-s period while the MSIVs are closing, the reactor vessel is progressively isolated, and, because the reactor is at power, the vessel pressure rapidly increases. The pressure increase causes the collapse of some of the voids in the core, inserting positive reactivity and increasing reactor power, which in turn causes increased steam generation and further increases pressure. This cycle is interrupted when the vessel pressure reaches the level of the SRV setpoints; the SRVs open to reduce the rate of pressure increase and the recirculation pumps are automatically tripped on high pressure. With RPT, the core flow is reduced to about 25% of its former value as the driving mechanism is shifted from forced to natural circulation. With reduced inlet flow, the temperature of the moderator in the core region is increased, producing additional voids and introducing negative reactivity. The rapid increase of reactor power is terminated, and power then rapidly decreases to about 30% of that at normal full-power operation.

If failure of the installed automatic protection logic caused the recirculation pumps to continue operation after the reactor vessel pressure had exceeded their trip setpoint (highly improbable), then two possible outcomes must be considered. Because the total relief capacity of the SRVs is about 85% of normal full-power steam generation, an increasing spiral of reactor power and vessel pressure might continue to the point of overpressure failure of the primary system, inducing a LOCA. On the other hand, with all SRVs open and very little makeup water being added to the vessel, the loss of coolant through these valves could cause uncovering of the core and subcriticality by loss of moderator before the pressure became sufficiently high to cause rupture of the vessel pressure boundary. Calculations with the RAMONA code at Brookhaven National Laboratory have indicated a peak pressure of 1340 psia (9.24 MPa) for ATWS without RPT, which is below the design pressure of the reactor vessel. Thus, these calculations indicate that the loss of coolant from the vessel would effectively terminate the power-pressure spiral.

Assuming that the RPT does function as designed, it is axiomatic that although all transient-initiated accident sequences can most easily and quickly be brought under control and terminated by scram, they can also be controlled and terminated by appropriate other operator-initiated actions. In other words, given *properly trained operators and properly functioning equipment,* a failure-to-scram can be considered to be merely a nuisance requiring more complicated and time-consuming methods of achieving shutdown. The real difficulty for the ATWS accident sequence is that inappropriate actions by the operator might create an unstable and threatening situation.

2B.7.2.2 Standby Liquid Control System (SLCS)

Injection with the SLCS is the normal means for adding boron to the reactor vessel. Although this system is designed to inject sufficient neutron-absorbing sodium pentaborate solution into the vessel to shut down the reactor from full power (independent of any control blade motion) and to maintain the reactor subcritical during cooldown to ambient conditions, the SLCS is not intended to provide a backup for the rapid shutdown normally achieved by scram. Additional information on the basic design of the SLCS is provided in Chapter 3, Section 3.7.3.

In most of the current BWR facilities, the sodium pentaborate enters the reactor vessel via a single vertical sparger located at one side of the lower plenum just below the core plate as indicated in Figure 2B-3. (In an effort to improve the mixing and diffusion of the injected solution [which has a specific gravity of about 1.3] throughout the core region, some BWR facilities have been modified to provide a third positive displacement pump and to permit the injected solution to enter the reactor vessel via the core spray line and sparger.) With injection into the lower plenum, upward flow at the core inlet is necessary to sweep the heavier-than-water sodium pentaborate solution into the core.

2B.7.2.3 Manual Rod Insertion

Failure of the automatic scram function requires that the operators manually take the actions necessary to introduce enough negative reactivity into the core to produce shutdown. The operators might do this by manual scram, in case the ATWS was caused by failure of the protective system logic. Otherwise, the operators could manually drive in the control blades, one at a time for plants such as Browns Ferry. As indicated by Figure 2B-4, this procedure, for the most part, involves different piping and valves than are used for scram. Therefore, although relatively slow, manual blade insertion has a significant probability of success as an alternative to scram.

Manual control blade insertion may be essential to avoid containment pressures sufficient to threaten structural integrity in the unlikely event that the liquid neutron poison cannot be injected. However, for the BWR-4 and BWR-5 plants that have these systems, manual insertion requires that the operators bypass the rod worth minimizer (RWM) and the rod sequence control system (RSCS). Typically, the RWM can be quickly overridden from the control room, but the RSCS can only be bypassed by the installation of jumpers in the relay room, an action that can reasonably be expected to take about 15 minutes once the decision to initiate the bypass is made. Because manual blade insertion for these plants is a slow process anyway (one blade at a time, at a speed requiring about one minute for travel from fully withdrawn to fully inserted), the additional time required to effect bypass of the RSCS may be unacceptable from the standpoint of preplanning for effective ATWS management.

The RSCS was originally intended to eliminate the potential for local core damage from a high-worth control rod drop accident at low power. However, a more recent analysis by General Electric has demonstrated that such damage would not occur because local voiding would limit the associated power excursion. The NRC has issued a Safety Evaluation Report[13] that concludes that it is acceptable to remove the plant Technical Specification requirements for the RSCS. From the standpoint of enhancement of the ability of the operators to successfully respond to ATWS, it is desirable that this system be removed from the affected plants[14].

2B.7.2.4 Control of Vessel Injection

While the reactor vessel remains pressurized, makeup flow under the conditions of an MSIV closure ATWS can only be provided by the HPCI, RCIC, and CRDHS. (For purposes of illustration, this discussion is based upon the Browns Ferry/Peach Bottom configuration. Some other plants have different systems available.) The operators can manually reduce reactor power by taking control of these high pressure injection systems and decreasing the injection rate. As illustrated in Figure 2B-2, the HPCI and RCIC systems inject into the reactor vessel through the feedwater lines whereas the relatively small CRDHS flow enters the vessel through the control rod guide tubes.

It is demonstrated in Appendix B of Reference 1 that given an ATWS situation in which the reactor core is capable of unrestricted power operation, the average power depends only on the injection rate. The proof is simple, using only the first law of thermodynamics. Furthermore, if the injection rate to the vessel is specified, then the average power can be determined by a simple hand calculation. Figure 2B-2 illustrates the flows to the reactor vessel provided by operation of HPCI, RCIC, and CRDHS; these total to 2.846×10^6 lb/hr, which under these conditions is equivalent to 5700 GPM (0.360 m^3/s). Employing the simple method explained in Reference 1 (Appendix B), the average reactor power is 28%, as shown on Figure 2B-2.

As an example of the possible development of ATWS mitigation strategies based on injection control, it is known that about 4% power can be removed from the pressure suppression pool with all four Residual Heat Removal (RHR) heat exchangers in operation. It is easy to show, using the equations demonstrated in Reference 1 (Appendix B), that injection of about 1100 GPM (0.0694 m^3/s) to the reactor vessel will result in transfer of about four percent power to the pressure suppression pool. However, determination of the resultant reactor vessel water level is not a simple matter. An injection rate of 1100 GPM might well correspond to a substantial portion of the upper core being uncovered while the power (and steam) generation was confined to the lower, covered, region of the core. Steam cooling under these conditions would prevent degradation of the uncovered region.

As discussed in the next Section, the ATWS mitigation procedures recommended by the BWR Owner's Group do not invoke control of vessel injection rate, but rather direct the operators to maintain the reactor vessel water level in the vicinity of the top of active fuel. This seemingly simple shift of the operator control parameter from the injection rate to the indicated vessel water level greatly complicates both the operators role and the calculation of the average core power.

2B.7.3 Application of Emergency Procedure Guidelines

The control room operators would recognize the onset of an ATWS by the unique combination of scram signals, continued indication of reactor power on the average power range monitors (APRMs), and continued indication that multiple control blades remained in their fully withdrawn positions. For a case in which the reactor did not scram automatically in conjunction with an MSIV closure event, entry into the Reactor Vessel Control Guideline of the EPGs would be triggered by vessel pressure above the high pressure scram setpoint and "a condition which requires reactor scram, and reactor power above APRM downscale trip..."[15] Either of these triggers is by itself sufficient for entry; only the second, however, is a unique signature of ATWS. The high reactor vessel pressure would also cause tripping of the recirculation pumps.

The Reactor Vessel Control Guideline calls for simultaneous efforts to control reactor vessel water level, vessel pressure, and reactor power. Initial measures would be taken to induce reactor shutdown by manual scram. The alternate rod insertion (ARI) system would be initiated, which vents the reactor scram air header and closes the scram discharge volume vent and drain valves. Each of these actions has the potential to induce scram, but for the purposes of this discussion, it is assumed that the ATWS is not terminated.

If the main condenser is available, the EPGs direct action to open the MSIVs and employ the turbine bypass valves to establish the condenser as a heat sink. Since the bypass valves can pass about 25% of the normal full-power steam flow from the vessel, this maneuver would greatly reduce the steam flow into the pressure suppression pool and the pool heatup. Implementation of all available pool cooling is directed by the primary containment control guideline of the EPGs.

With the MSIVs closed and the recirculation pumps tripped, several SRVs would be continuously open (the number depending on reactor power), while one valve cycled open and closed. (This is illustrated in Figure 2B-2, where three SRVs continuously open to pass 19.41% of the normal steam flow and one valve slowly cycles to pass another 0.37%.) In accordance with the EPGs, the operators would attempt to terminate the valve cycling by taking remote-manual control of the SRVs and reducing vessel pressure.

Reduction of reactor vessel pressure by manual SRV actuation under ATWS conditions would be extremely difficult.[7] If the operator attempted to open a valve that was already open (by automatic actuation), nothing would happen. When the operator opened a previously closed valve, the vessel pressure would drop only slightly, until one of the previously open valves went shut. Thus, there would be only a negligible response to operator SRV control until the operator had manually opened as many valves as had previously been automatically open (three in our example). Upon manual opening of the next valve (the valve previously cycling, now to be held continuously open), the vessel pressure would rapidly decrease because of the power reduction (caused by increasing voids) occurring while several relief valves (four in our example) are held open.

The operator would have to be extremely quick to avert a complete vessel depressurization. However, closing the SRVs with the reactor critical at low pressure causes void collapse with rapid reactivity insertion. The concomitant power increase and steam generation would cause a full vessel repressurization. (The relative intensity of void collapse at low pressure is much greater than at high pressure, as illustrated by Table 2.B-1.) Under these rapidly changing conditions involving power and pressure oscillations, it could not be claimed that the operator had control of either reactor vessel power or pressure.

Initiation of the SLCS to inject sodium pentaborate solution into the reactor vessel is directed by the EPGs "before suppression pool temperature reaches the Boron Injection Initiation Temperature (BIIT)". Simultaneous action to manually drive the control blades into the core is also directed. Several backup methods are specified for each endeavor should the primary means of accomplishment fail.

The BIIT is defined to be the greater of either the pressure suppression pool temperature at which scram is required (by the plant Technical Specifications) or the highest pool temperature at which SLCS initiation would result in reactor (hot) shutdown during ATWS before the Heat Capacity Temperature Limit (HCTL) is exceeded. It is important to recognize that if the HCTL is exceeded, then rapid depressurization of the reactor vessel is required by the EPGs. Clearly the intent here is to avoid imposition of a requirement for rapid depressurization of a critical reactor by achieving hot shutdown before the pool temperature reaches the HCTL. In some plants, however, this may not be possible, and the only way to avoid having to attempt a rapid depressurization with the reactor critical is to adopt a higher HCTL during ATWS.

Instructions for control of reactor vessel water level under ATWS conditions are provided by Contingency #5 "Level/Power Control" of the EPGs. With the reactor remaining at power while sodium pentaborate solution is being injected, this contingency directs that the reactor vessel water level should be lowered to the top of the core. (Operation of the Automatic Depressurization System [ADS] while the water level is reduced is to be manually prevented.) Water level reduction is accomplished by restricting injection to the relatively small amounts provided by the SLCS and the CRDHS.

The effects of reactor vessel water level reduction upon core power are illustrated in Figure 2B-5. It should be noted that the major reduction occurs as the feedwater spargers become uncovered. Prior to this time, the feedwater (much colder than normal since the feedwater heaters are not operating) is injected underwater and passes directly downward through the jet pumps to the core inlet. With the spargers uncovered, however, the feedwater droplets are sprayed into the steam atmosphere within the vessel, where the steam condenses upon and heats the feedwater. In effect, this restores a form of feedwater heating and much warmer water enters the core inlet, which tends to increase the voids in the lower core and thereby reduce reactor power.

The discontinuity in the power vs level curve near the top of the core (at 366 in.) should also be noted on Figure 2B-5. This occurs because the water recirculation loop within the reactor vessel becomes broken as the level falls below the bottom of the steam separators. In effect, the core boiling takes on the characteristics of a swimming pool reactor, with only enough flow at the core inlet to replace the water mass being converted to steam.

Once the reactor vessel water level has been reduced, the EPGs specify that the new level is to be maintained (by control of injection rate) between the top of the core and the Minimum Steam Cooling RPV Water Level, which (employing several very conservative assumptions) is defined so as to ensure adequate steam cooling of the upper regions of a partially uncovered critical core.

When sufficient time has passed since SLCS initiation to inject the Hot Shutdown Boron Weight (HSBW) into the reactor vessel, the EPGs specify that the vessel water level should be restored to the normal range. Raising the water level involves increased flow at the core inlet, which serves to sweep the sodium pentaborate solution that has collected within the lower plenum up into the core region.

2B.7.4 Summary

Automatic recirculation pump trip reduces the reactor power. The operators can act to reduce power further by initiating the injection of liquid neutron poison (some plants have automatic provisions for this) and by manual insertion of control blades. However, these measures require time to produce effects.

The strategy provided by the EPGs for dealing with an MSIV closure ATWS can be summarized as follows: initiate injection of sodium pentaborate solution and lower the reactor vessel water level to the vicinity of the top of the core; when sufficient boron has been injected to achieve hot shutdown, restore the vessel level to the normal range. These actions should terminate the accident sequence before the pressure suppression pool temperature reaches the HCTL and without core damage. The principal challenge that might thwart this desired conclusion is that the operator actions taken while attempting to achieve the pressure control directed by the EPGs might unintentionally create an unstable situation.

If, however, all means of injection of sodium pentaborate solution into the reactor vessel fail, then temporary, partial measures to reduce core power such as lowering the reactor vessel water level can only delay the progression of events into a severe accident. Manual control blade insertion can bring about permanent reactor shutdown, but this is a very slow process. Failure of the boron injection systems is a premise of the ATWS accident sequences leading to severe core damage identified by NUREG-1150. (The sole exception involves ATWS combined with early total loss of injection.)

Severe core damage resulting from ATWS can occur only if the reactor vessel injection systems become failed and sufficient water cannot be kept in the core region. Containment events provide the bases for a potential loss of vessel injection systems during BWR ATWS, and the various injection systems might be lost in different ways. Most are low pressure systems, requiring that the reactor vessel be depressurized for performance of function. The HPCI and RCIC systems are capable of high pressure injection, but are susceptible to elevated pressure suppression pool temperatures when taking suction from this source. In addition, both of these systems have high turbine exhaust pressure trips so that high primary containment pressure can defeat their function. Steam-driven feedwater pumps would be lost at the inception of the accident sequence when MSIV closure cuts off their steam supply.

Table 2.B-1 The change in vapor specific volumes for a given change in pressure is much greater at low pressure (Table entries based on values taken from steam tables)

Pressure (psia)	Relative Change in Vapor Specific Volume per Unit Change in Pressure
15.0	3634.4
100.0	92.5
200.0	24.7
300.0	11.0
400.0	6.4
500.0	4.2
600.0	2.9
700.0	2.2
800.0	1.7
900.0	1.3
1000.0	1.1
1050.0	1.0

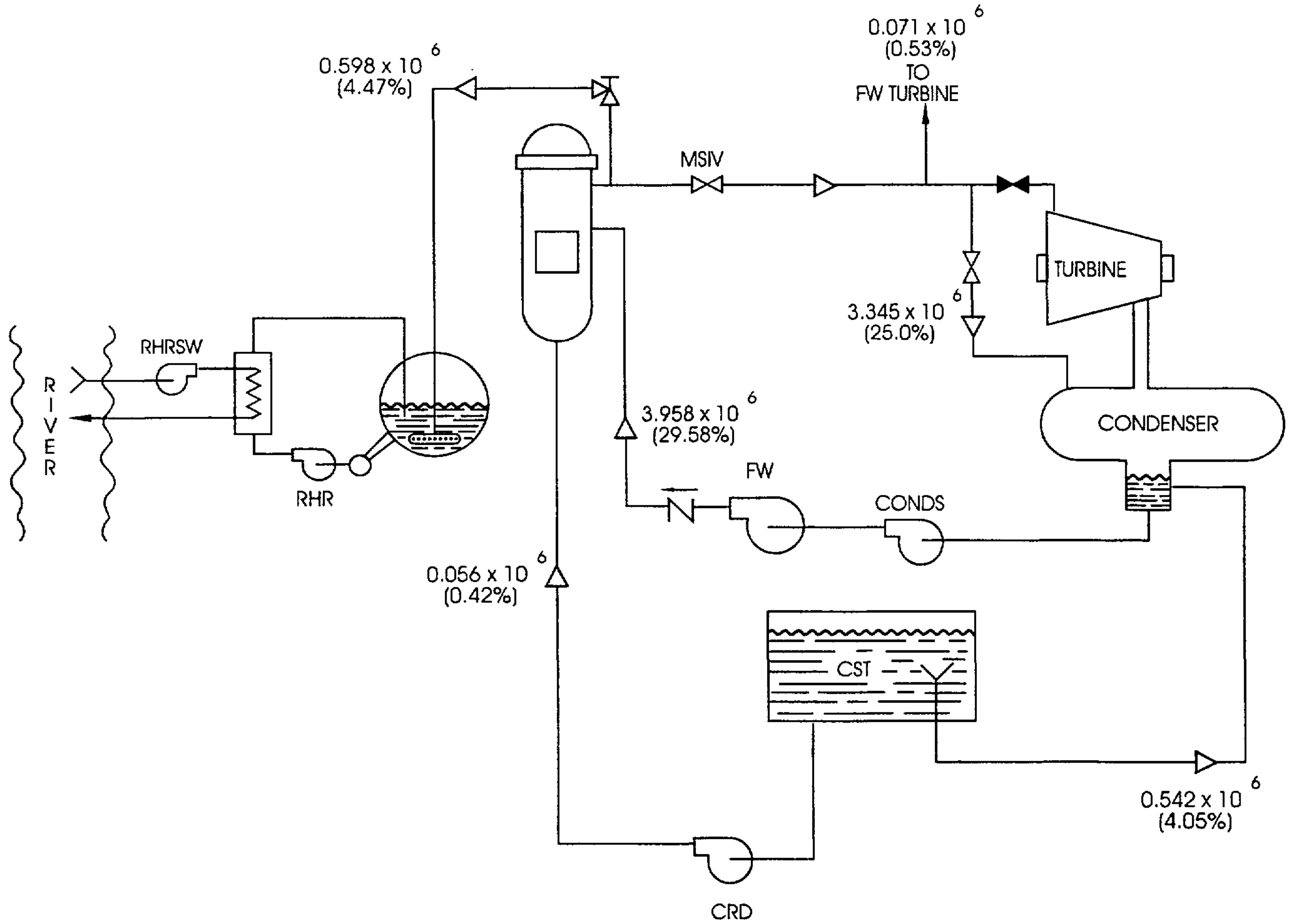


Figure 2B-1 BWR operation after failure of scram in the turbine trip-initiated ATWS accident sequence (flows in lbs/hr)

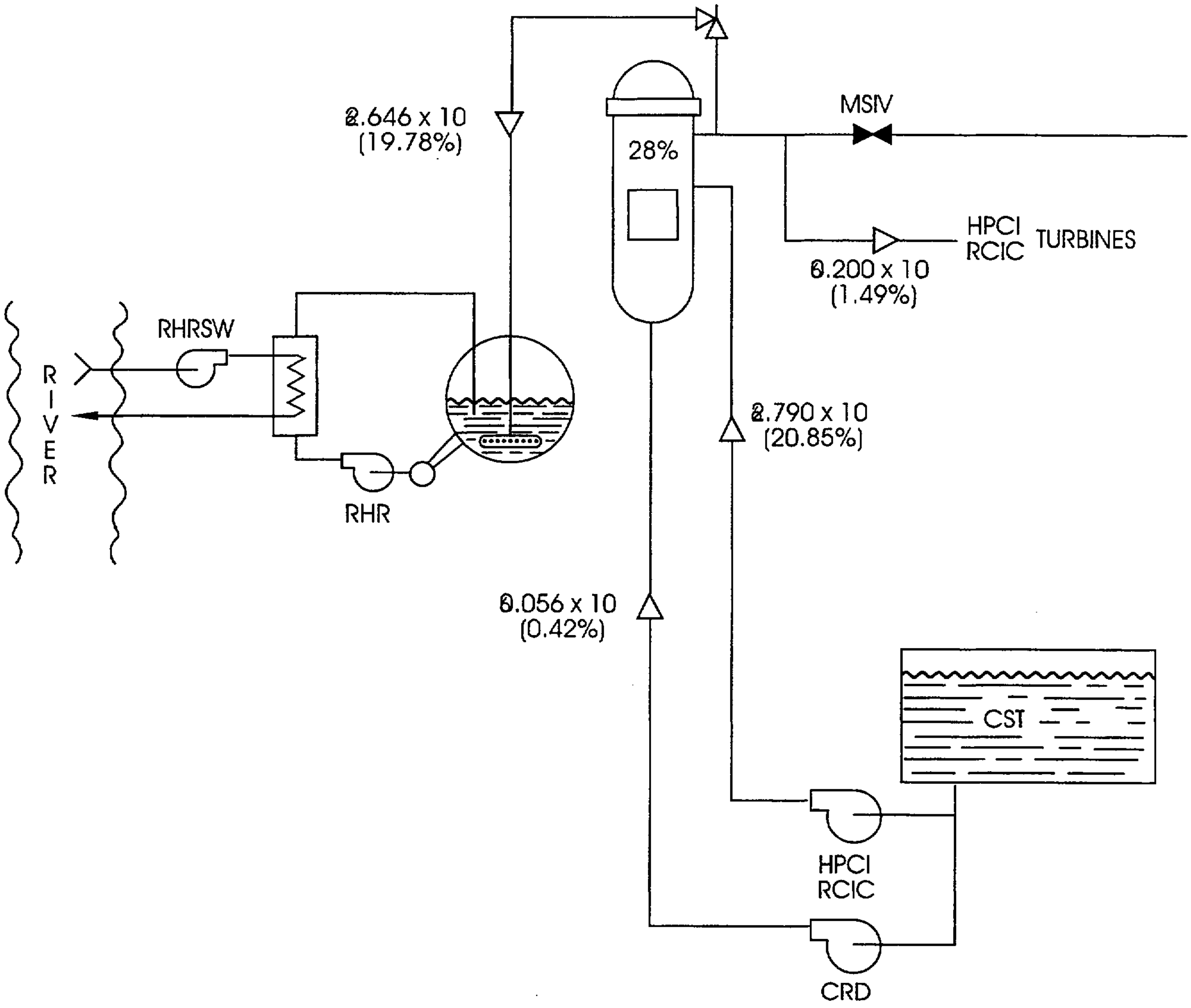


Figure 2B-2　BWR operation after failure to scram in the MSIV closure - initiated ATWS accident sequence (flows in lbs/hr)

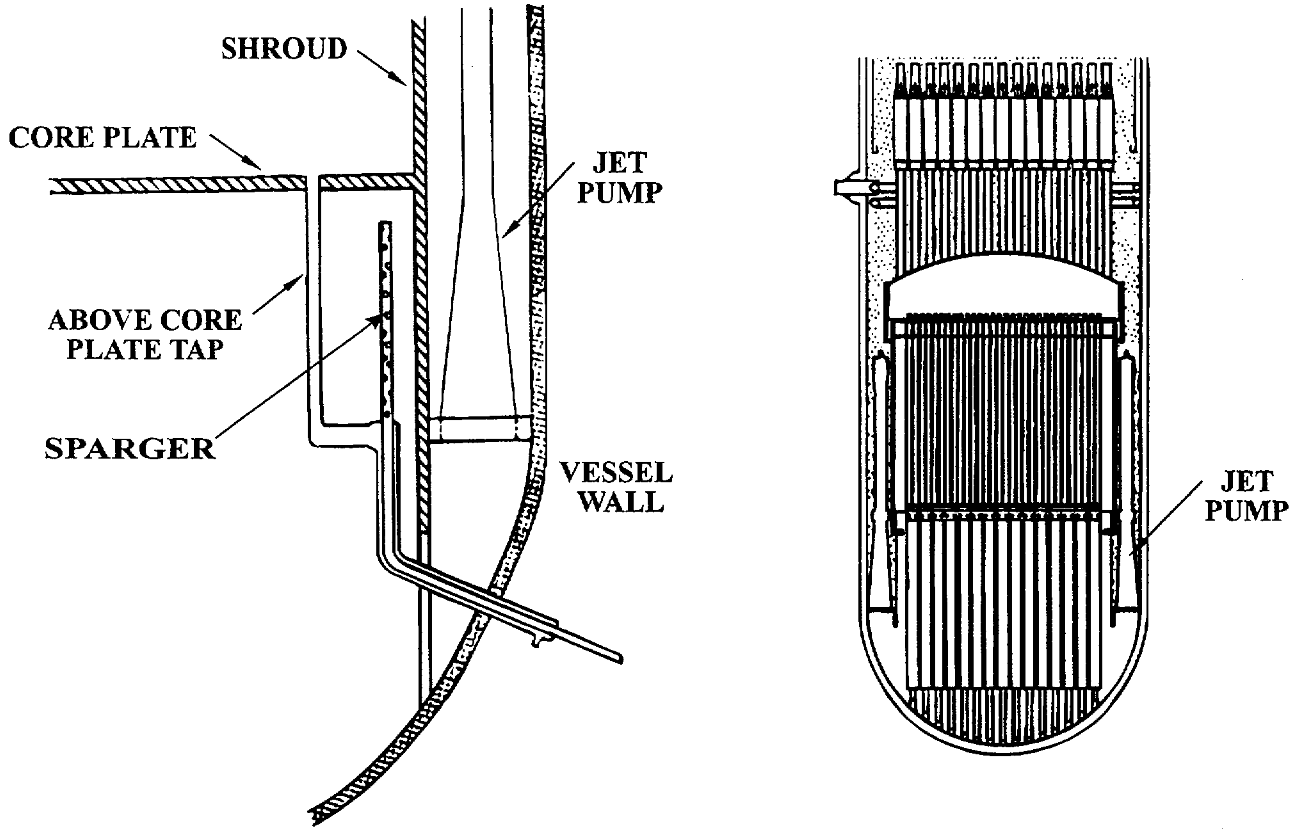


Figure 2B-3 **The single SLCS injection sparger is located to the side of the control rod guide tubes and injects horizontally into the lower plenum**

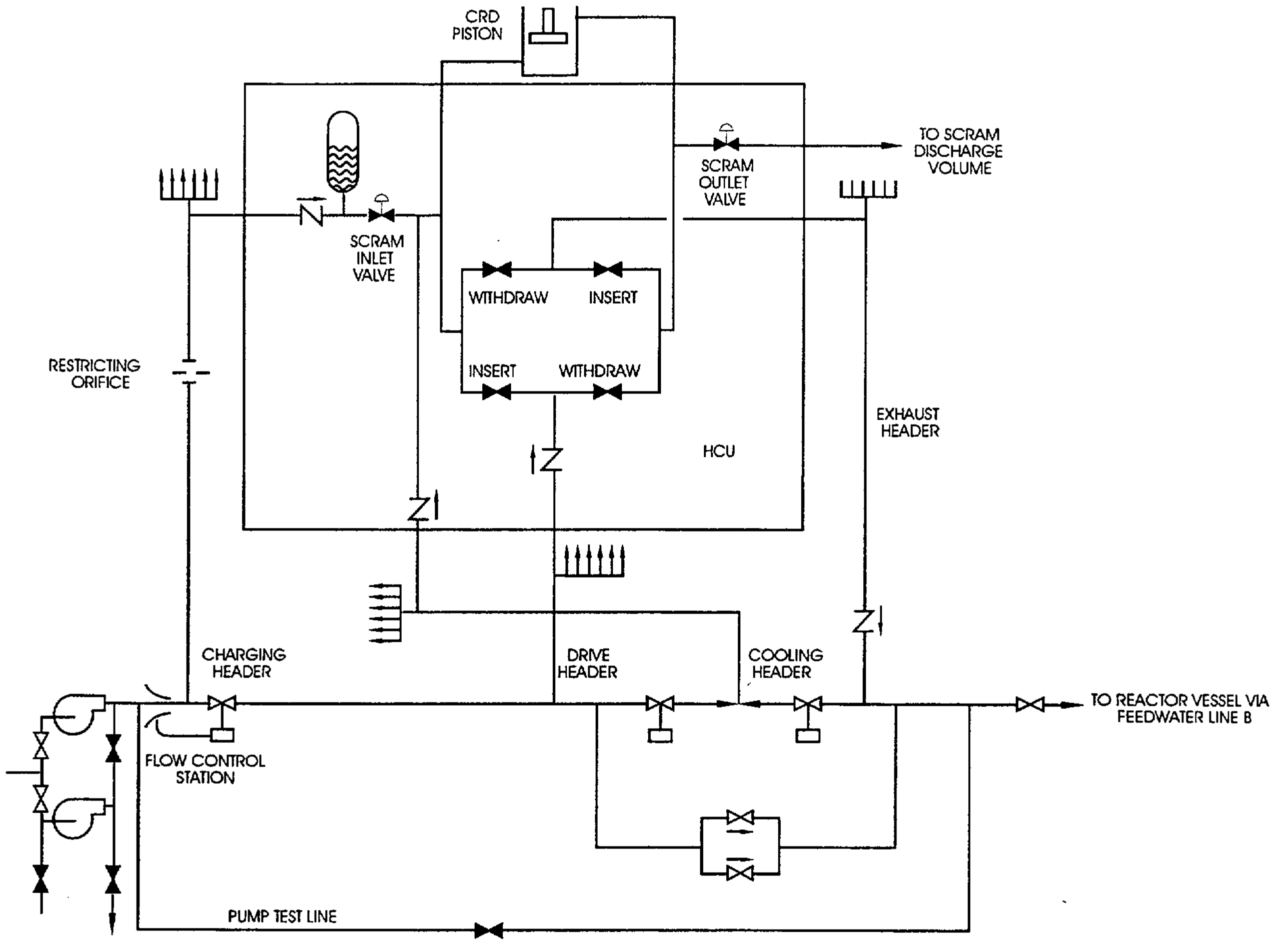


Figure 2B-4 **Manual rod insertion involves different piping and valves and might be effective even if scram has failed**

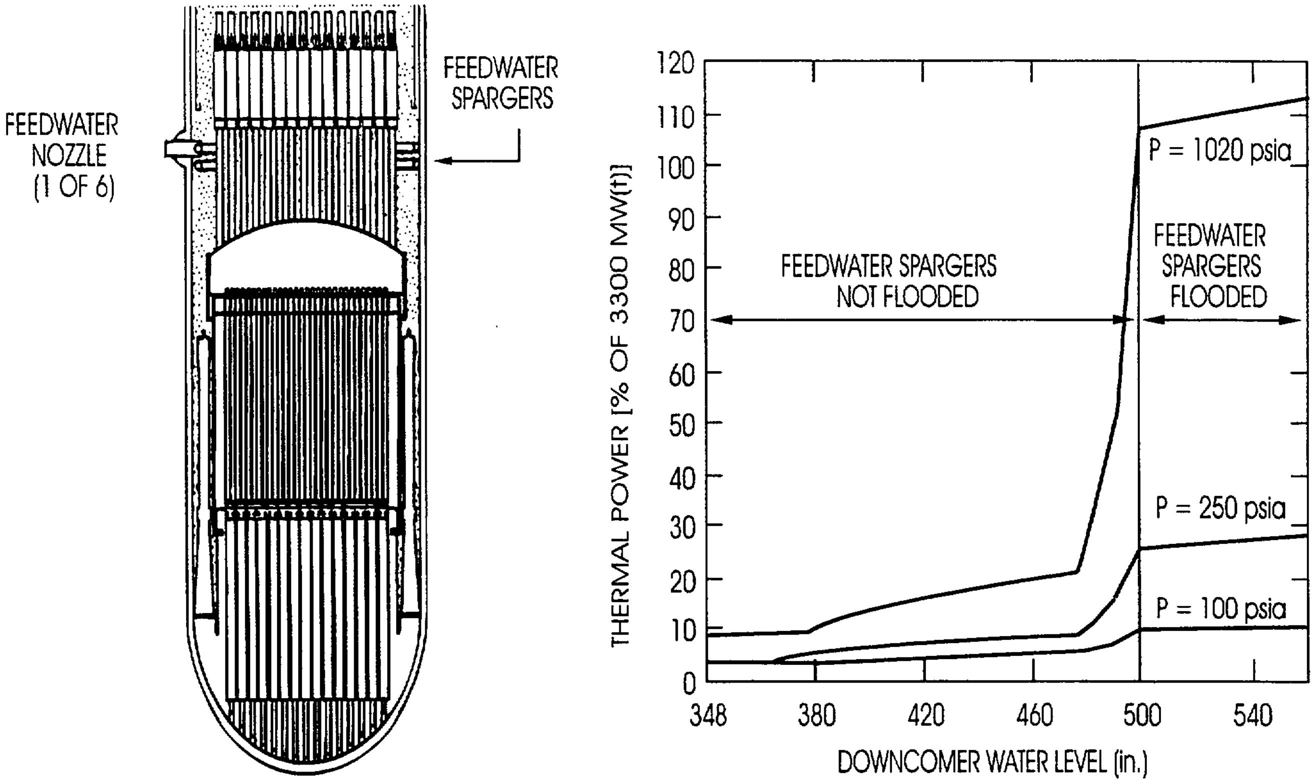


Figure 2B-5 The major effect of lowering the reactor vessel water level upon core power occurs when feedwater spargers are uncovered

References for Appendix 2B

1. U. S. Atomic Energy Commission Regulatory Staff, "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors," WASH-1270, September 1973.

2. U.S. Nuclear Regulatory Commission, Inspection and Enforcement Bulletin No. 83-01, "Failure of Reactor Trip Breakers (Westinghouse DB-50) to Open on Automatic Trip Signal," February 25, 1983.

3. U.S. Nuclear Regulatory Commission, "NRC Fact-Finding Task Force on the ATWS Events at Salem Nuclear Generating Station, Unit 1, on February 22 and 25, 1983," USNRC Report NUREG-0977, March 1983.

4. U.S. Nuclear Regulatory Commission, Inspection and Enforcement Bulletin No. 83-04, "Failure of the Undervoltage Trip Function of Reactor Trip Breakers," March 11, 1983.

5. Letter from Richard C. DeYoung, Director, NRC Office of Inspection and Enforcement, to Robert Smith, Chairman of the Board, Public Service and Gas Company, transmitting a Notice of Violation and Proposed Imposition of Civil Penalties, Docket Nos. 50-272 and 50-311, May 5, 1983.

6. U.S. Nuclear Regulatory Commission, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," NUREG-1000, Vol. 1, April 1983.

7. R. M. Harrington and S. A. Hodge, “ATWS at Browns Ferry Unit One - Accident Sequence Analysis,” Oak Ridge National Laboratory, NUREG/CR-3470, ORNL/TM-8902, July, 1984.

8. General Electric Company, “Assessment of BWR Mitigation of ATWS,” Volume II (NUREG-0460 Alternate No. 3), NEDO-24222, February 1981.

9. U. S. Nuclear Regulatory Commission, “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants,” NUREG-1150, Vol. 1, Final Summary Report, December 1990.

10. D. L. Kelly et al., “An Assessment of BWR Mark II Containment Challenges, Failure Modes, and Potential Improvements in Performance,” EG&G Idaho, Inc., Idaho National Engineering Laboratory, NUREG/CR-5528 (EGG-2593), July 1990.

11. Pennsylvania Power and Light Company, “Susquehanna Steam Electric Station Probabilistic Risk Assessment Report,” NPE 86-003, April 1986.

12. P. Saha, G. C. Slovik, and L. Y. Neymotin, “RAMONA-3B Calculations for Browns Ferry ATWS Study,” NUREG/CR-4739 (BNL-NUREG-52021), February 1987.

13. Safety Evaluation by the Office of Nuclear Reactor Regulation Relating to Amendment 17 General Electric Topical Report NEDE-24011-P, "General Electric Standard Application for Reactor Fuel," dated December 27, 1987.

14. S. A. Hodge, J. C. Cleveland, T. S. Kress, and M. Petek, "Identification and Assessment of BWR In-Vessel Strategies," Oak Ridge National Laboratory, NUREG/CR-5869, ORNL/TM-12080, October 1992.

15. General Electric Company, "BWR Owner's Group Emergency Procedure Guidelines," Revision 4, NEDO-31331, March 1987.

3.0 Accident Progression In The Reactor Vessel

3.0.1 Introduction

Given an accident sequence that leads to sustained uncovering of the core, the progression of core damage involves overheating of fuel; exothermic oxidation of the cladding with accompanying production of high temperature hydrogen gas; distortion and breach of the fuel cladding; melting of the cladding; fuel liquefaction; downward relocation of core materials; interactions between molten fuel and residual water in the reactor vessel; and breach of the reactor vessel accompanied by the discharge of molten core materials to the containment.

In-vessel processes are important for a number of reasons. The temperatures attained by fuel, cladding, and other core materials determine the releases of radionuclides from the fuel. The temperature and flow patterns of hot radioactive gases determine the potential for trapping and retention of radionuclides on surfaces within the reactor coolant system. Hydrogen gas produced in-vessel can escape to containment, where its combustion can pressurize and heat the containment. In-vessel processes determine the likelihood of arresting core degradation and radionuclide releases from fuel upon restoration of coolant. The melting and relocation of core materials in the reactor vessel, if unarrested by the restoration of coolant, can cause failure of the reactor vessel resulting in the discharge of hot core debris, radionuclides, and aerosols into containment, where they may interact with the containment atmosphere, water, and/or concrete. The characteristics of these discharges strongly affect the likelihood and timing of various containment failure modes and the magnitudes of radionuclide releases to the environment should containment fail.

3.0.2 Learning Objectives

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

1. List three energy sources that would be of concern in a severe accident.

2. Identify three conditions that must be achieved to arrest a severe accident.

3. Characterize the time intervals in which the following events would be expected in severe accidents involving complete failure of cooling water flow to the core.

   a. Core uncovering.
   b. Onset of zirconium oxidation
   c. Core relocation
   d. In-vessel molten-core-coolant interaction
   e. Failure of the lower head of the reactor pressure vessel

4. Indicate, for each pair of accident types below, the one that would proceed faster and explain why.

   a. Large LOCA versus small LOCA
   b. PWR transient versus comparable BWR transient
   c. Accident initiated at power versus one initiated at shutdown.

5. Explain what is meant by alpha-mode containment failure and indicate the currently perceived likelihood of such an event.

6. List at least one concern regarding the restoration of cooling water when molten core material is present in-vessel.

7. Describe the possible modes of bottom head failure and melt release to containment.

3.1 Introduction

3.1.1 In-Vessel Accident Stages

This chapter discusses in-vessel processes that strongly influence the severity and consequences of severe accidents. For the purpose of this discussion, in-vessel accident progression is divided into six successive stages, which commence with:

1. The initiating event and failures leading to inadequate core cooling.
2. The onset of sustained core uncovering, which leads to core heatup.
3. The onset of exothermic oxidation of cladding by steam, resulting in hydrogen production, cladding failure, and the release of gaseous fission products from the fuel-cladding gap.
4. The onset of clad melting and fuel liquefaction, which result in more substantial releases of radionuclides from the fuel.
5. Flow of molten material into the lower plenum of the reactor vessel, which may contain residual reactor coolant.
6. Failure of the reactor vessel lower head with consequent discharge of hot core debris into containment.

Each stage begins with a specific event and, as indicated in Table 3.1-1, gives rise to new processes, which can significantly alter the progression of the accident. The processes initiated in previous stages generally continue, so each stage is more complicated than its predecessor. The processes and factors determining their timing and impacts are introduced below and discussed by stage in Sections 3.2 through 3.6.

3.1.2 Severe Accidents Conditions

Over the years, computer code calculations have been extremely useful for forming and reinforcing engineering judgment regarding the progression of severe accidents; however, care must be taken in using and interpreting severe accident code calculations. It is not practical to perform the wide variety of experiments that would be required for complete validation of severe accident codes. Even given the years of severe accident research that followed the 1979 accident at Three Mile Island Unit 2, no computer code can calculate all major aspects of the accident.

Several factors contribute to the difficulty in modeling the in-vessel progression of severe accidents. As indicated in Table 3.1-2, an extremely broad spectrum of accident conditions may be encountered in such accidents. In addition, the behavior of a wide variety of materials at elevated temperatures must be modeled. Figures 3.1-2 and 3.1-3 illustrate the wide range of melt and boiling temperatures for elements, alloys, fuel, and fission products. Figure 3.1-4 indicates the chemical interactions and liquid phases that can form in LWR cores with increasing temperature.[1] Finally, chemical reactions, phase changes, and movement of both particulate and molten debris would significantly change the configuration of core materials during a severe accident. As a result, modeling uncertainties tend to increase as the accident progresses.

Accordingly, rather than display a plethora of code calculations, a general discussion of in-vessel processes and their potential implications is presented in this Chapter.

3.1.3 Factors Influencing Timing

In spite of uncertainties encountered in modeling severe accidents, some factors are known to have a strong influence on the timing of successive stages. These factors include a) the initiating and failure events that lead to core uncovering, b) the amount and timing of any coolant injection into the core region, and c) the pressure history within the reactor coolant system.

It should be evident from the variety of potential core damage accidents discussed in Chapter 2 that Stage 1, accident initiation, has an extremely wide range of durations. In a large-break loss-of-coolant accident, reactor coolant blowdown and pressure reduction occur very rapidly, and, if emergency core cooling systems fail on demand, Stage 1 has a very short duration. On the other hand, in many postulated accidents, the failure of coolant injection may take hours. For example, consider the BWR loss of suppression pool cooling accident first identified in the Reactor Safety Study. In this accident, the core is successfully cooled for approximately a full day before suppression pool heating causes overpressurization and failure of containment, which, in turn, results in suppression pool flashing and failure of core cooling systems.

A longer accident initiation stage is desirable because it provides more time for recovery actions that could prevent or arrest core damage. A longer accident initiation stage also results in a significant decreases in decay heat, so that, when core heatup begins, it occurs at a slower rate. As indicated in Figure 1.4-1, decay heat represents approximately 7% of operating core power but decreases rapidly after shutdown, reaching about 1% of operating core power at 24 hours.

Even limited amounts of coolant can have a significant impact on severe accident progression. For accidents involving boiloff (not rapid blowdown), injection flow of only a few hundred gallons of water per minute may suffice to keep the core of a 3300 MWt plant covered.[2] In BWRs, residual water in the reactor vessel can be used to steam cool the core for a brief period of time (Section 3.7.2.2). Finally, if coolant injection capability is recovered after the onset of core damage, it may be possible to arrest the damage within the reactor vessel and prevent the discharge of molten core debris to containment. Reflooding during a severe accident is discussed further in Section 3.1.5.

Accidents generally proceed faster at higher pressures because less energy is required to evaporate a given mass of reactor coolant. The discussions of in-vessel stages in Sections 3.2 through 3.6 generally focus on high-pressure PWR accidents, but the impact of lower pressures and the potential for temperature-induced failures of the reactor coolant system pressure boundary are specifically considered. The discussions generally presume that reactor shutdown (scram) successfully terminates the fission process, so that decay heat drives the core-damage process. Processes discussed in the context of pressurized, decay-heat driven PWR accidents would also occur in depressurized, ATWS, and BWR accidents; however, their timing and impacts could be significantly different. The in-vessel progression of BWR accidents is specifically discussed in Section 3.7.

Table 3.1-1 and Figure 3.1-4 indicate temperature intervals and processes associated with the successive in-vessel accident stages. Ranges of the stage durations are also indicated for PWR accidents in which early failure of coolant injection causes the onset of sustained core uncovering (Stage 2) to occur within about two hours of reactor shutdown. The indicated stage durations provide a baseline for the discussions of in-vessel processes in Sections 3.2 through 3.6. If there is partial injection of core coolant (as there was at TMI-2) or if the core uncovering is delayed for many hours (allowing decay power to decrease) the accident stages can take significantly longer than indicated in Table 3.1-1 and Figure 3.1-4. BWR accidents tend to progress more slowly than corresponding PWR accidents due to a number of factors including lower pressure, smaller core power density, and larger masses of water and structural materials below the active core region.

3.1.4 Review of Selected Design Features

The student is presumed to be familiar with the general design features of both BWRs and PWRs. The purpose of this subsection is to review, with the aid of figures, design features that can significantly influence the in-vessel progression of severe accidents, particularly features that differ markedly between BWRs (Figures 3.1-5 to 3.1-7) and PWRs (Figures 3.1-8 to 3.1-11).

As shown in Figure 3.1-5, BWRs have massive steam separators and dryers above the core region. This is not the case for PWRs in which the reactor coolant is subcooled during normal operation and steam is produced in the steam generators (Figure 3.1-8).

BWR fuel assemblies have outer Zircaloy flow channels (Figure 3.1-6) that prevent coolant flow between assemblies. PWR fuel assemblies, on the other hand, have no surrounding flow channels, so there is coolant mixing between assemblies (Figure 3.1-9).

BWRs have cruciform control blades (Figure 3.1-7) that enter from the bottom (Figure 3.1-5). PWRs have rod cluster control assemblies (Figure 3.1-10) that enter from the top (Figure 3.1-8). As a result, BWRs have a forest of control rod drives and guide tubes in the lower plenums of their reactor vessels, whereas PWRs have only secondary support assemblies (Figure 3.1-9). Westinghouse and Babcock & Wilcox plants also have bottom-entry in-core instruments and guide tubes (Figure 3.1-11).

BWRs operate at about 1000 psia whereas the PWRs operate at about 2200 psia. BWRs have larger pressure vessels to accommodate their steam separators and dryers and their lower power densities (51-56 versus 95-105 W/liter). Finally, BWRs cores contain roughly three times as much Zircaloy as comparable PWR cores, mainly because of the fuel assembly channel box walls. Special considerations for BWR facilities under severe accident conditions are discussed in Section 3.7.

3.1.5 Reflooding During Accident Progression

The reintroduction of coolant into a damaged core occurred at TMI-2, and is likely in some postulated accidents, for example, when lost electrical power is restored. If water is reintroduced early enough, the configuration of the fuel rods would differ little from the original geometry, and the temperatures of the fuel and cladding would be only slightly above operating levels. Cooling of the core under these conditions is reasonably assured. In Sections 3.2 through 3.6, each in-vessel stage of accident progression is first discussed under the presumption that adequate cooling is not restored. The potential for arresting core damage during each stage is then discussed.

Core damage can only be terminated when three conditions are satisfied:

1. Water must be continuously available to the core or core debris in quantities sufficient to quench the material and remove decay heat and heat associated with metal-water reactions.

2. The core or core debris configuration must be coolable.

3. Means must be available for cooling the water or condensing the steam produced.

Figure 3.1-12 is a functional event tree which shows the outcomes obtained by meeting all three termination conditions at various stages of core damage either in the reactor vessel or in containment.[3] Water could be delivered in-vessel by normal or emergency coolant supply systems. Water could be delivered ex-vessel by containment sprays or by normal or emergency coolant supply systems with coolant entering the vessel but flowing out of the opening in the lower head into the reactor cavity. Possible heat sinks include steam generators, the suppression pool and suppression pool cooling system, residual heat removal systems, and containment heat removal systems (fan coolers or spray recirculation systems).

If adequate coolant injection is reestablished early enough to prevent melting, the core geometry would still be coolable and releases would be limited to activity in the fuel-clad gap (Outcome 1). To reestablish coolant injection and arrest core damage in-vessel after the onset of melting (Outcome 2), the resulting core debris configuration would still have to be coolable, perhaps with some debris in the lower head as at TMI-2. Coolability of core debris discharged to containment (Outcomes 3 and 6 in Figure 3.1-12) is discussed in Chapter 4.

If some, but not all, of the necessary termination conditions can be met, the accident progression can be delayed. For example, partial coolant injection flow can be used to delay the onset of cladding oxidation. Similarly, if only a limited amount of water can be supplied to a coolable debris configuration, the accident progression may be delayed until the water supply is exhausted (Outcomes 5 and 8 in Figure 3.1-12).

Table 3.1-1 In-vessel accident stages

Stage	Starting Condition	Description	PWR Durations, No-Injection*	Section
1	Accident Initiator	Initiation	0-90 min	3.1
2	Core uncovering begins	Core uncovering and heatup	5-35 min	3.2
3	Hottest cladding reaches 1832°F (1273 K, 1000°C)	Cladding oxidation, melting of structural and control materials	5-10 min	3.3
4	Hottest cladding reaches its melt temperature, 3200°F (2033 K, 1760°C)	Clad melting, fuel liquefaction, holdup in core region	10-30 min	3.4
5	Core materials first enter lower plenum	Core slumping, quenching, reheating	0-80 min	3.5 & 3.6
6	Vessel Breach	Vessel breach and materials discharge to containment	--	3.5, 3.6, 4.3, 4.4, & 4.5

*Approximate duration ranges for PWR accidents with total failure of coolant injection

Table 3.1-2 Severe Accident Conditions

Pressure Range	15 - 2500 psia	(0.1 - 17 MPa)
Decay Power Level	0.5- 5 %	
Local Heatup Rates	1.3 - 18°F/s	(0.7 - 10 K/s)
Steam Flow Rates	0 - 6,600 $lb_m/ft^2/hr$	(0 - 9 $kg/m^2/s$)
Maximum Midcore Steam Superheat	> 3600°F	(> 2273 K, 2000°C)
Maximum Fuel Temperature	> 5180°F	(> 3133 K, 2860°C)

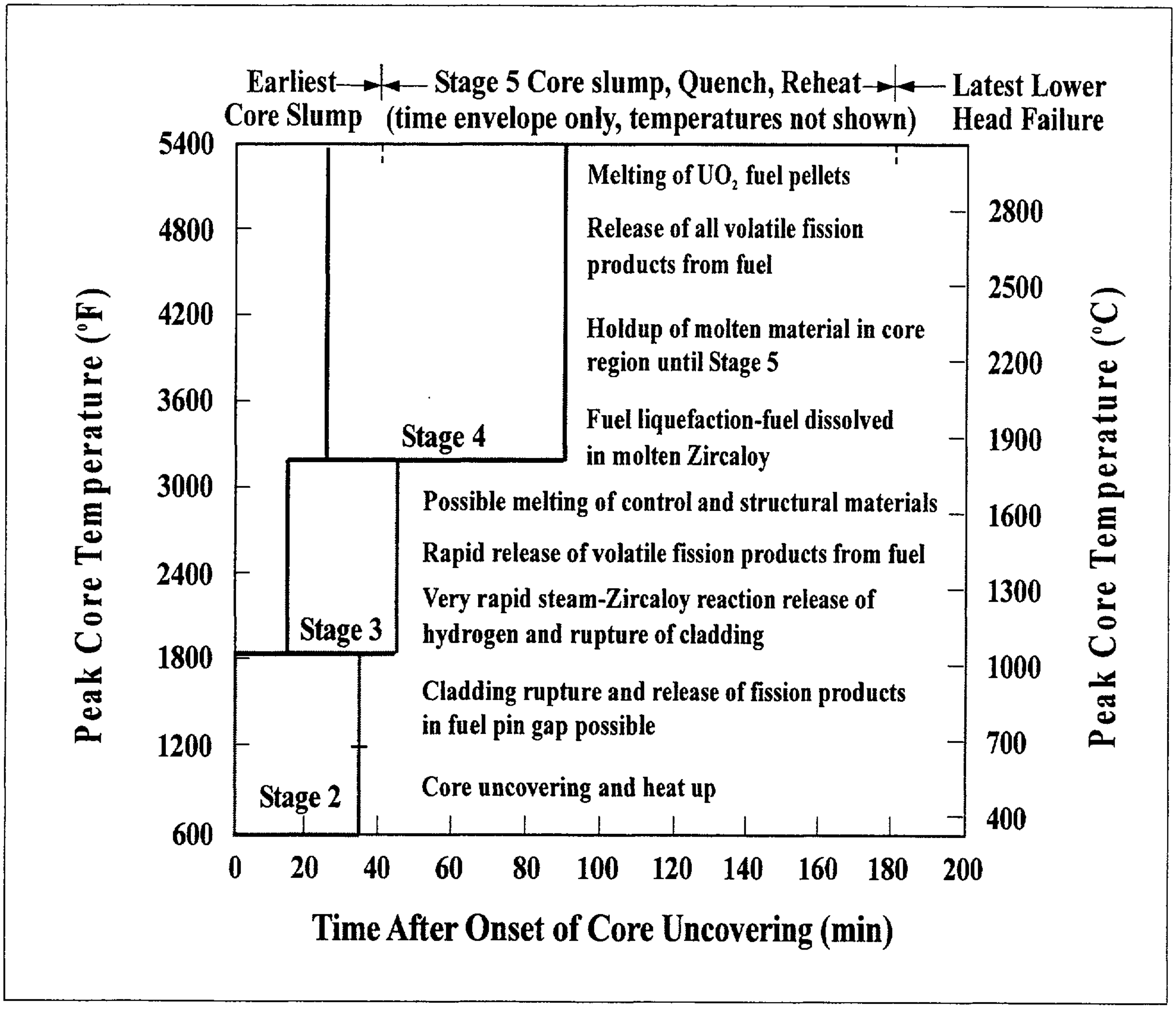


Figure 3.1-1 Approximate temperature and time envelopes for in-vessel severe accident stages assuming no coolant injection during PWR core heatup and degradation.

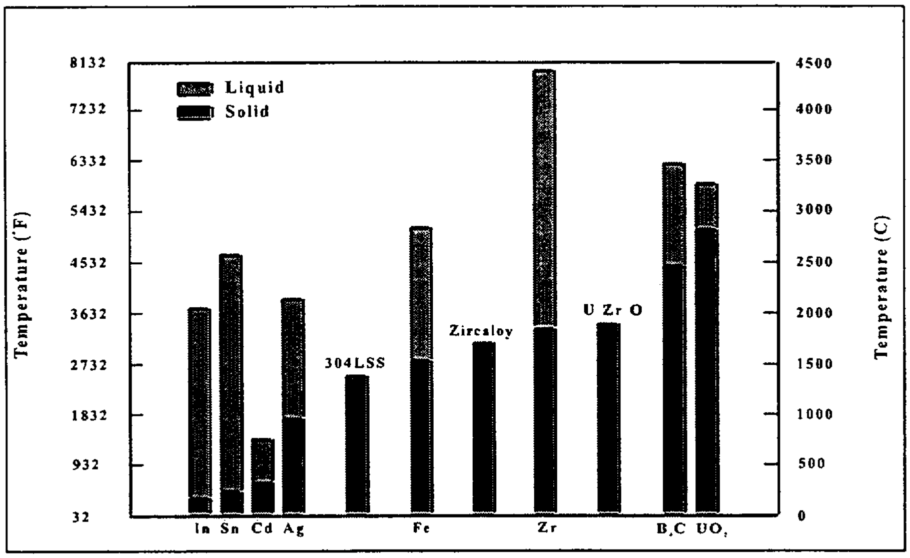


Figure 3.1-2 Melting points for metallic elements, reactor metals, and compounds

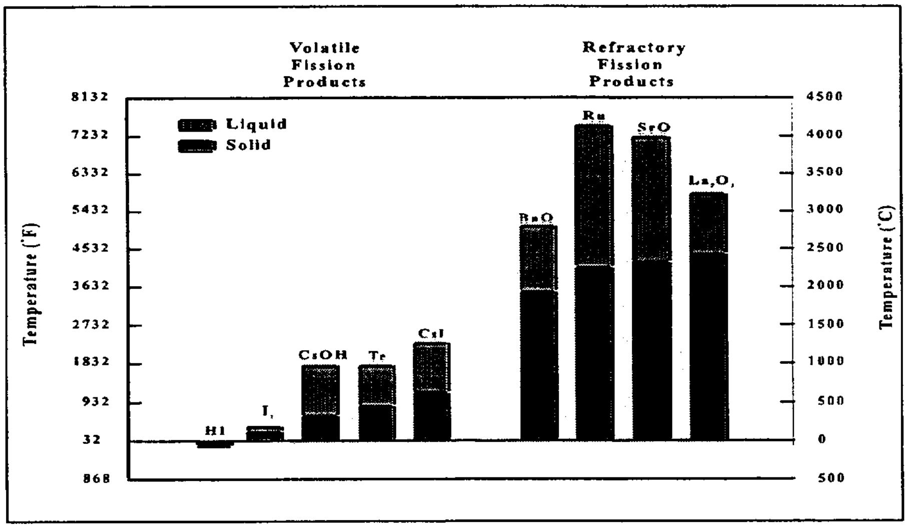


Figure 3.1-3 Melting and boiling points for fission products.

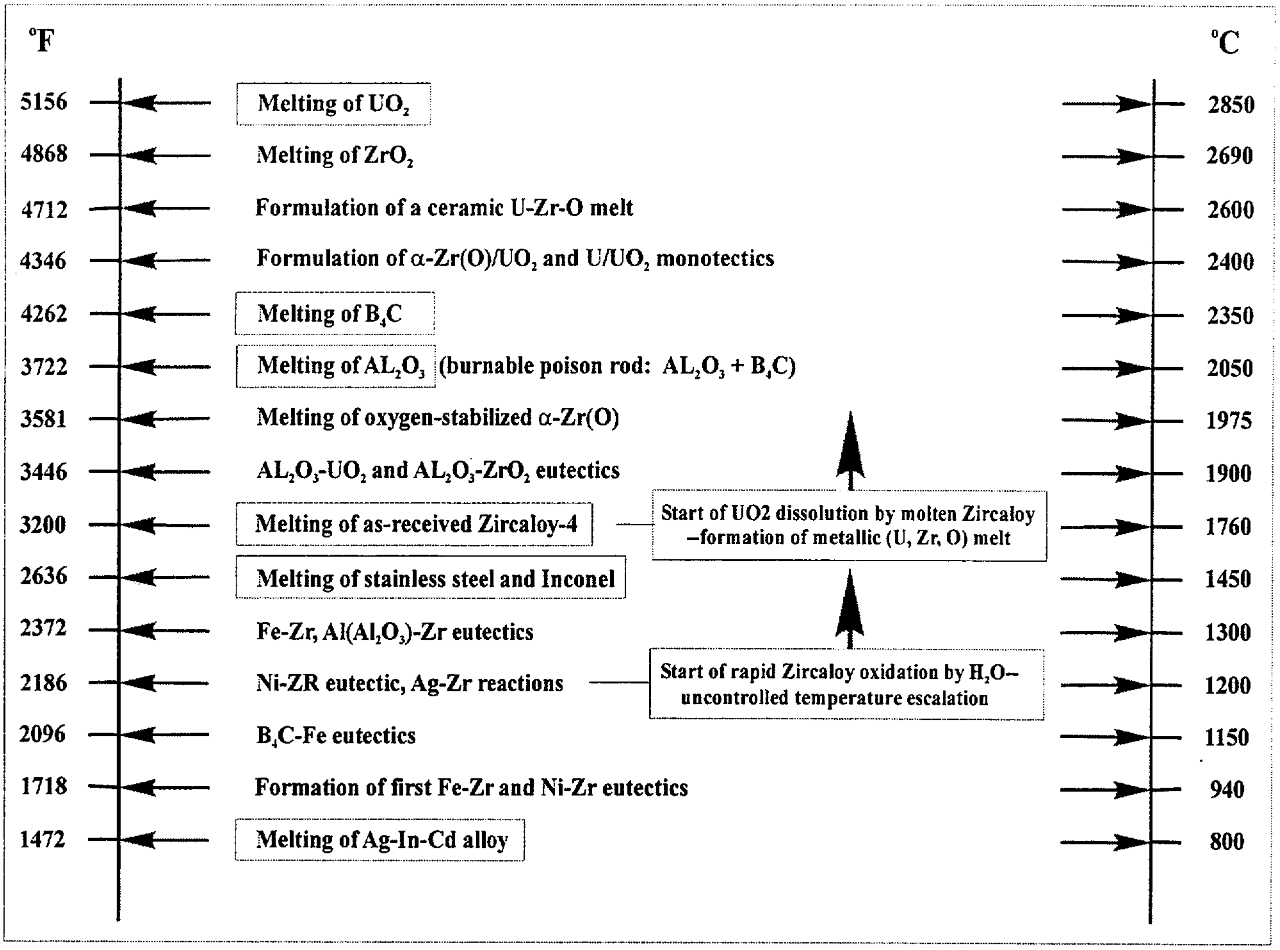

°F
°C
5156
Melting of UO_2
2850
4868
Melting of ZrO_2
2690
4712
Formulation of a ceramic U-Zr-O melt
2600
4346
Formulation of α-Zr(O)/UO_2 and U/UO_2 monotectics
2400
4262
Melting of B_4C
2350
3722
Melting of AL_2O_3 (burnable poison rod: AL_2O_3 + B_4C)
2050
3581
Melting of oxygen-stabilized α-Zr(O)
1975
3446
AL_2O_3-UO_2 and AL_2O_3-ZrO_2 eutectics
1900
3200
Melting of as-received Zircaloy-4
Start of UO2 dissolution by molten Zircaloy –formation of metallic (U, Zr, O) melt
1760
2636
Melting of stainless steel and Inconel
1450
2372
Fe-Zr, Al(Al_2O_3)-Zr eutectics
1300
2186
Ni-ZR eutectic, Ag-Zr reactions
Start of rapid Zircaloy oxidation by H_2O– uncontrolled temperature escalation
1200
2096
B_4C-Fe eutectics
1150
1718
Formation of first Fe-Zr and Ni-Zr eutectics
940
1472
Melting of Ag-In-Cd alloy
800

Figure 3.1-4 Chemical interactions and formation of liquid phases in an LWR fuel rod bundle with increasing temperature

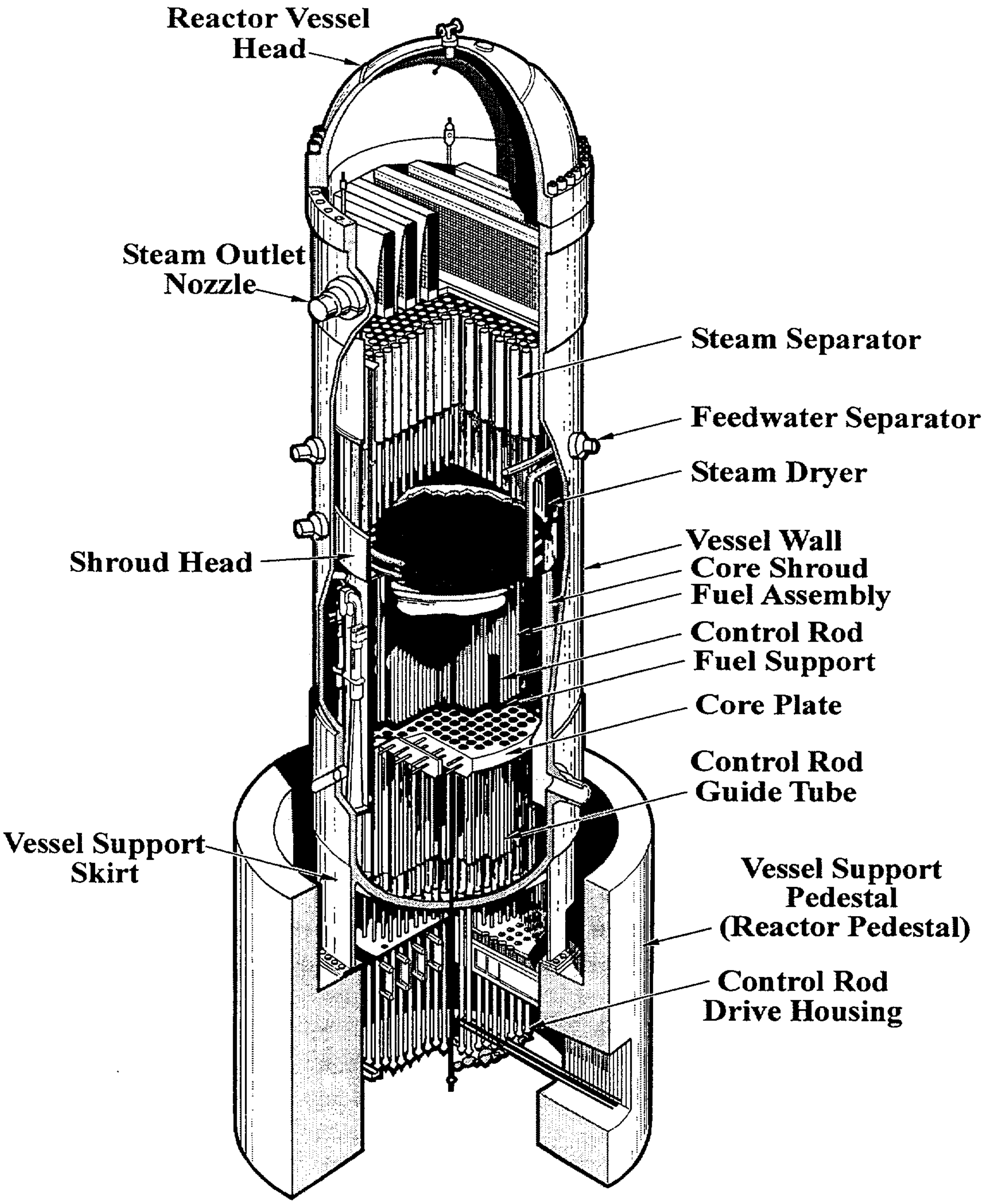


Figure 3.1-5 Schematic of BWR reactor vessel internal structure

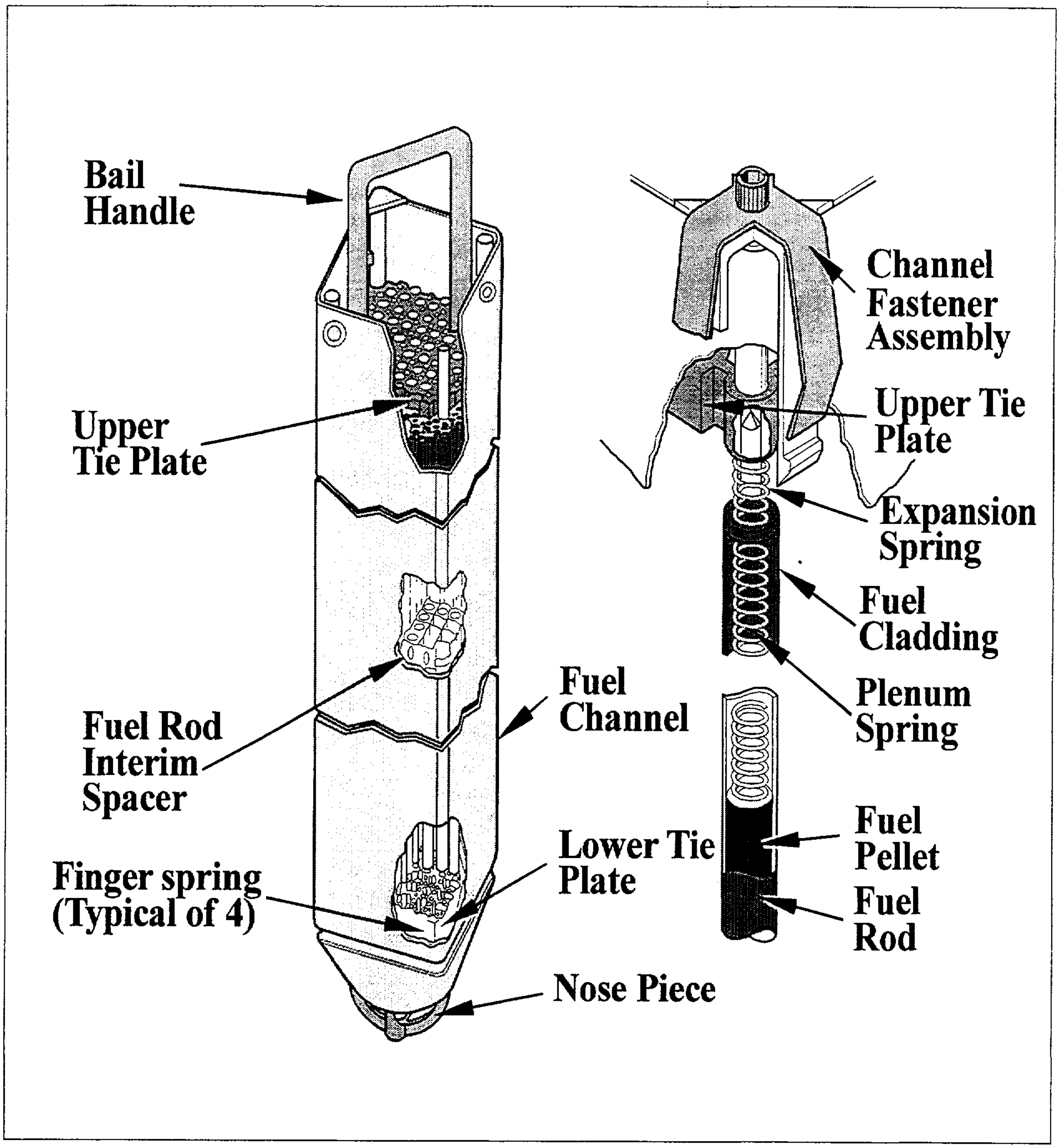


Figure 3.1-6 BWR fuel assembly

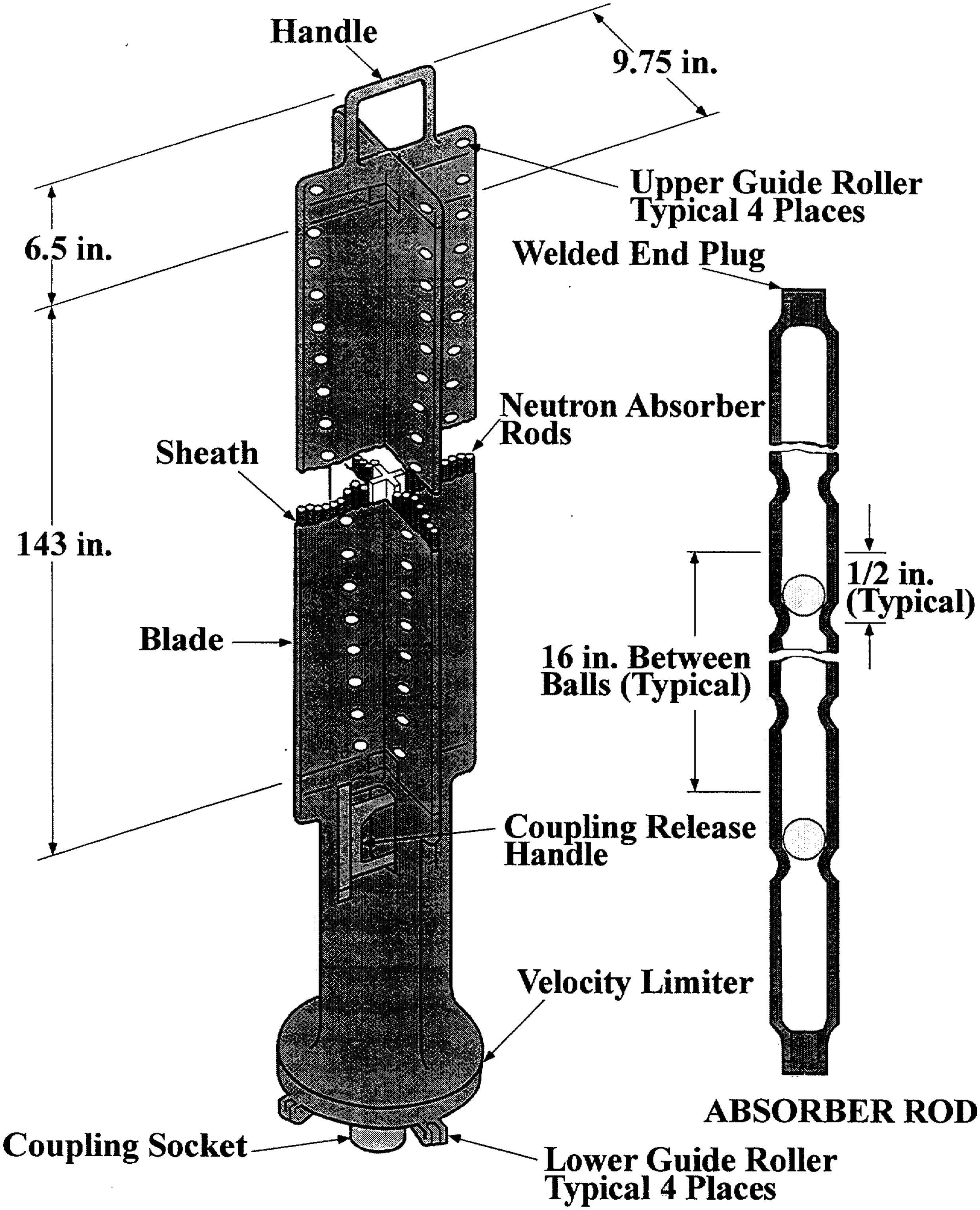


Figure 3.1-7 BWR control rod

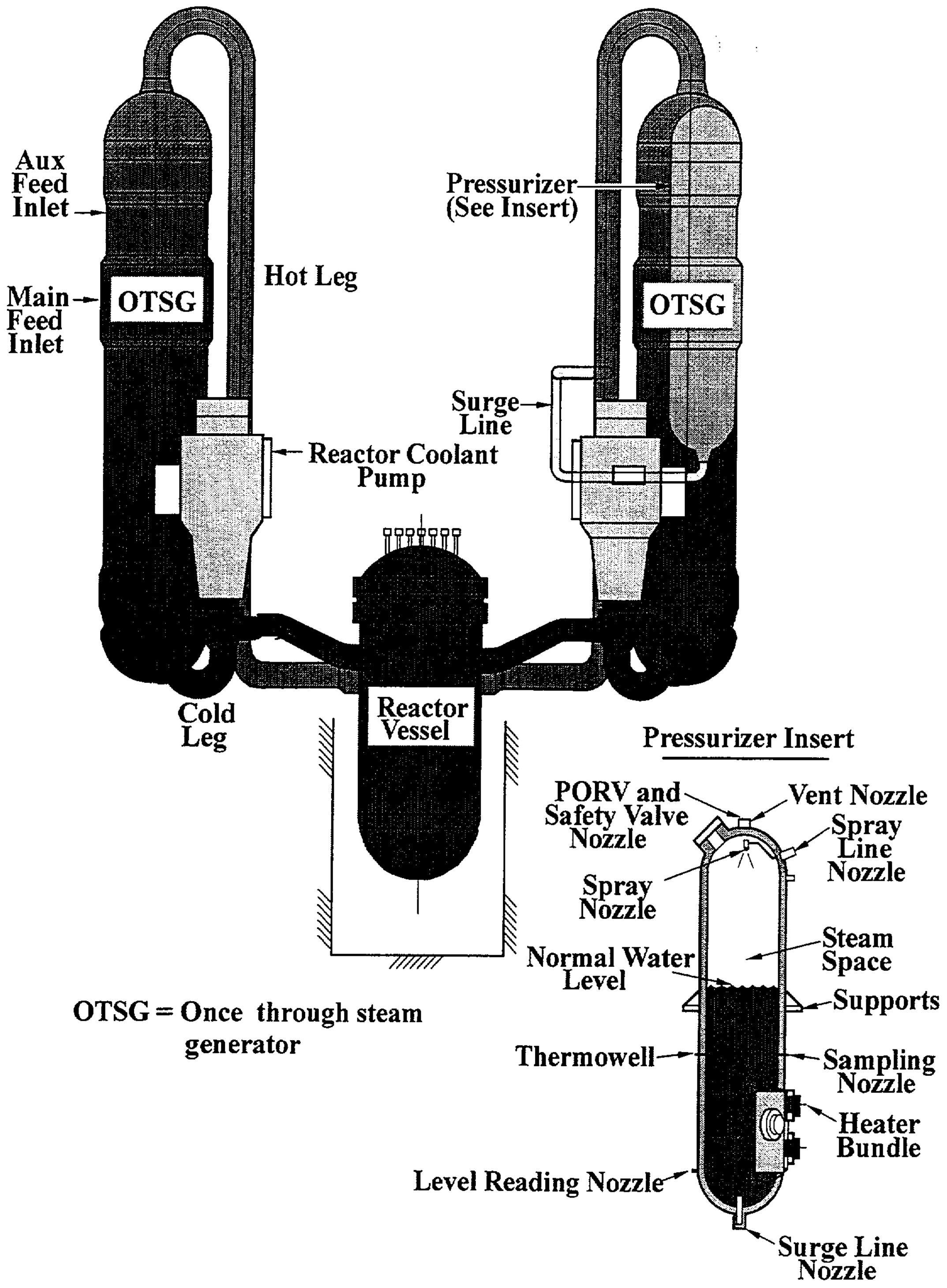


Figure 3.1-8 PWR reactor coolant system arrangement (B&W)

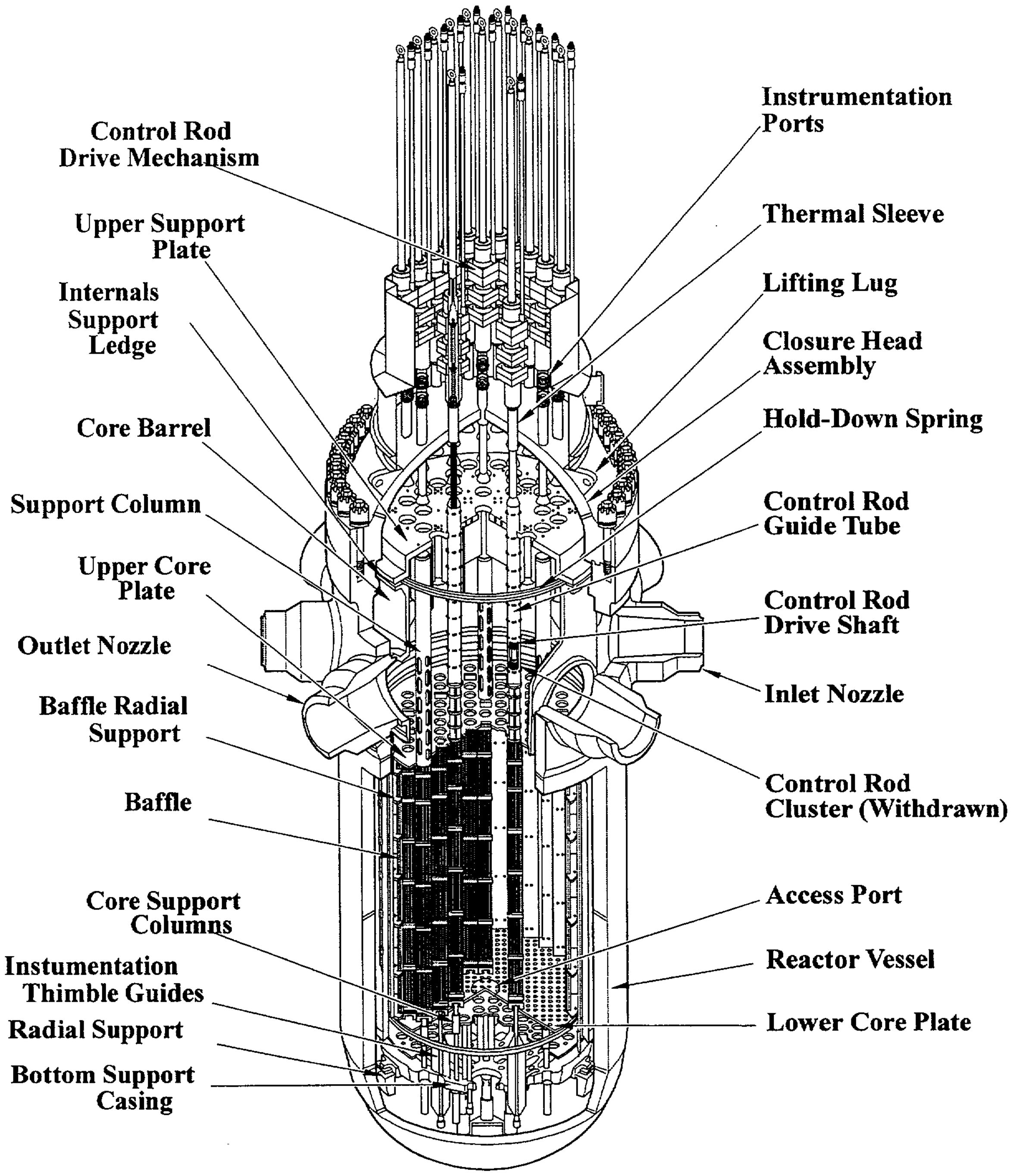


Figure 3.1-9 PWR reactor vessel internals (Westinghouse)

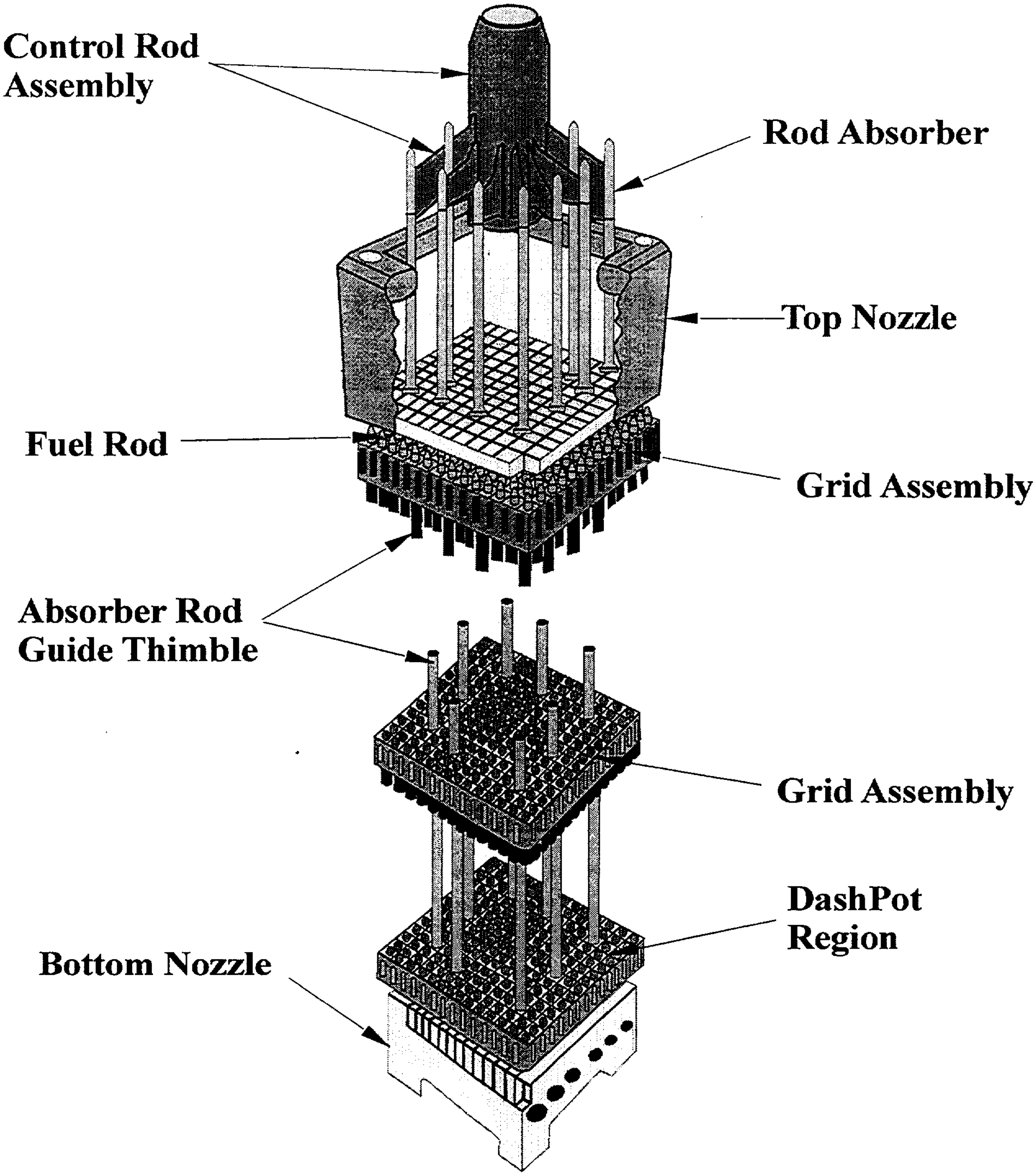


Figure 3.1-10 Cutaway view of typical rod cluster control assembly

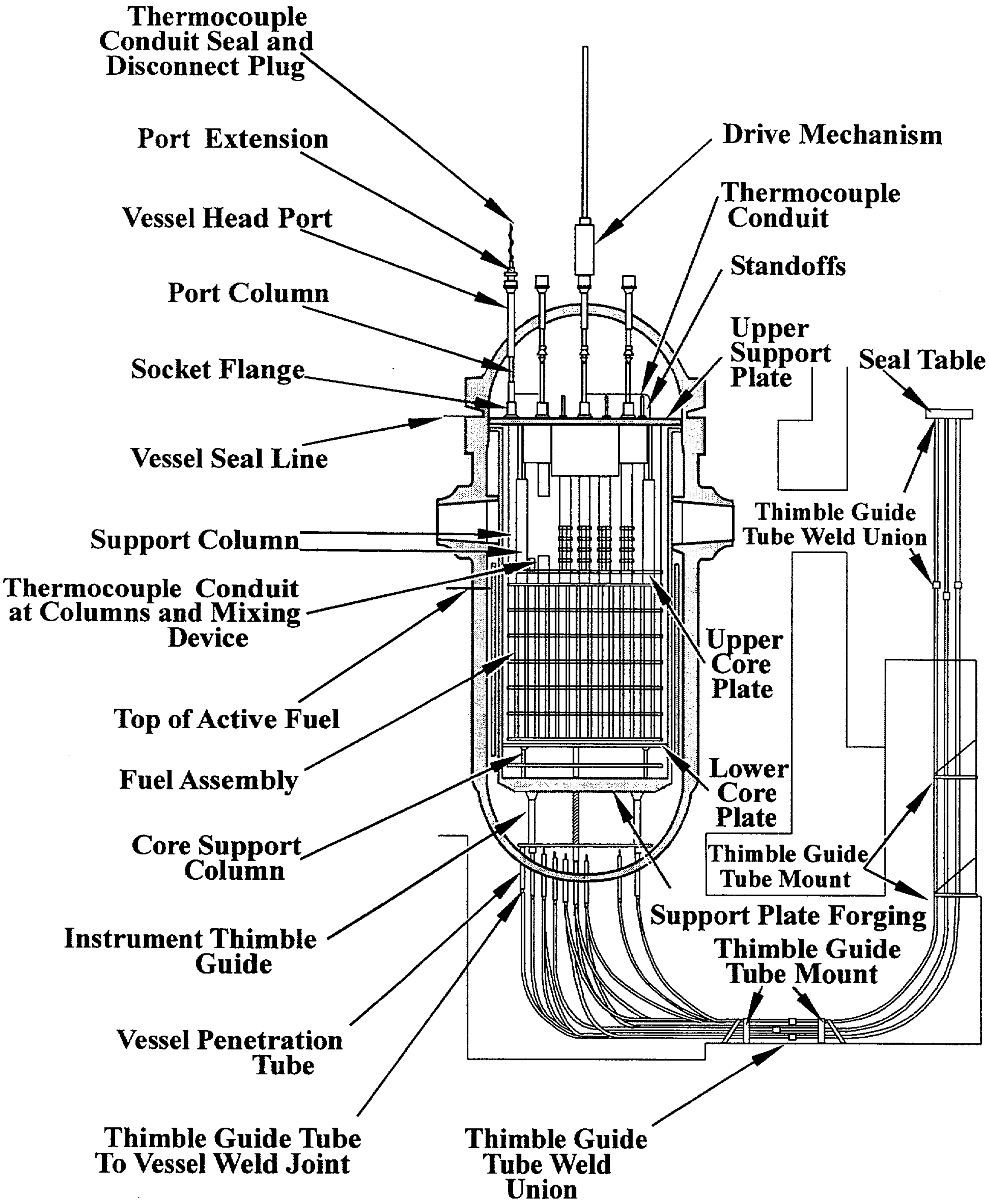


Figure 3.1-11 Typical PWR arrangement for in-core instrumentation (Westinghouse)

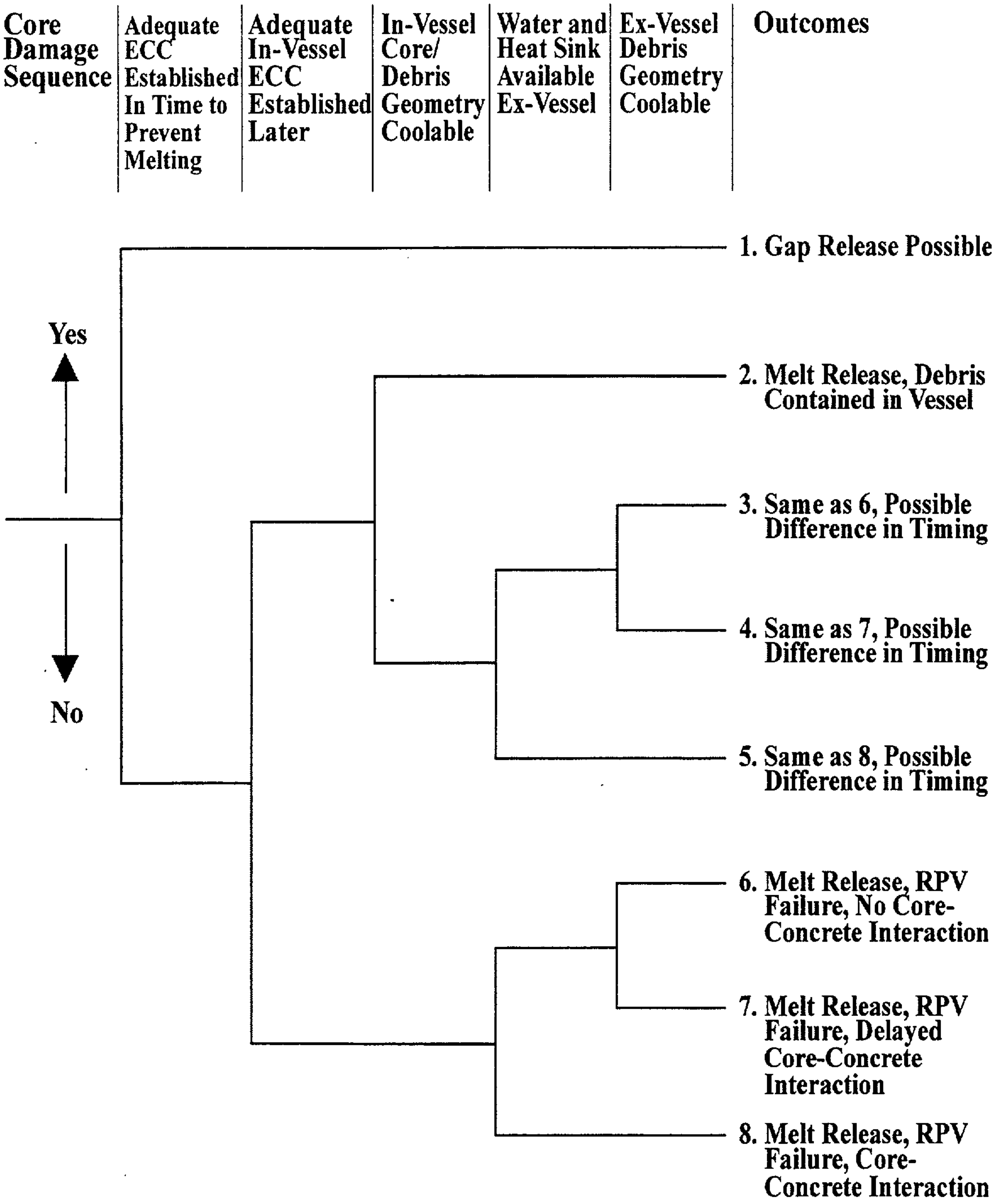

Core Damage Sequence
Adequate ECC Established In Time to Prevent Melting
Adequate In-Vessel ECC Established Later
In-Vessel Core/ Debris Geometry Coolable
Water and Heat Sink Available Ex-Vessel
Ex-Vessel Debris Geometry Coolable
Outcomes
Yes
No
1. Gap Release Possible
2. Melt Release, Debris Contained in Vessel
3. Same as 6, Possible Difference in Timing
4. Same as 7, Possible Difference in Timing
5. Same as 8, Possible Difference in Timing
6. Melt Release, RPV Failure, No Core-Concrete Interaction
7. Melt Release, RPV Failure, Delayed Core-Concrete Interaction
8. Melt Release, RPV Failure, Core-Concrete Interaction

Figure 3.1-12 Core damage event tree

References for Section 3.1

1. P. Hofman, S.J.L. Hagen, G. Schanz, and A. Skokan, "Reactor Core Materials Interactions at Very High Temperatures," *Nuclear Technology*, **87**, August 1989, 147.

2. R. M. Harrington and L. J. Ott, "The Effect of Small-Capacity, High-Pressure Injection Systems on TQUV Sequences at Browns Ferry Unit One," U.S. Nuclear Regulatory Commission, NUREG/CR-3179, ORNL/TM-8635, September 1983.

3. F. E. Haskin, J. L. Darby, and W. B. Murfin, "Analysis of Hypothetical Severe Core Damage Accidents for the Zion Pressurized Water Reactor," U.S. Nuclear Regulatory Commission, NUREG/CR-1989, SAND81-0504, October 1982.

3.2 Core Uncovering and Heatup

Core heatup begins when the water level drops below the top of the active fuel as a result of boiloff. Before this time fuel temperatures are close to the system saturation temperature because there is very little heat transfer resistance between the fuel and liquid reactor coolant. So long as fuel remains submerged, it is not expected to be damaged due to high temperature.

3.2.1 Boiloff of Water in Core Region

During the uncovering of the core, the fraction of the core decay power that is utilized to vaporize water is reduced as the water level decreases. To a first approximation, all of the decay heat generated in the water-covered region results in evaporation, and the water level decreases exponentially with time.[1] In a PWR, sustained core uncovering begins when the water level reaches the top of the active core, the exponentially decreasing water level depicted in Figure 3.2-1 follows from the equation

$$L(t) = L(0)\ e^{-t/\tau} \qquad (3.2\text{-}1)$$

where

$L(t)$= water level above bottom of active core region at time t since the onset of core uncovering,

$L(0)$= water level at the beginning of core uncovering, for a PWR this is the height of the active core region Z (12 ft),

t = time since onset of core uncovering, and

τ = time constant for boiloff in core region, which is given by the equation

$$\tau = \frac{\rho A Z h_{fg}}{P_D} \qquad (3.2\text{-}2)$$

with

ρ = liquid density,

A = cross-sectional area of liquid in active core region,

h_{fg} = the energy required to evaporate a unit mass of saturated liquid, that is, the latent heat of vaporization, which decreases with increasing reactor coolant system pressure,

P_D = core decay power (approximated as constant during boiloff of water in the core region).

Given the exponentially decreasing water level associated with boiloff in the core region, it takes one time constant for the water level to decrease by a factor of e (from 12 to 4.4 ft) and another time constant for the water level to decrease by another factor of e (from 4.4 ft to 1.6 ft). It should be noted that the time constant for boiloff in the core region, τ, varies with the reactor coolant system pressure since both the density ρ and latent heat of vaporization h_{fg} vary with saturation pressure. Figure 3.2-2 depicts the change in τ with pressure for the Zion PWR at the decay power (32.5 MW) used in the following example. The total time duration for Stage 2, core uncovering and heatup, is approximately 2τ or, as noted in Table 3.1-1, 5 to 35 minutes depending on the reactor coolant system pressure.

Example 3.2-1 - Time Required for Boiloff in Core Region

In the Zion station blackout accident sequence, steam is discharged from the primary system at the relief valve set point of 2500 psig.[2] The active core height is 12 ft. The area of the core occupied by water is 53.4 ft^2. The core decay power during boiloff is approximately 32.5 MW. Estimate the time required for the water level to decrease from the top of the active core to the core midplane.

Solution:

Solving Eq. (3.2-1) for t and using Eq. (3.2-2) for τ gives

$$t = \frac{\rho A Z h_{fg}}{P_D} \ln\left(\frac{L(0)}{L(t)}\right) \qquad (3.2\text{-}3)$$

From the steam tables, for saturated water at 2515 psia,

$$h_{fg} = 357.0 \text{ Btu/lbm}$$
$$\rho = 34.83 \text{ lbm/ft}^3$$

Substituting:

$$t = \frac{(34.83\frac{lbm}{ft^3})\ (53.4\ ft^2)\ (12\ ft)\ (357.0\frac{Btu}{lbm})}{(32.5\ x\ 10^6\ \frac{J}{s})\ (\frac{Btu}{1055 J})} \ln(\frac{12}{6})$$

$$t = 258.7 \ln(2)\ s = 179.3\ s = 2.99 \text{ min}$$

A detailed treatment of the axial power distribution, local heat transfer, two-phase mixture dynamics, and coupling with the rest of the reactor coolant system requires the use of complex computer models. Figure 3.2-3 compares the predictions based on Eq. 3.2-1 with code calculations for a Zion station blackout scenario compounded by failure of turbine-driven auxiliary feedwater.[3] As indicated by the comparison, the exponentially decreasing function defined by Equations 3.2-1 and 3.2-2 is a reasonable approximation for the water level in the core region during this stage of the accident. This approximation is valid for about two time constants, which corresponds roughly to the onset of the next stage. Beyond this point, cladding oxidation and heat transfer from the uncovered region of the core to the residual water must be considered.

3.2.2 Initial Heatup of Uncovered Fuel

Because of low vapor flow rates, the cooling of fuel in the uncovered part of the core by the flow of steam generated during PWR boiloff is relatively ineffective. The temperature rise in the uncovered fuel during the boiloff and initial core heatup stage can, therefore, be approximated as an adiabatic absorption of fission-product decay energy. Using this approximation, the temperature *T(z,t)* at uncovered elevation *z* and time *t* is

$$T(z,t) = T(z,0) + \frac{ZP_D(z)}{mC_P}(t-t_{L=Z})$$

where

Z = height of active core region (ft)

mC_P = heat capacity of entire core, J/K (Btu/°F),

$P_D(z)$ = decay power per unit axial height at z above bottom of active core, MW/ft

$t_{L=Z}$ = time at which the water level in the core region equals z, seconds

Figure 3.2-3 compares the results of an adiabatic heatup calculation with code calculated core temperatures. The difference between the fuel temperature and the residual (saturated) water temperature is read on the horizontal axis. The axial position in the core is read on the vertical axis. Curves are shown for three successive times. The times are measured from the point when the water level reaches the top of the active fuel and divided by the characteristic boiloff time constant defined in Equation 3.2-2. The lower intercept of a curve with the vertical axis indicates the water level at that time. The adiabatic heatup approximation appears reasonable based on the comparisons with code calculations. This merely indicates that during this stage the temperature rises in the uncovered regions of the core are determined almost entirely by distribution of decay heat in the core. For a PWR at high pressure the saturation temperature would be about 650°F, and the peak temperature (650+1080=1730°F) with t/τ=1.58 would be approaching the 1832°F (1000°C) criterion for the onset of the next stage.

The simplifying assumptions used to develop the analytic approximations presented above break down near the start of the next stage, cladding oxidation, which occurs when the peak fuel temperature reaches about 1832°F (1000°C or 1273 K).

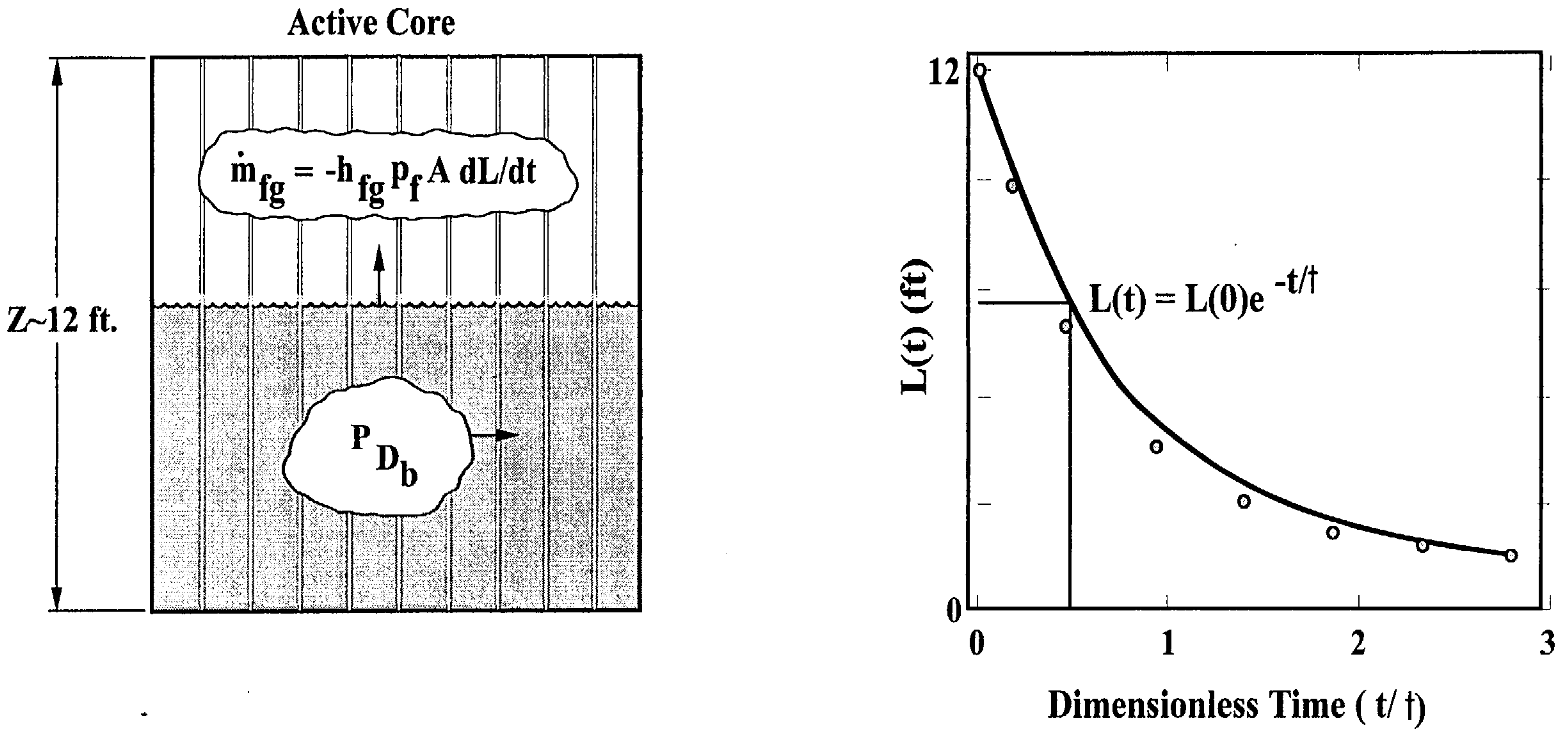


Figure 3.2-1 Exponentially decreasing water level

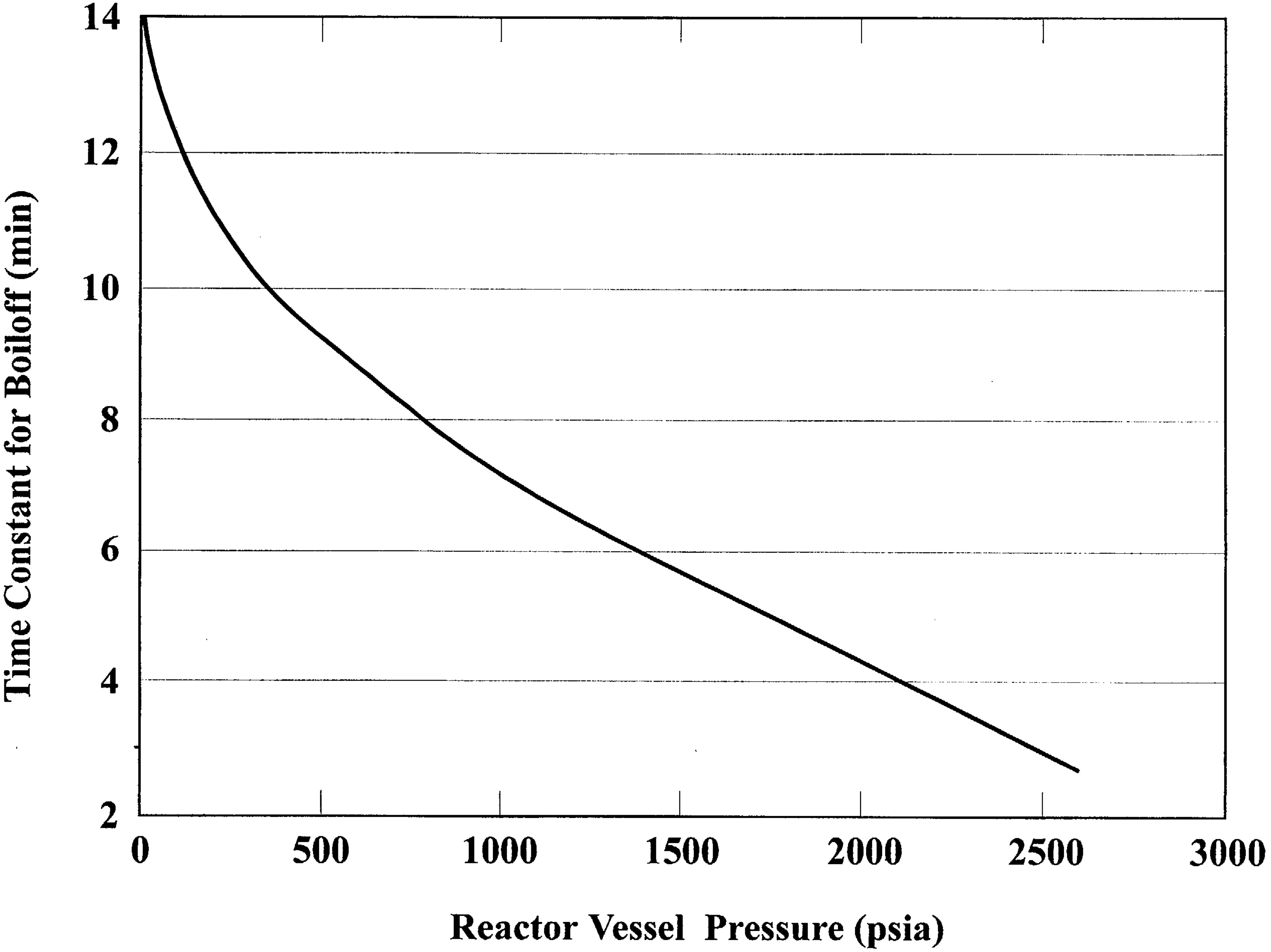


Figure 3.2-2 Variation of boiloff time constant with saturation pressure

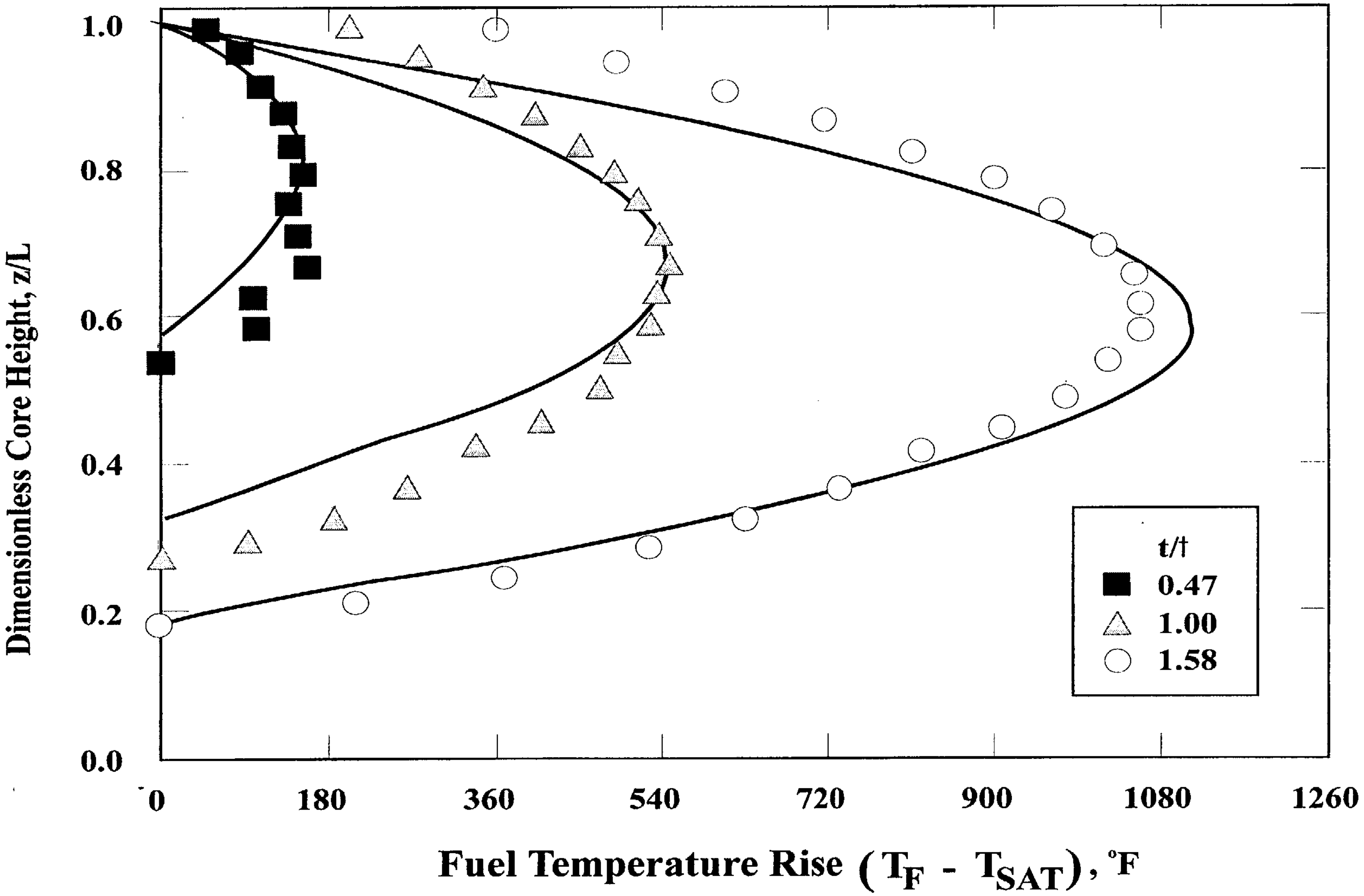


Figure 3.2-3 Approximate calculation of fuel temperature rise (curves) at three different times compared with code results

References for Section 3.2

1. J. B. Rivard and F. E. Haskin, "LWR Meltdown Analyses and Uncertainties," ANS/ENS Topical Meeting on Reactor Safety Aspects of Fuel Behavior, Sun Valley, Idaho, August 2-6, 1981.

2. F. Eric Haskin, Walter B. Murfin, Joseph B. Rivard, and John L. Darby, "Analysis of a Hypothetical Core Meltdown Accident Initiated by Loss of Offsite Power for the Zion 1 Pressurized Water Reactor," U.S. Nuclear Regulatory Commission, NUREG/CR-1988, SAND81-0503, November 1981.

3. J. B. Rivard, et al., "Interim Technical Assessment of the MARCH Code," U.S. Nuclear Regulatory Commission, NUREG/CR-2285, SAND81-1672, February 1981.

3.3 Cladding Oxidation

The start of Stage 3 (Table 3.1-1) is marked by the initiation of significant cladding oxidation, which occurs when the peak fuel temperature reaches about 1832°F (1273 K, 1000°C).[1] The chemical reaction is

$$Zr + 2H_2O \rightarrow ZrO_2 + 2H_2 \qquad (3.3\text{-}1)$$

This reaction is important because it is highly exothermic releasing 6.5 MJ/kg (280 Btu/lb_m) of Zr reacted, the reaction rate increases strongly with cladding temperature, and the noncondensible gaseous reaction product is hydrogen.

3.3.1 Reaction Kinetics

A considerable amount of data on oxidation-reaction kinetics exists. If adequate steam is available, it is generally believed that the reaction is limited by oxygen diffusion through the ZrO_2 film and the underlying metal. In this case, the reaction rate is governed by parabolic kinetics; that is, $W^2=kt$ where W is the weight of metal reacted, t is the time, and k is the rate constant, which increases exponentially with temperature. The following equation can be used to estimate the mass of Zr oxidized at a particular temperature in a steam environment as a function of time

$$W_{Zr} = \sqrt{A\ t\ e^{-B/RT}} \qquad (3.3\text{-}2)$$

where,

W_{Zr} = mass of Zr oxidized per unit area exposed to steam, kg_{Zr}/m^2 ($lb_{m,Zr}/ft^2$)

t = exposure time, s

T = temperature of surface, K, (°R)

R = universal gas constant, 8314.29 J/(kg-mole·K). (1.98583 Btu/lb-mole/°R)

Correlations with experimental data have provided several alternative estimates of the empirical constants A and B.[2,3,4] The values obtained by Cathcart are

A = 294 $kg^2/m^4/s$ (12.3 $lb_m^2/ft^4/s$)

B = 1.672×10^8 J/kg-mole (7.195×10^4 Btu/lb-mole).

Figure 3.3-1 shows the mass of hydrogen produced as a function of time for several temperatures. Figure 3.3-2 shows the mass Zr oxidized in 5 minutes at constant temperature as a function of temperature for surface area of 5400 m^2 (58000 ft^2), corresponding to a PWR core.

3.3.2 Oxidation Front

The preceding isothermal example is not realistic for a severe accident because the exothermic energy associated with the oxidation reaction would actually cause the cladding and fuel temperatures to increase rapidly. Reaction energy is removed from the surface by hydrogen and by inward and axial transfer to the metal substrate and then to the fuel. When the reaction zone attains temperatures above about 2420°F (1600 K, 1327°C), the oxidation rate becomes so large that nearly all the available steam is reacted for typical boiloff sequences. This condition is referred to as steam limiting because the oxidation rate is limited by the amount of steam available to react with the cladding.

Example 3.3-1: Hydrogen Production Rate

a. What is the hydrogen production per unit surface area of Zr after 5 minutes exposure to steam at 2192°F (1473 K, 1200°C)?

b. If all of the cladding (5400 m^2, 26,940 lb$_m$) in the Zion PWR were exposed to such an environment in a severe accident, how much hydrogen (kg) would be produced?

c. Estimate the total energy release.

Solution:

a. Substituting into Eq (3.3-2) gives

$$W_{Zr} = \sqrt{\frac{294\ (kg_{Zr})^2}{m^4 \cdot s} \Big| \frac{5\ \text{min}}{} \Big| \frac{60\ s}{\text{min}}\ \exp\left(\frac{-1.672\times10^8\ J}{kg\text{-}mole} \Big| \frac{kg\text{-}mole \cdot K}{8314.29J} \Big| \frac{}{1473.15\ K} \right)}$$

$$W_{Zr} = 0.322\ kg_{Zr}/m^2$$

Multiplying W_{Zr} by the surface area of 5400 m^2 gives the mass of Zr that could be oxidized according to the parabolic kinetics:

$$m_{Zr} \le \frac{0.322\ kg\ Zr}{m^2} \Big| \frac{5400\ m^2}{} = 1{,}740\ kg\ Zr = 3.83\times10^3\ lb_m\ Zr$$

This is 14.2% of the 26,940 lb$_m$ Zr present.

b. By Equation (3.3-1), two moles of hydrogen are produced per mole of Zr reacted; hence, the number of moles of hydrogen released is

$$n_{H_2} = \frac{1{,}740\ kg\ Zr}{} \Big| \frac{kg\text{-}mole\ Zr}{91.22\ kg\ Zr} \Big| \frac{2\ kg\text{-}moleH_2}{kg\text{-}mole\ Zr} = 38.1\ kg\text{-}mole\ H_2$$

The corresponding mass of hydrogen is

$$m_{H_2} = \frac{38.1\ kg\text{-}mole\ H_2}{} \Big| \frac{2.016\ kg\text{-}H_2}{kg\text{-}mole\ H_2} = 76.9\ kg\ H_2$$

c. The total energy released is estimated as the mass of Zr reacted times 6.5 MJ/kg.

$$\Delta h_{rxn} \approx \frac{1{,}740\ kg\ Zr}{} \Big| \frac{6.5\ MJ}{kg\ Zr} \Big| \frac{GJ}{10^3\ MJ} = 11.3\ GJ$$

Figure 3.3-3 illustrates a calculation of the thermal behavior of fuel during the oxidation stage of core degradation.[5] The calculation is one dimensional, and does not account for the natural-circulation flow discussed later (see 3.3.5). Significant oxidation occurs first near the location of maximum axial power. As oxidation continues, a sharp temperature profile develops, reflecting a distinct oxidation front. Oxidation increases rapidly near the front and then decreases with elevation due to steam depletion. The relatively short 5 minute duration in Table 3.1-1 for Stage 3 is based on calculations that indicate rates of temperature increase exceeding 3.6°F/s (2 K/s) in regions undergoing vigorous oxidation.[5]

Figures 3.3-4 and 3.3-5 illustrate the potential contribution of the zirconium oxidation energy to the overall energy release rate in the core region, as a function of oxidation temperature. Decay heat transfer to residual saturated water below the uncovered portion of the core results in a steam production rate that is proportional to the below-water portion of the decay heat power, P_{Db}. As indicated in Figure 3.3-5, at sufficiently low peak cladding temperature, the energy release rate due to oxidation is negligible compared to that due to decay power. However, as the cladding temperature in the uncovered core region increases to about 1832°F (1273 K, 1000°C), more and more of the vapor generated by evaporation of residual water participates in the zirconium oxidation reaction. At sufficiently high cladding temperatures, virtually all of the resulting vapor could participate in the zirconium oxidation reaction. In this so-called steam limited condition, the energy h_{fg} consumed in evaporating a unit mass of residual water would result in an energy release in the oxidation reaction of Δh_{rxn} (normalized to a unit mass of steam). Therefore, the ratio of the energy release rate by the oxidation reaction to the decay power released below the water level, $P_{oxidation}/P_{Db}$, would at least equal $\Delta h_{rxn}/h_{fg}$. As indicated in Figure 3.3-5, this ratio varies from 6.3 at atmospheric pressure to 19 at 2500 psig. Even if P_{Db} were just 1/20 of the total decay heat power, the oxidation energy could be comparable to the decay heat power during Stage 3.

The preceding argument ignores downward energy transfer (e.g., by thermal radiation or movement of debris) from the hot, uncovered core region to the residual water. As indicated in Figure 3.3-4, each unit of energy that is transferred downward to the saturated residual water results in the production of additional steam to fuel the oxidation reaction. With significant feedback, for example due to radiative heat transfer from the hot reaction zone to the residual water, the energy release rate from oxidation can substantially exceed that from decay heat power. The acceleration of energy release rates from Zircaloy oxidation with temperature, which is illustrated by Figure 3.3-5, has been observed experimentally.

3.3.3 Core Damage Due to Oxidation

Clad melting is excluded during Stage 3, which is by definition (Table 3.1-1) limited to temperatures of 3200°F (2033 K, 1760°C) or less. Nevertheless, several types of cladding damage can occur during Stage 3. The cladding is simultaneously subjected to thermal transients and, particularly if the reactor coolant system is depressurized, to stresses resulting from increased internal pressure of the initial fill gases and fission gases. At low reactor coolant system pressures, ballooning of the cladding is expected prior to rupture. The temperature and pressure at which ballooned Zircaloy-4 cladding bursts in a steam environment has been studied, and it has been found that, even at low (initial) internal pressures, cladding usually bursts at temperatures below 2192°F (1473 K, 1200°C).[6]

Zirconium-burning tests result in clouds of smoke issuing from the test chamber, indicating that large quantities of aerosols are generated during the oxidation.[7] Such aerosols may have a tendency to accelerate the plateout of fission products within the reactor coolant system.

As oxidation proceeds, embrittlement and spallation of ZrO_2 from the surface of the cladding as oxidation proceeds can weaken the fuel rods, expose more fresh zirconium metal, and/or produce debris with the potential for blocking coolant flow channels. Increases in the cladding surface area exposed to steam can increase the oxidation rate if the reaction is not already steam starved.

Because low-melting-point silver-indium-cadmium alloys are often employed in PWR control rods, the possibility exists for formation of significant molten quantities of these materials at the temperatures attained during Stage 2. The behavior of such melts and their impact on PWR accident progression is discussed in Section 3.4.

For BWRs, melting of the stainless steel control blades would occur during Stage 3, well before the onset of fuel relocation. Special accident management guidelines (procedures) are in place to both delay the onset of rapid zirconium oxidation and to limit its extent once initiated. These special BWR measures are discussed in Section 3.7.2.

3.3.4 Reflooding During Stage 3

During a normal boiloff, mechanisms for transferring energy from uncovered fuel to residual water are limited principally to radiative heat transfer. On the other hand, if water is reintroduced to the core zone (reflooding) during the oxidation (Stage 3), the core-damage processes may initially be accelerated (and the rate of hydrogen generation increased) due to cladding oxidation by the additional steam generated during the cooling of overheated fuel.

Considerable fracturing of cladding embrittled during oxidation is expected during reflood. This may lead to the formation of fairly coarse rubble (fractured cladding, fuel, and control materials) in some regions of the core. Such rubble formation occurred in the upper portion of the TMI-2 core as a result of the temporary restart of reactor coolant pump 2B (see section 3.4.4). It is likely that the rubble beds formed would be coolable and, given a continuous supply of coolant injection, the accident would be terminated during this stage. (At TMI-2 coolant was not permanently restored until the accident had progressed beyond Stage 3, yet the debris was ultimately cooled in-vessel.) However, cooling of a reflooded core that has undergone severe damage would have to be maintained long-term. Additional aspects of rubble-bed cooling are discussed in Section 3.5.

Reflooding of a damaged core from which a significant fraction of the control rods have melted introduces a potential for criticality if the injected water is unborated. Section 3.7.3 discusses recriticality concerns for BWRs.

3.3.5 Natural Circulation During Core Degradation

In PWR accidents in which the reactor coolant system is not depressurized as the core heats up, gas movement in the uncovered core and upper head regions begins to be driven by natural convection (buoyancy forces).[8] Heat and mass transfer from the core to the reactor coolant system structures are dominated by buoyancy-driven components of the flow field. Steam from the boiloff of residual in-vessel water and hydrogen from oxidation of fuel cladding rise from the hot central core region and lose heat and entrained fission products to relatively colder structures above the core. As depicted in Figure 3.3-6, the cooled gases recirculate downward through the colder regions of the uncovered core and are reheated again by flowing up through the hot central core region.

In BWRs, the fuel channels which enclose the rods of individual fuel assemblies impede in-core natural circulation. However, if the residual water level falls below the bottom of the BWR downcomer region while fuel is still heating up in the core region, a strong natural convection loop can be established from the core to the steam separators and dryers with return to the core inlet via the downcomers. This is depicted in Figure 3.3-7.

As indicated in Figure 3.3-8, the strength of steel decreases rapidly above 1000°F (811 K, 538 °C). For some high-pressure PWR accidents, it has been suggested that the natural circulation flows in PWRs could transfer sufficient heat to the reactor coolant system pressure boundary to result in relatively early temperature-induced failure, in particular, failure of a hot leg.[9] The resulting depressurization of the primary system would alter the thermal-hydraulic progression of the accident. In particular, depressurization would preclude the potentially severe ramifications associated with high-pressure ejection of melt into the containment (see Sections 3.6 and 4.5). It should be noted, however, that early temperature-induced failure did not occur at TMI-2. Nevertheless, codes capable of modeling natural circulation indicate that early temperature-induced failures are possible and may be likely in a number of PWR severe accident scenarios.

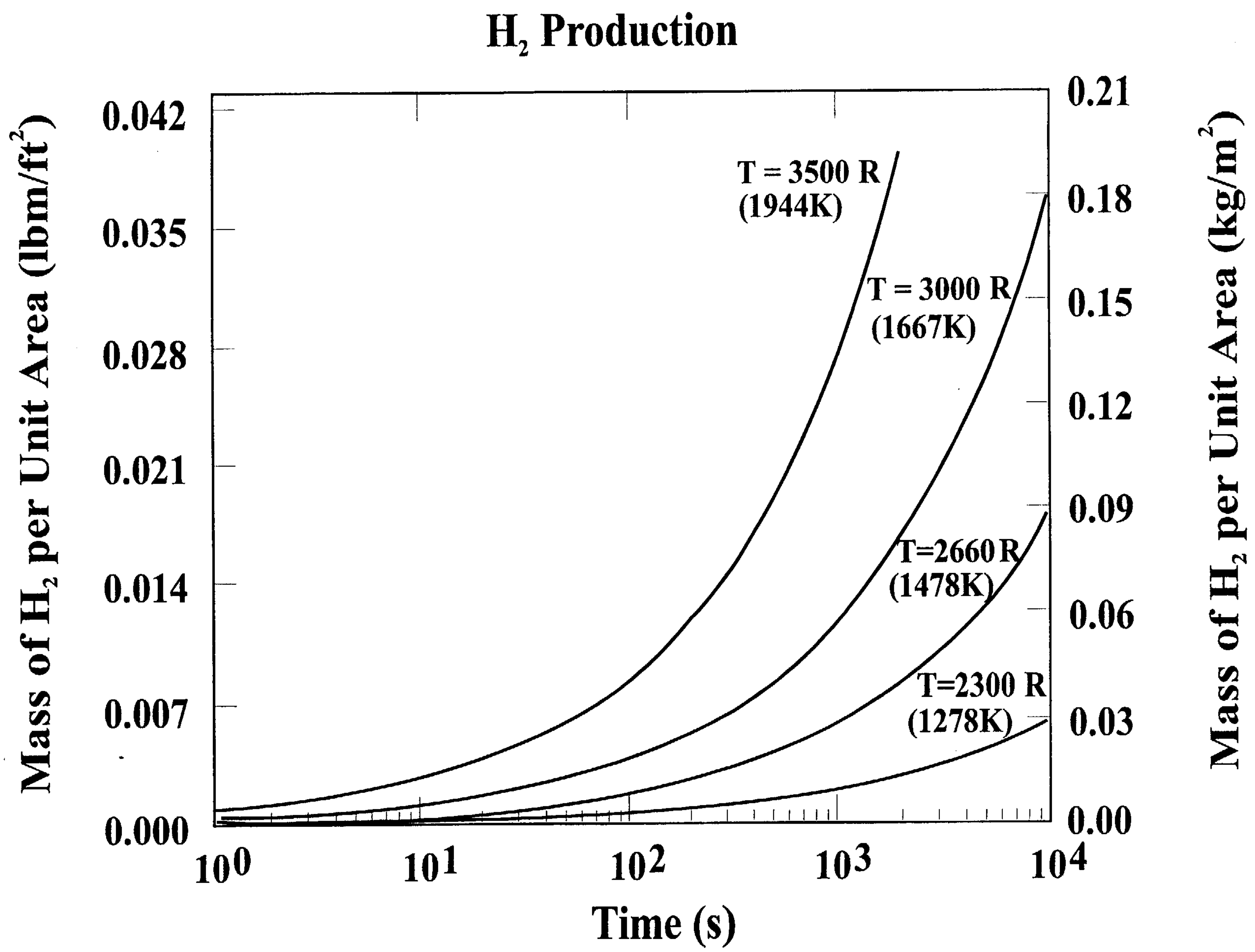


Figure 3.3-1 Hydrogen production per unit area from the Zr : H_2O reaction

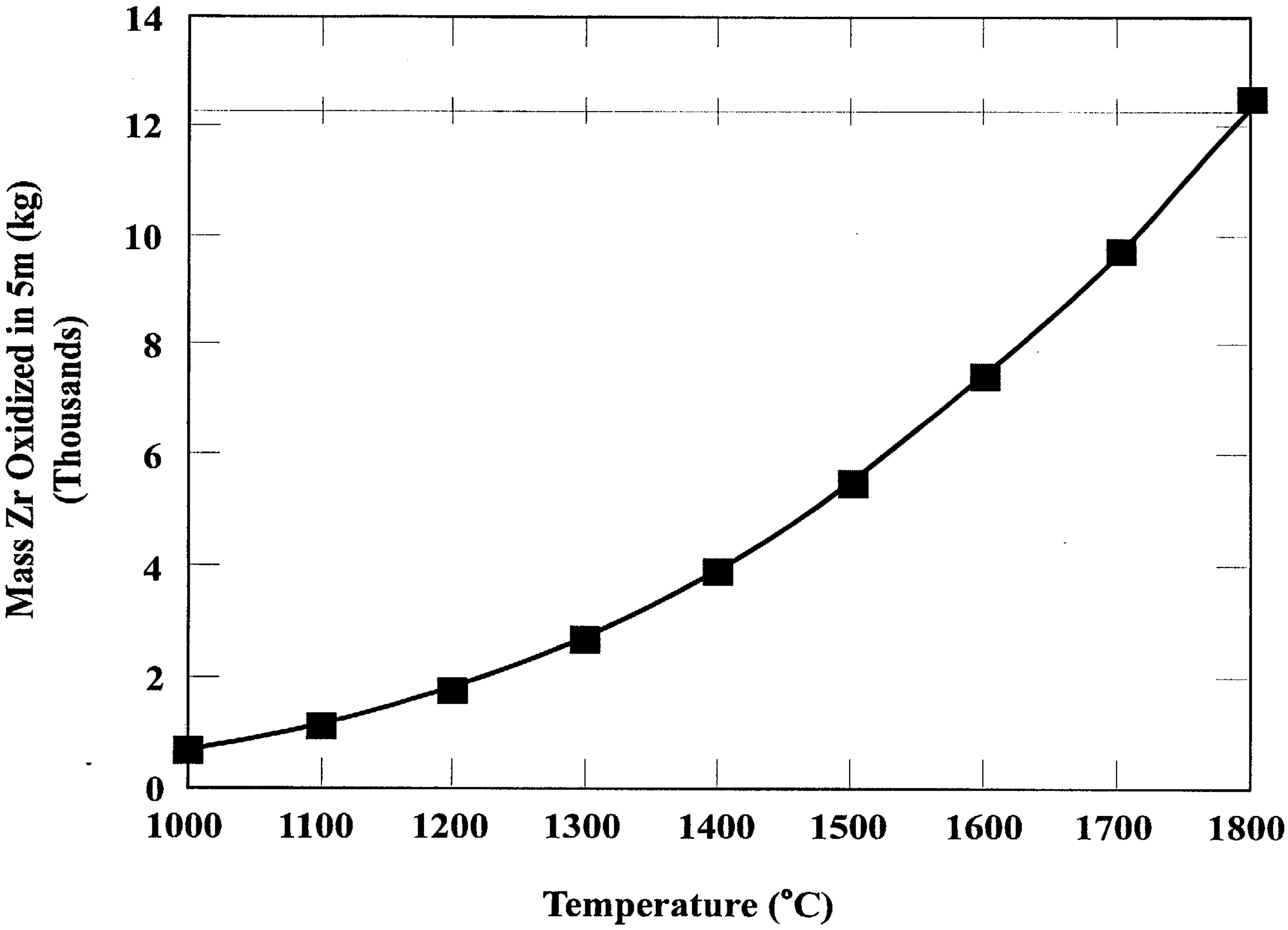


Figure 3.3-2 Mass of Zr oxidized in 5 minutes exposure of 5400 square meters Zircaloy

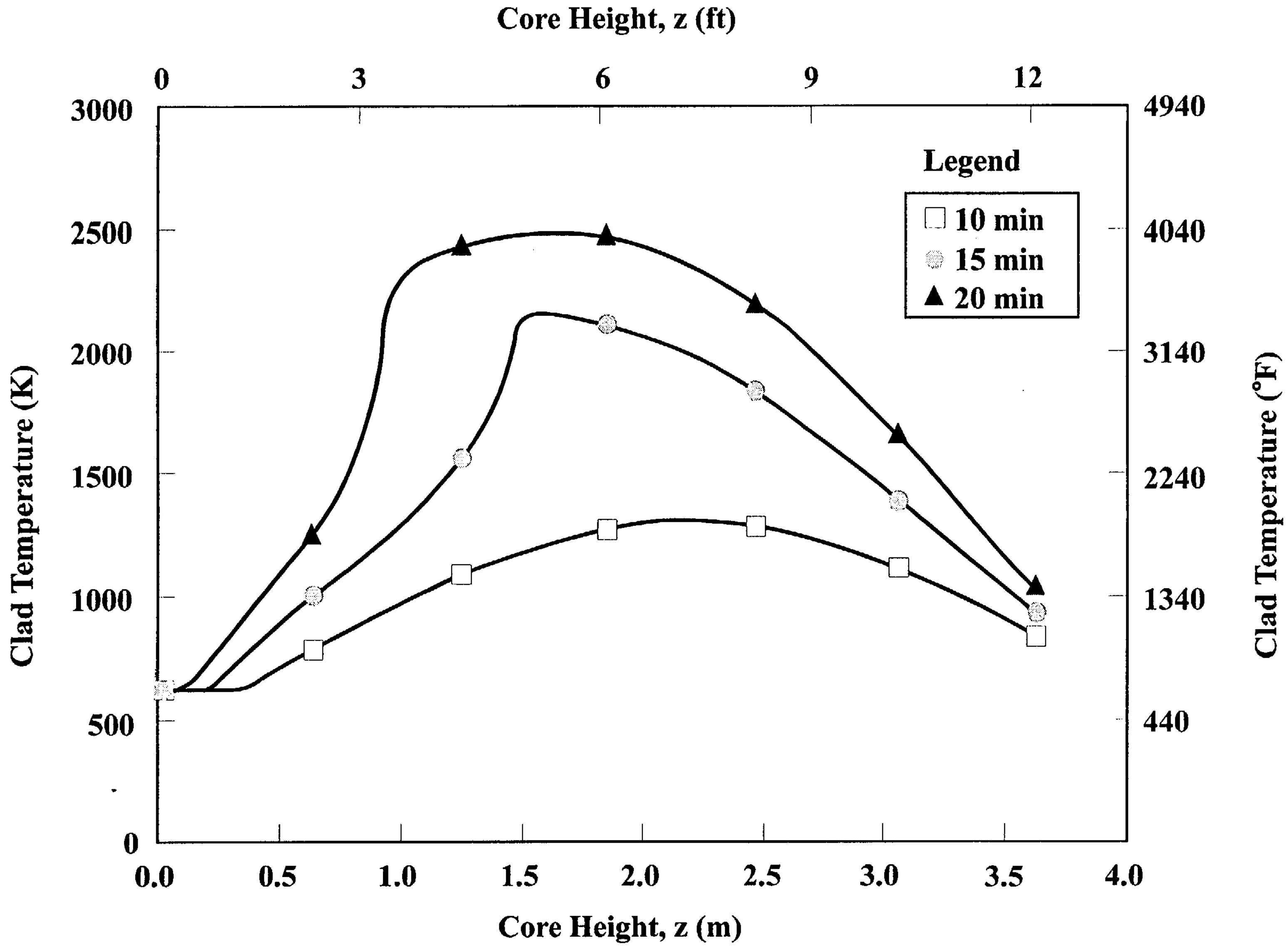


Figure 3.3-3 Calculated axial cladding temperatures at three different times following start of core uncovering for a PWR station blackout

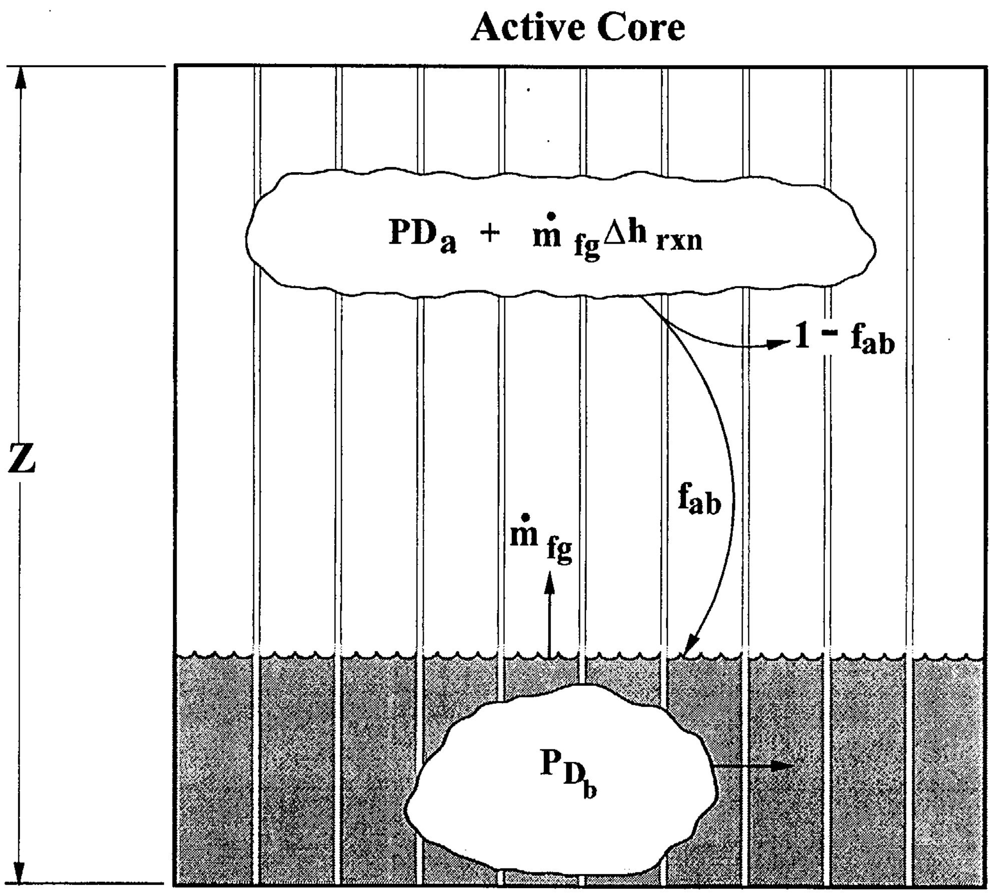


Figure 3.3-4 Heat balance between uncovered core and residual water

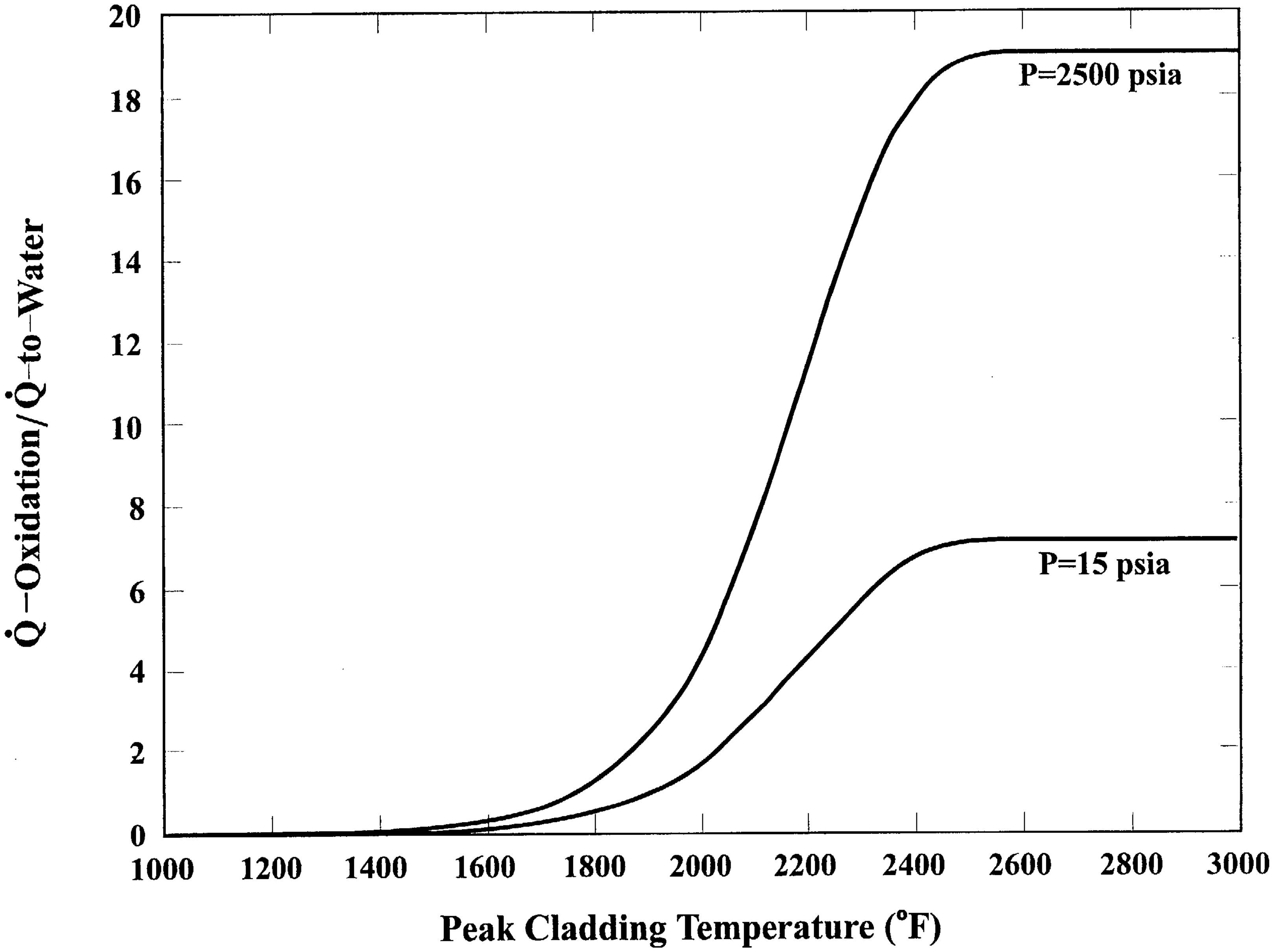


Figure 3.3-5 Ratio of heat release rate via oxidation to heat transfer rate to residual saturated water

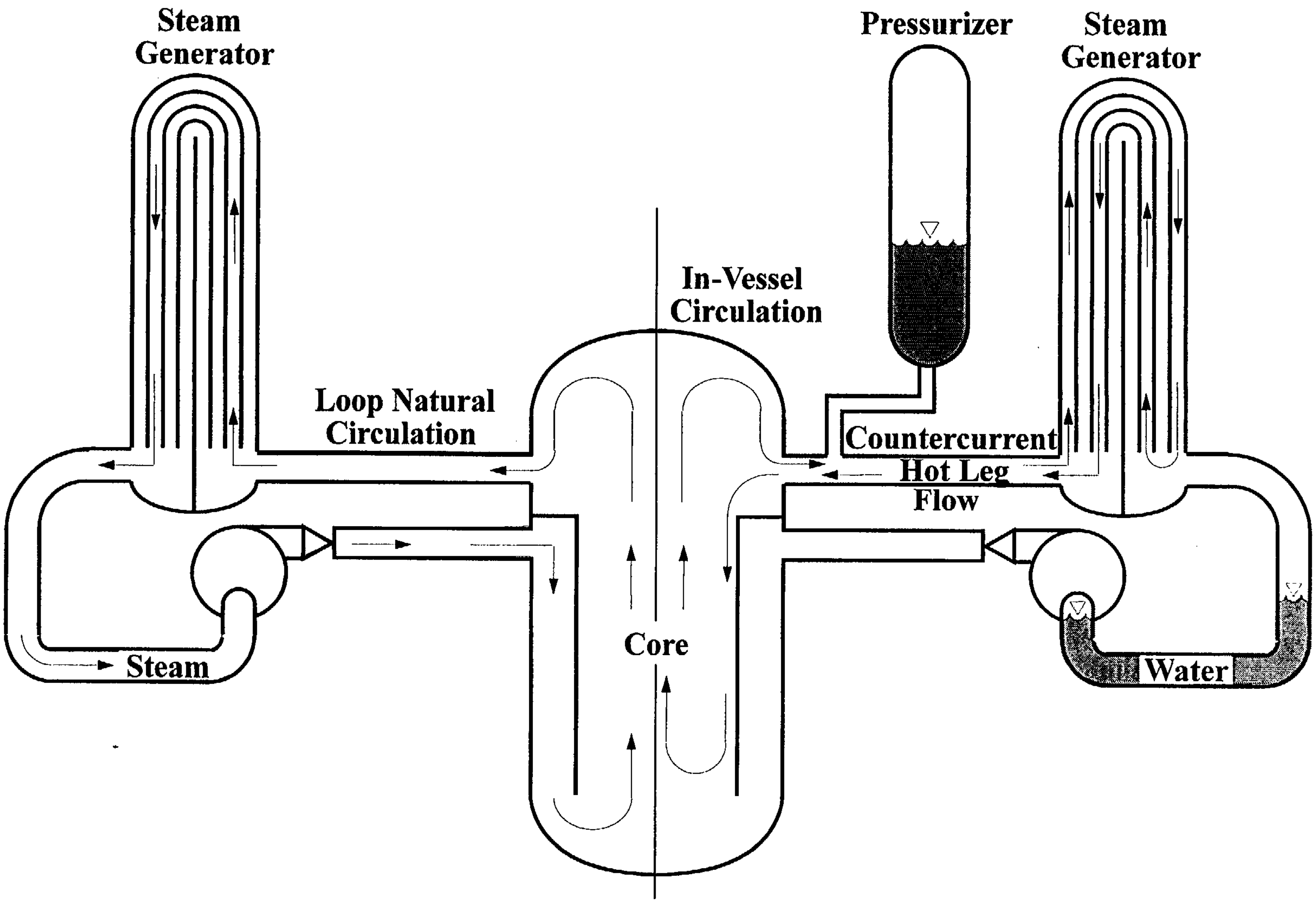


Figure 3.3-6 Severe accident natural circulation flows

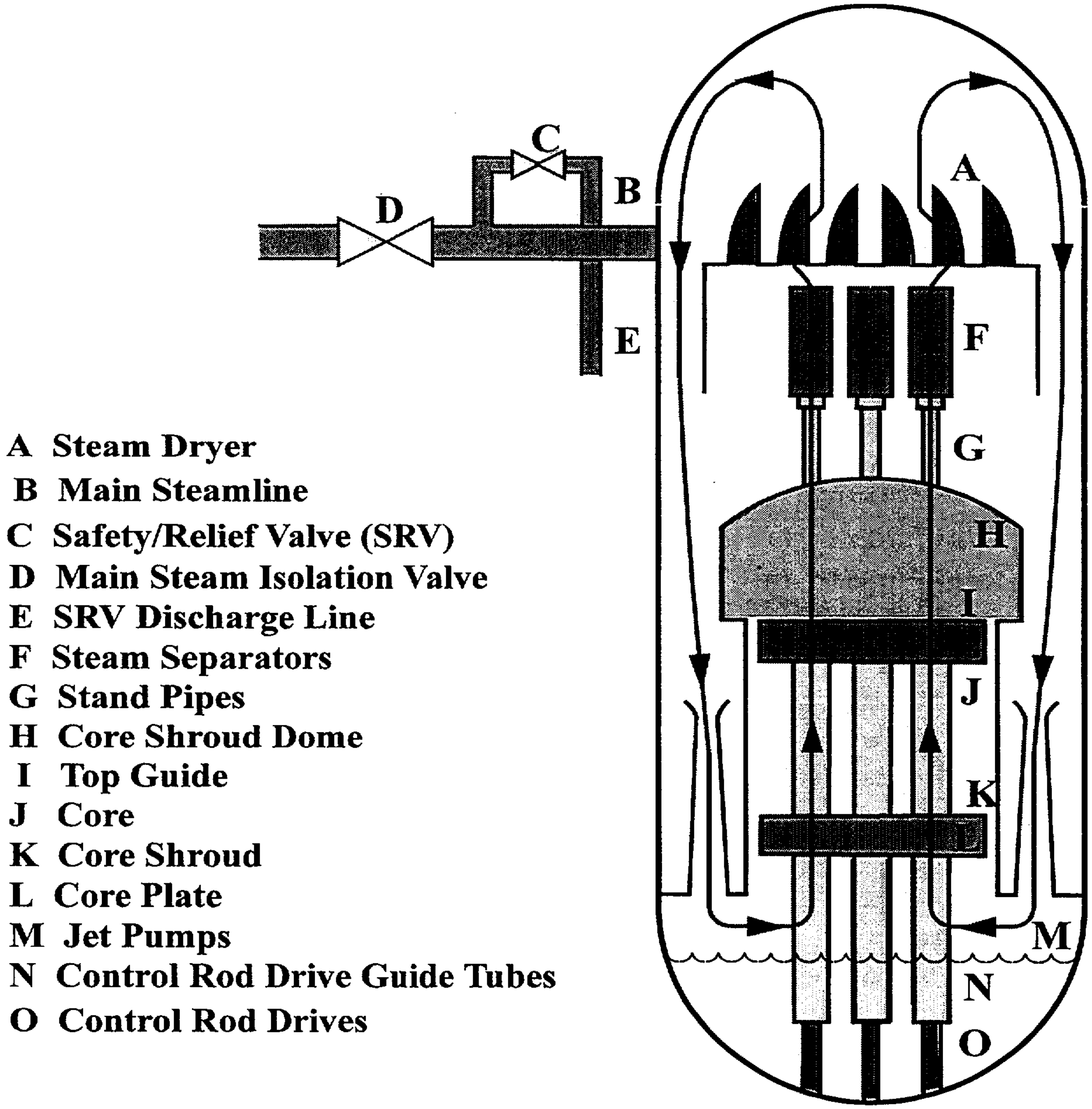


Figure 3.3-7 Schematic diagram of a BWR with interńal circulation

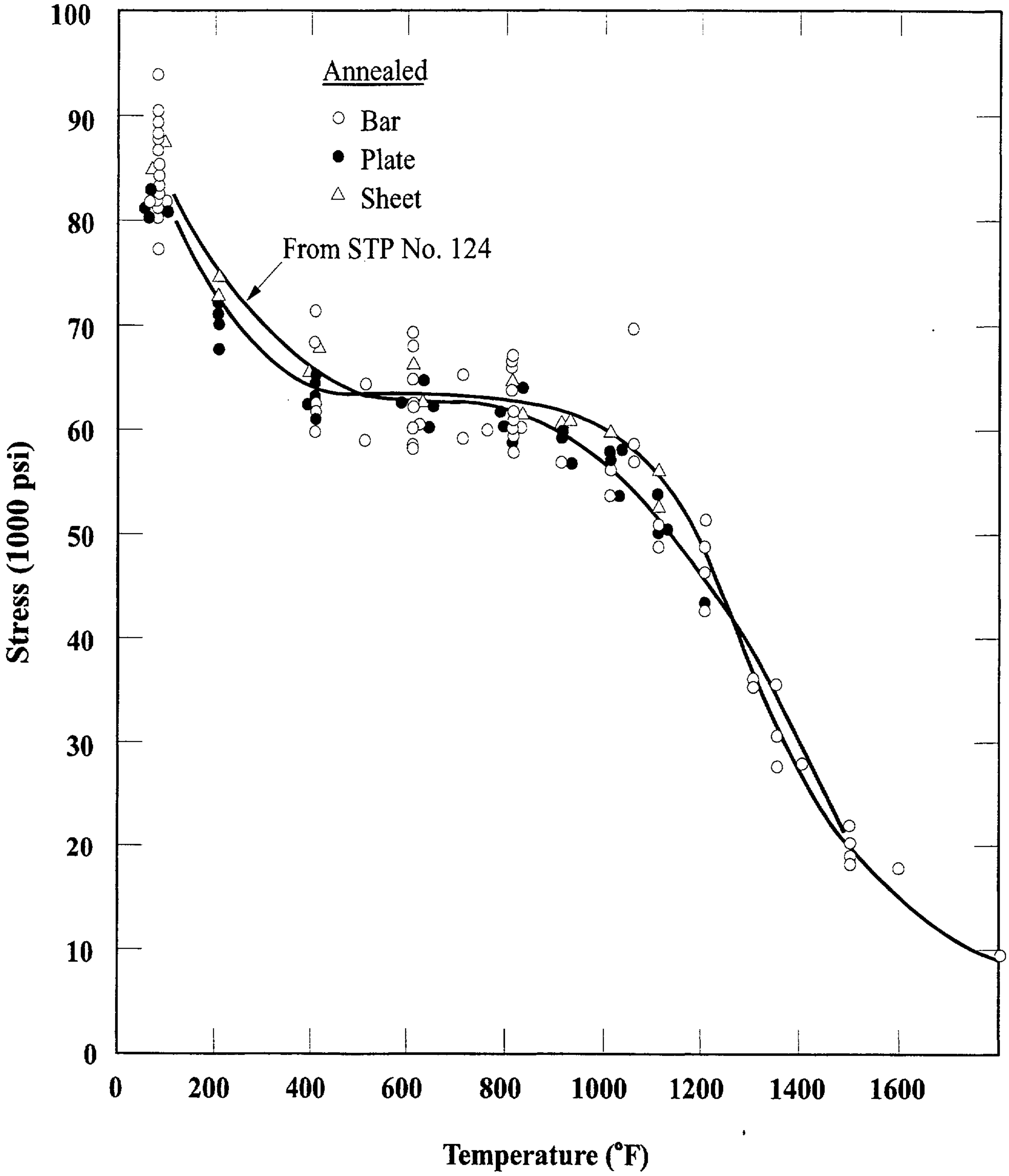


Figure 3.3-8 Tensile strength, type 304 stainless steel

References for Section 3.3

1. L. Baker, Jr., and R. O. Ivins, "Analyzing the Effects of a Zirconium-Water Reaction," *Nucleonics*, 23, 7, p. 70, 1965.

2. L. Baker, Jr. and L. C. Just, "Studies of Metal-Water Reactions at High Temperatures III," ANL-6548, Argonne National Laboratory, Argonne, Illinois, 1962.

3. J. V. Cathcart, et al., "Zirconium Metal-Water Oxidation Kinetics IV, Reaction Rate Studies," ORNL/NUREG-17, Oak Ridge National Laboratory, Oak Ridge, Tennessee, August 1977.

4. V. F. Urbanic and T. R. Heidrick, "High Temperature Oxidation of Zircaloy-2 and Zircaloy-4 in Steam," *J Nucl Materials*, 75(2):251-61, 1978.

5. F. Briscoe, J. B. Rivard, and M. F. Young, "Fuel Rod Temperature Transients During LWR Degraded Core Accidents," *Proceedings, International Meeting on Thermal Nuclear Reactor Safety*, NUREG/CP-0027, U.S. Nuclear Regulatory Commission Conference Proceeding, Chicago, Illinois, August 29 - September 2, 1982.

6. R. H. Chapman et al., "Zircaloy Cladding Deformation in a Steam Environment with Transient Heating," *Zirconium in the Nuclear Industry (Fourth Conference)*, ASTM STP 681, pp. 393-408, American Society for Testing and Materials, Philadelphia, Pennsylvania, 1979.

7. J. B. Rivard et al., "Identification of Severe Accident Uncertainties," NUREG/CR-3440, SAND83-1689, Sandia National Laboratories, Albuquerque, NM, p. 3-8, September 1979.

8. V. E. Denny and B. R. Sehgal, "Analytic Prediction of Core Heatup Liquefaction/Slumping," (*Proc. Int. Mtg. on LWR Severe Accident Evaluation*, Cambridge, Massachusetts, p. 5.4-1, 1983.

9. F. T. Harper et al., "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters," NUREG/CR-4551, SAND86-1309, Vol. 2, Rev. 1, Part 1, Issue 1, U.S. Nuclear Regulatory Commission, December 1990.

3.4 Melting, Liquefaction, Holdup

Stage 4 begins with the initial downward relocation of molten fuel in the core region. It extends to the time that fuel-bearing melt enters the lower plenum of the reactor vessel. Fuel damage during Stage 4 is extensive. It is driven both by decay power and by oxidation. There is a strong coupling between fuel damage that occurs during this stage and the release, chemistry, and transport of fission products within the reactor coolant system.

3.4.1 Initial Melting

As indicated in Section 3.2, the local decay-heat generation rate determines how rapidly a given uncovered region of the core would heat up. The decay-heat generation rate is proportional to the thermal power during operation. The thermal power distribution can therefore be used to provide a rough idea of the core regions most susceptible to the onset of rapid oxidation and subsequent melting. Figure 3.4-1 shows the power distribution in the TMI-2 core prior to the accident.[1] Less than half of the core by volume produces power at 25 kW/m or greater. Heat generation rates at the periphery of the core are markedly lower. This suggests that melting would start near the center of the core and might be restricted to the central region of the core. Some of the outermost fuel rods may not attain temperatures resulting in severe damage because of their low power levels and their location adjacent to surrounding structures.

Zircaloy-4 melts at about 3200°F (2033 K, 1760°C); however, the onset of melting may occur at lower temperatures. At TMI-2, a Ni-Zr eutectic, which forms at 2192°F (1473 K, 1200°C), was probably the first melt formed as a result of interactions between the Inconel grid spacers and Zircaloy cladding near the center of the core. The TMI-2 Ag-In-Cd control rod material melts at 1472°F (1073 K, 800°C), and the stainless steel control rod cladding melts at approximately 2642°F (1723 K, 1450°C). Both of these melt points are well below that of Zircaloy, so molten control rod material also flowed to the liquid steam interface relatively early. Molten silver and iron form relatively low-temperature eutectics with Zircaloy. Thus, the initial molten mixture contained significant zirconium.

The postulated condition of the TMI-2 core shortly after the onset of melting (150 to 160 minutes into the accident) is shown in Figure 3.4-2.[2] Upon reaching the steam/liquid interface the metallic mixture froze to form a lower crust that blocked coolant channels between fuel rods. Post-accident analyses confirm that the crust was a Zr-Ag-In-Fe-Ni metallic mixture surrounding standing columns of fuel pellets. The lowest crust was near the lowest grid spacer and corresponds to the lowest water level in the core during the accident. Alternative scenarios in which a blockage does not form in the core region due to a lower water level are discussed in Section 3.4.3.

3.4.2 Fuel Liquefaction

Early views of core melt progression reflected in the 1975 Reactor Safety Study held that fuel melting did not occur until the UO_2 fuel material attained its melting temperature, 5156°F (3123 K, 2850°C). Research subsequent to the 1979 TMI-2 accident has shown that UO_2 can be liquefied far below its ceramic phase melting temperature. When the local temperature of the fuel reaches the Zircaloy melting temperature, 3200°F (2033 K, 1760°C), flow of metallic cladding beneath the oxidized layer can occur. Interactions can then occur between molten Zircaloy and solid UO_2 as indicated in Figure 3.4-3. In one series of laboratory experiments, UO_2 crucibles holding molten Zircaloy at temperatures between 3272°F (2073 K, 1800°C) and 3632°F (2273 K, 2000°C) in an argon atmosphere were rapidly destroyed by the dissolution of solid UO_2 in molten Zircaloy.[3] In another experiment, electrically-heated fuel-rod simulants in steam were massively liquefied and relocated when the oxidation-driven 9-rod-bundle temperature exceeded 3632°F (2273 K, 2000°C). Similar behavior has been reported in several other experiments.[4]

Apparently, zirconium reduces UO_2 preferentially along UO_2 grain boundaries near the UO_2-Zircaloy interface. This produces a homogeneous U-Zr-O melt at low oxygen concentrations or a heterogeneous U-Zr-O melt containing UO_2 particles at high oxygen concentrations. In either case, the process is called fuel liquefaction.

In addition to destroying the UO_2 matrix, fuel liquefaction accelerates the release of fission products from the fuel. However, minor alloying components or impurities can have large effects on such releases. For instance, tin, which is a 1% component of Zircaloy, may act as a getter for tellurium, resulting in significant holdup or retention of tellurium fission products.[5]

3.4.3 Flow Blockage Versus Streaming

The significant liquefaction of fuel that would occur after the Zircaloy cladding started to melt would result in downward flow of liquid U-Zr-O. Even in the absence of a blockage formed by the refreezing of lower melting temperature metallic mixtures (as occurred at TMI-2), molten U-Zr-O could refreeze on the surfaces of fuel rods or fuel assembly rod spacers in lower regions of the core where temperatures were cooler. Calculations indicate that, without additional oxidation, the liquefied fuel would rapidly freeze producing a significant core blockage. This is true even if freezing requires the transfer of the full UO_2 latent heat of fusion (270 kJ/kg). A latent heat of fusion more appropriate for the U-Zr-O mixture would require less heat transfer (about 50 kJ/kg) making freezing even more likely.[5]

On the other hand, the high temperature of the liquefied U-Zr-O would favor high oxidation rates per unit area exposed, and energy addition by oxidation as the liquid flowed downward could preclude its refreezing. If the water level during the meltdown were below the bottom of the active core, the melt could then stream into the lower plenum if not halted by freezing on cooler surfaces below the core region. Quenching of melt that streamed into residual water in the lower plenum could provide the additional steam required to maintain the streaming process. The question of blockage versus streaming is important because it affects the magnitude of resulting fuel coolant interactions and the timing and mode of eventual bottom head failure (Sections 3.5 and 3.6). Most current analyses predict the formation of a blockage in the core region of a PWR even if the residual water level is below the bottom of the active fuel. BWR core melt progression is discussed in Section 3.7.

A central blockage would redirect steam flow outward in an open lattice (PWR) core. This is depicted in Figure 3.4-4. The diversion of steam flow to the outer regions of the core could result in two possible alternatives. If the fuel rods have not yet attained temperatures capable of supporting rapid oxidation, they may be cooled by the additional flow, but if the rods are hot enough, they may rapidly oxidize.

Figure 3.4-5 shows the core condition postulated at TMI-2 at 173 min, just prior to the brief restart of reactor coolant pump 2B.[4] The damage had progressed to the point where the blockage was nearly complete with only the outermost fuel assemblies undamaged. The bowl-like shape of the lower crust or crucible may have been caused by the flow blockage diverting steam flow radially outward. Such flow diversion increases steam flow rates and thus heat transfer at the periphery of the damage zone. This results in freezing the downward relocating melt at elevations above the water level as shown in Figure 3.4-5. A second explanation for the shape of the lower crust is that the onset of melting is primarily controlled by decay heat, and, consequently, the freezing isotherm increased in elevation as core damage progressed radially outward to regions of lower core power density.

Above the TMI-2 lower crust, a region of at least partially molten material formed as depicted in Figure 3.4-5. At the time indicated (just prior to the restart of reactor coolant pump 2B), core heatup calculations indicate that peak temperatures within this region of consolidated core materials may have reached the UO_2 melt temperature, 5156°F (3123 K, 2850°C). The average temperature of the material was probably between 4220°F (2600 K, 2327°C) and 4580°F (2800 K, 2527°C).[4]

Undamaged fuel rod stubs were about 2 ft. (60 cm) long near the center of the core, indicating that water did not drop below this level for any significant period of time during the accident. Water covering the bottom of the core kept the lower supporting crust cooled. This helped maintain the structural stability of the crust. The ultimate thickness of the lower crust was 10 to 15 cm.[6]

3.4.4 Reflooding at TMI-2

Activation of reactor coolant pump 2B at approximately 174 min resulted in the first significant addition of coolant to the TMI-2 reactor vessel following the shutdown of the loop-A reactor coolant pumps at approximately 100 min. Reactor coolant pump 2B operated for approximately 19 min; however, significant flow was only measured during the first 15 s. Approximately 1000 ft^3 (28 m^3) of water was pumped into the reactor vessel from the loop B cold leg.

As discussed in Section 2.1, the reactor coolant pressure increased rapidly when pump 2B was turned on. This pressure increase was caused by steam generated when the water contacted hot surfaces in the core region, and by hydrogen generated by the rapid oxidation of hot Zircaloy.

The thermal-mechanical forces resulting from partial quenching of the oxidized fuel rod remnants in the top half of the core fragmented the oxidized cladding and fuel pellets to form a debris bed. The configuration postulated for the core just after the pump 2B restart is shown in Figure 3.4-6. As indicated in the figure, the upper support grid was damaged. Selected areas of the bottom of the upper core support grid were oxidized, melted, or ablated thermally. There was, however, no damage to structures in the plenum above the upper core support grid.

The upper core debris bed contained about 27,000 kg of material. Between 3 and 10% of this debris was less than 1 mm in diameter, and the control-rod materials (Ag-In-Cd) in this debris were concentrated in particles less than 1 mm in diameter.[3]

Particles of this type were found on various horizontal surfaces in the upper plenum. Jets of steam from the 2B pump restart are thought to have led to this transport.

Apparently quantities of loose debris also settled to the lower head of the reactor vessel during quiescent periods or were transported there by loop flow during the 2B pump transient. This would explain findings of Ag-Cd on the surfaces of several incore instrument nozzles and in surface cracks in the stainless steel cladding on the lower head. The alternative that molten control-rod material flowed all the way to the bottom head seems less plausible because of the thick metal-rich lower crust that formed just above the minimum water level in the core region. Unfortunately, the manner in which lower head debris was broken up and removed from the vessel (Section 3.5.3) precluded confirmation or detailed characterization of a possible initial layer of control-rod debris on the bottom head.

From approximately 180 min to about 200 min, the water level in the TMI-2 core decreased as heat from the degraded core caused reactor coolant remaining in the core region to evaporate. At approximately 200 min the water level was at its lowest level. The low thermal diffusivity of the large consolidated region of primarily ceramic core debris prevented the interior of this region from cooling even when the reactor vessel was subsequently refilled with water. Calculations indicate that a pool of molten material formed in the center of the consolidated region and increased in size during this period.

At 200 min. the high pressure injection system was manually actuated and cooling water was injected for the next 17 min. Analyses indicate that the core region was refilled with water by 207 min. As the cooling water filled the reactor vessel, it penetrated the debris bed above the consolidated region. By about 230 min. debris in this upper debris bed was fully quenched.

The postulated condition of the core debris at 224 min. is depicted in Figure 3.4-7. Water covered the core region and penetrated the upper debris bed, but could not cool the consolidated region. The material between the upper and lower crusts was predominately molten.

Relocation of approximately 19.2 tonnes of molten core material into the lower plenum of the reactor vessel occurred between 224 and 226 min. As explained in Section 3.5.1, the pour was initiated by a failure of the crust at the periphery of the core region, but the failure does not appear to have been caused by the reflooding of the core region with water.

3.4.5 Additional Reflooding Considerations

If water is reintroduced into the core during Stage 4, acceleration of cladding oxidation may occur, because

- the quantity of unoxidized cladding may be relatively large due to the slow rate of steam evolution from boiloff prior to reflooding,
- a large fraction of the unoxidized cladding may be at elevated temperatures,
- quenching of hot fuel upon reflooding the lower part of the core would produce copious amounts of additional steam, and

- there could be relatively uninhibited access of steam to unoxidized cladding.

Acceleration of oxidation associated with reintroduced coolant might, given these assumptions, add tens of GJ of energy to the system in a short time and evolve large quantities of hydrogen. Because the energy required to destroy the entire core geometry at these temperatures may be as little as 6 GJ,[5] a significant redistribution of core materials in a very short time following the reintroduction of water is possible.[5] An attendant possibility is one or more steam explosions caused when hot, liquefied fuel contacts reflooding water. (Steam explosions are discussed in Section 3.6.) The actual scenario is quite uncertain, and this leads to corresponding uncertainties regarding subsequent processes and events.

TMI-2 demonstrates, however, that the reintroduction of sufficient water during Stage 4 can ultimately succeed in terminating the meltdown process within the reactor vessel. To achieve a stable in-vessel condition, the water supply must be maintained and heat must be removed from the core debris by reestablishing forced or natural circulation through the reactor coolant system or by local convection within debris beds. The effectiveness of debris cooling, especially that by local convection, depends upon the size, shape, and characteristics of the core debris (Section 3.5). In the long-term, heat transport to an ultimate heat sink may also be required to store the energy removed from the core debris without challenging containment integrity (Chapter 4).

3.4.6 Natural Circulation During Stage 4

In PWR accidents, even if the steam generator secondary-side inventory is depleted at the time of core damage, gaseous natural convection between the vessel and the primary side of U-tube steam generators is favored. Because of potential loop seals in the reactor coolant pump suction lines, the convective flows would most likely be required to traverse the hot leg piping, displacing cooler steam/hydrogen in the generator tubes by warmer steam-hydrogen from the core, as depicted on the right hand side of Figure 3.3-6. The great height of the steam generator tubes (18 m) provides a large driving force.

To the extent that the convection is effective, the steam generator tubes provide at least a temporary sink for heat and fission products. The effectiveness of the steam generators as a sink would decrease significantly as the tubes heated up. It has been estimated that halving the temperature difference between hot gases and steam generator tubes reduces the convective heat flux by 40%.[5]

As discussed in Section 3.3.5, because the strength of steel decreases rapidly above 1000°F (811 K, 538°C), sufficient natural circulation of hot gases to the steam generators would cause heated reactor coolant system structures such as the hot legs to weaken and fail. By depressurizing the reactor vessel, such temperature-induced failures could prevent large containment pressures and temperatures that might otherwise result from high-pressure melt ejection due to reactor vessel bottom head failure (Section 4.5).

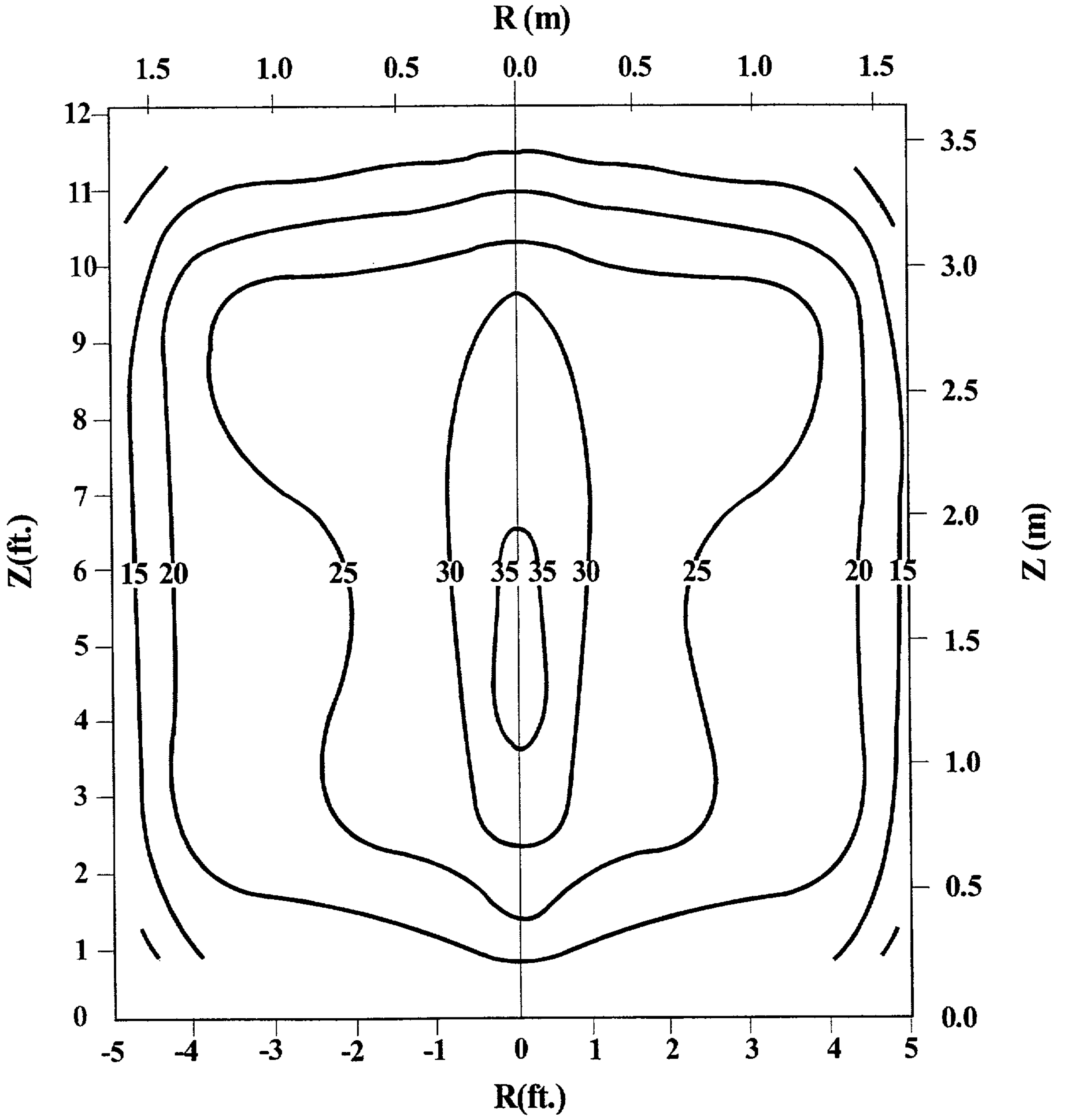


Figure 3.4-1 Distribution of fuel rod rating (kW/m) in the TMI-2 core

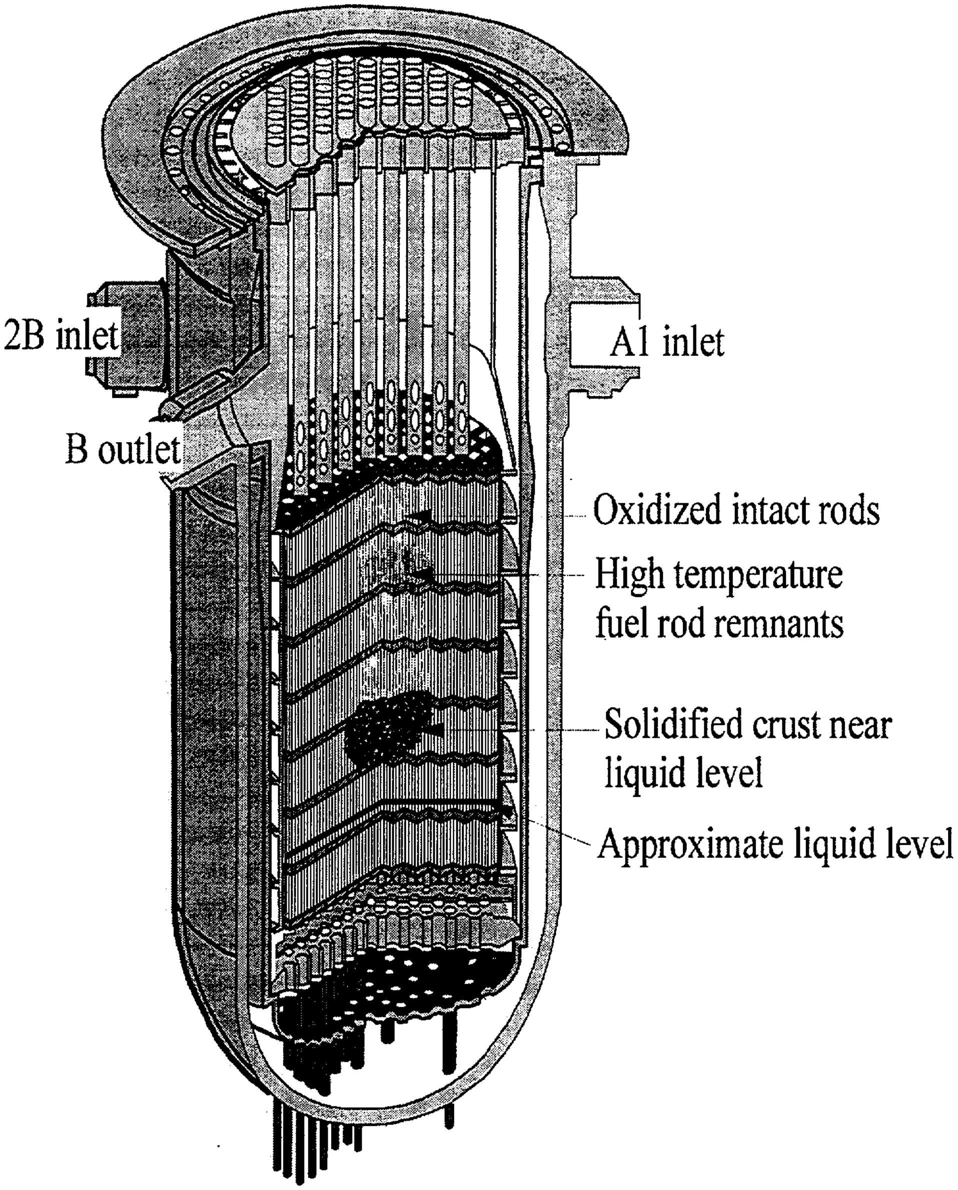

2B inlet
A1 inlet
B outlet
Oxidized intact rods
High temperature fuel rod remnants
Solidified crust near liquid level
Approximate liquid level

Figure 3.4-2 Hypothesized TMI-2 condition between 150 and 160 minutes

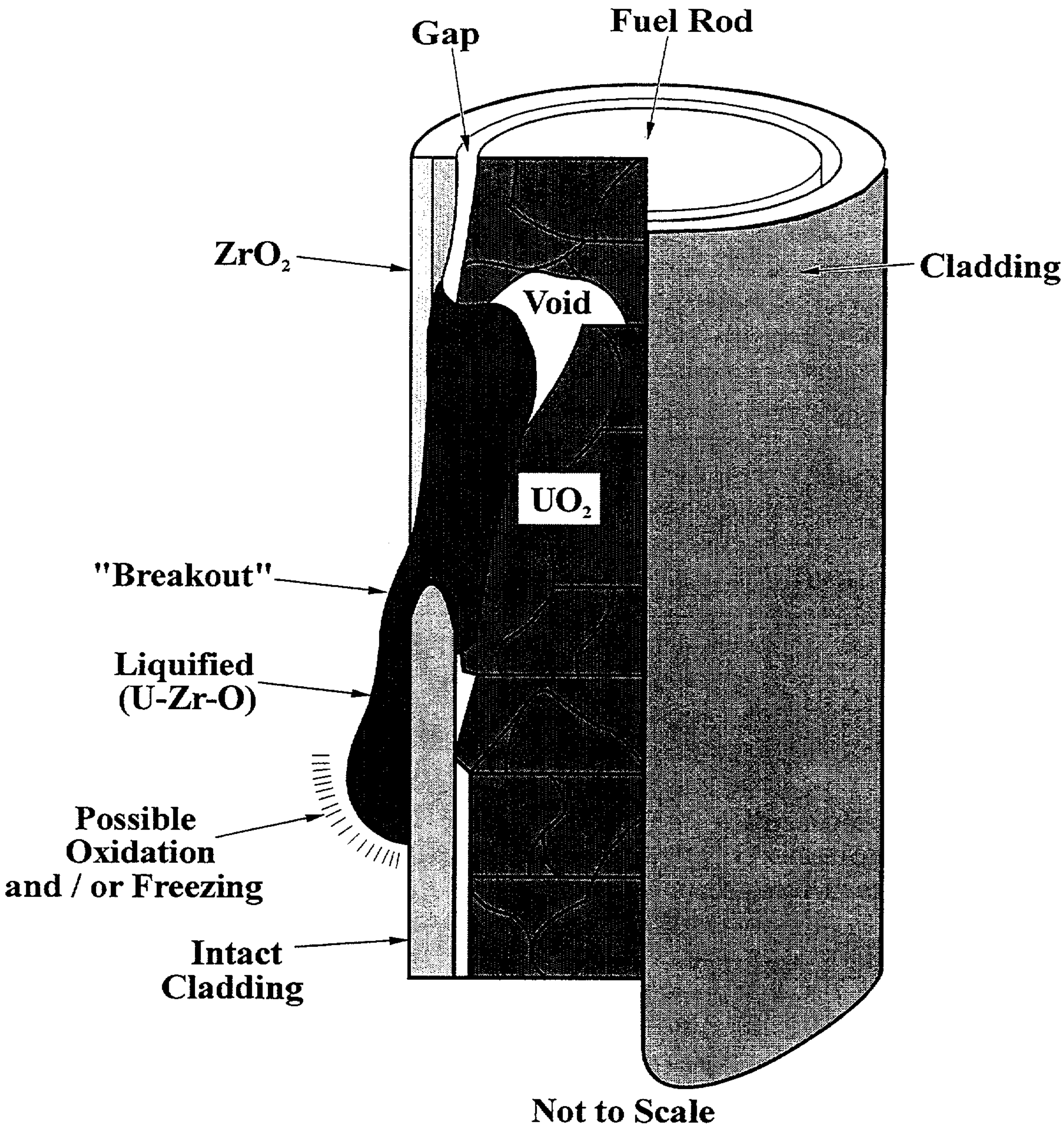


Figure 3.4-3 Schematic representation of possible mode of initial fuel liquefaction and downward flow.

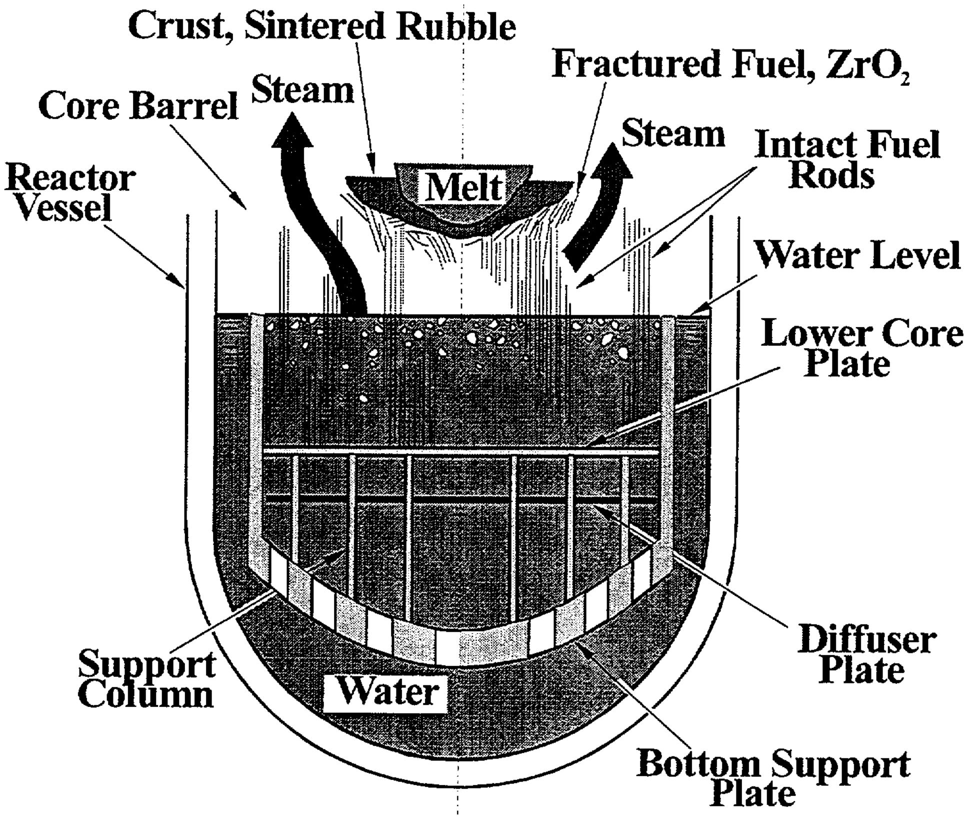


Figure 3.4-4 Initial core degradation in a PWR

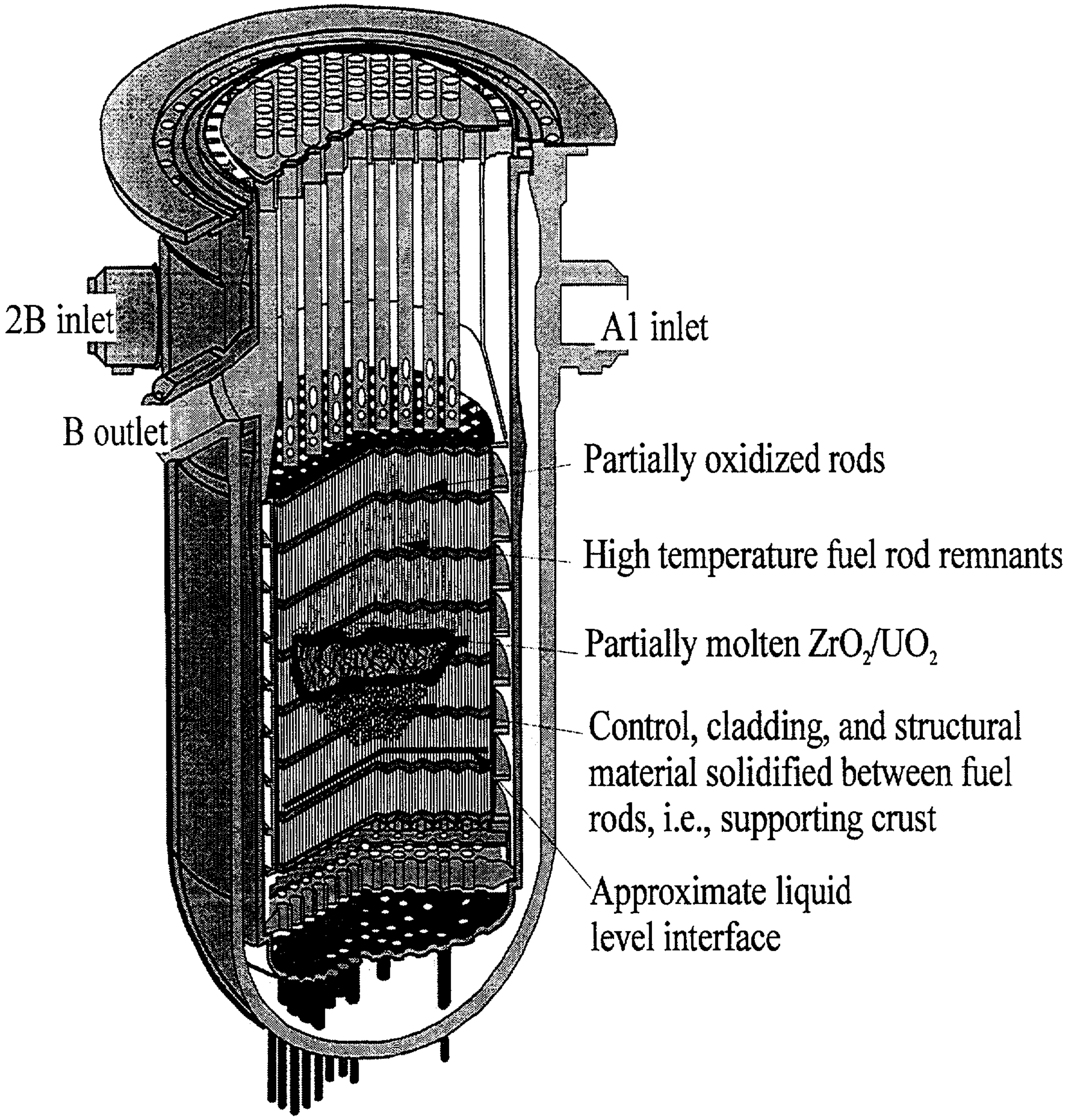

2B inlet
B outlet
A1 inlet
Partially oxidized rods
High temperature fuel rod remnants
Partially molten ZrO_2/UO_2
Control, cladding, and structural material solidified between fuel rods, i.e., supporting crust
Approximate liquid level interface

Figure 3.4-5 Hypothesized TMI-2 core at 173 minutes

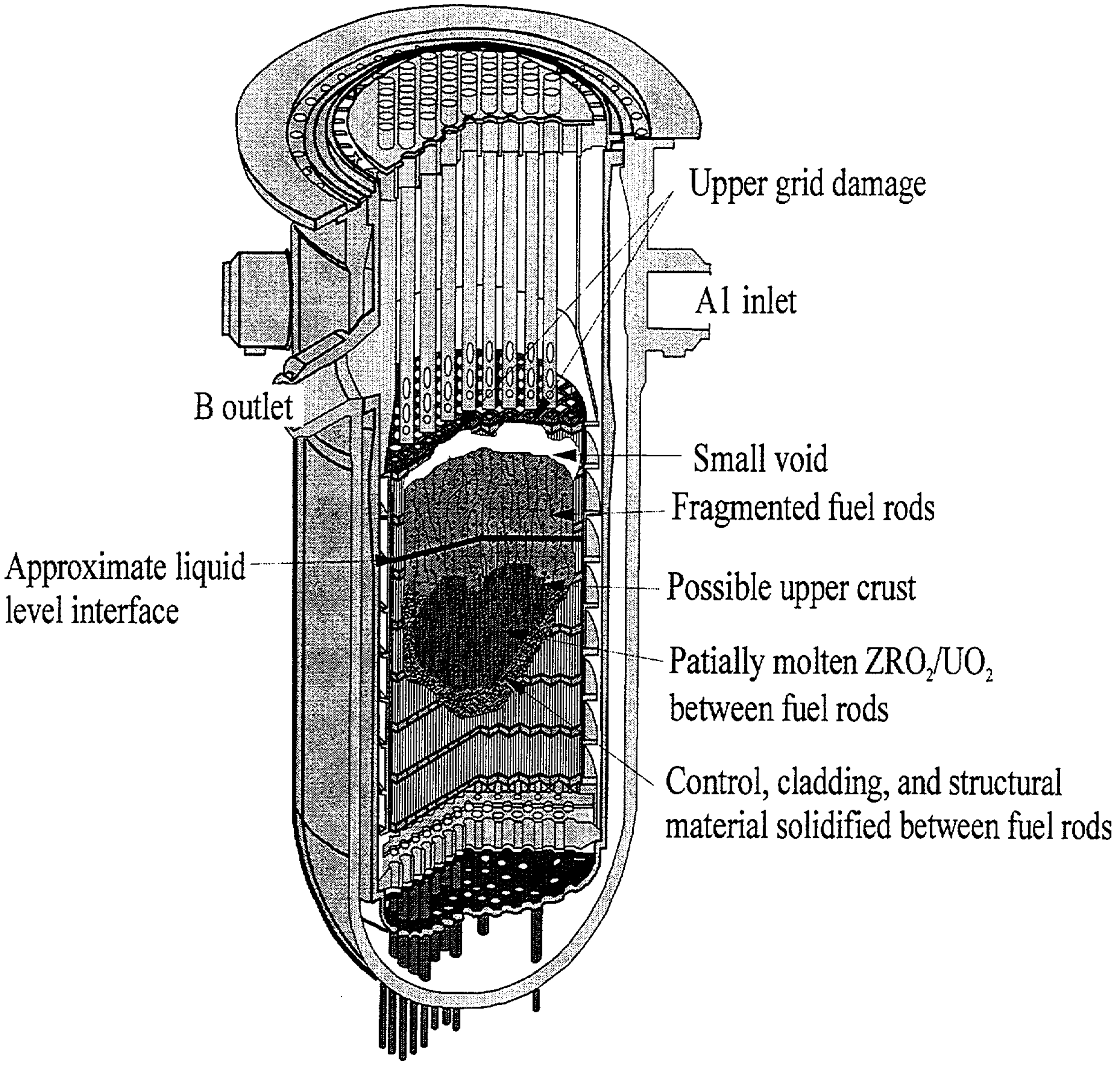

Upper grid damage
A1 inlet
B outlet
Small void
Fragmented fuel rods
Approximate liquid level interface
Possible upper crust
Patially molten ZRO_2/UO_2 between fuel rods
Control, cladding, and structural material solidified between fuel rods

Figure 3.4-6 **Hypothesized TMI-2 core configuration between 174 and 180 minutes**

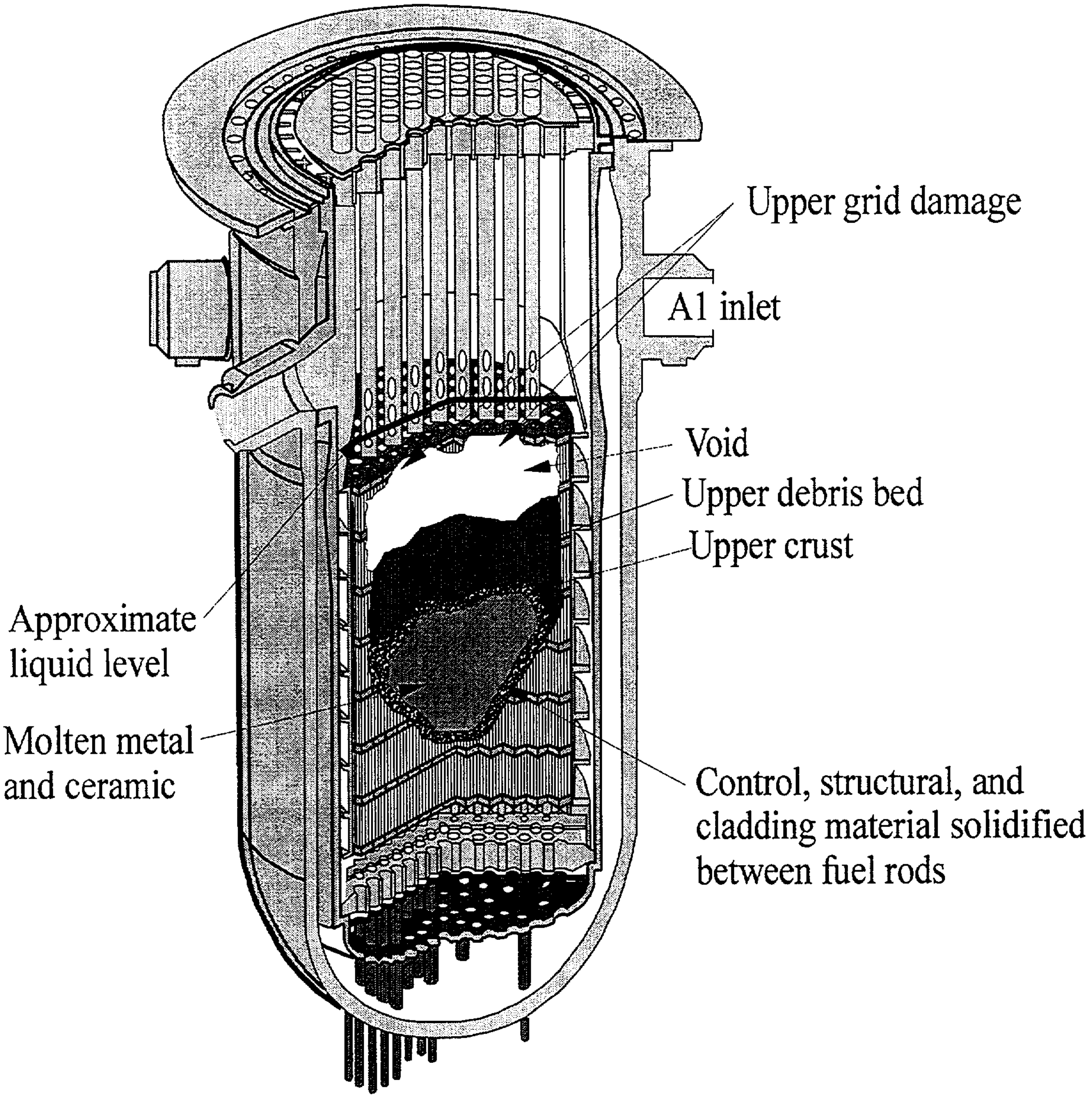


Figure 3.4-7 Hypothesized TMI-2 core configuration at 224 minutes (just prior to molten pour)

References for Section 3.4

1. K. H. Ardron and D. G. Cain, "Core Temperature Transient in the Early Phase of Core Uncovering at TMI-2," *Progress in Nuclear Energy,* 7:197-228, 1981.

2. J. M. Broughton et al., "A Scenario of the Three Mile Island Unit 2 Accident, *Nuclear Technology,* 87(1):34-53, August 1989.

3. P. Hofmann, D. Gerwin Peck, and P. Nikolopoulos, “Physical and Chemical Phenomena Associated with the Dissolution of Solid UO_2 by Molten Zircaloy-4,” PNS-NR.675/82, Karlsruhe, Federal Republic of Germany: Kernforschungszentrum Karlsruhe, GmbH, 1982.

4. P. Hofmann, S. J. L. Hagen, and G. Schanz, "Reactor Core Materials Interactions at Very High Temperatures," *Nuclear Technology,* 87(1):146-186, August 1989.

5. J. B. Rivard, et al., “Identification of Severe Accident Uncertainties,” NUREG/CR-3440, SAND83-1689, U.S. Nuclear Regulatory Commission, September 1989.

6. J. R. Wolf, D. W. Akers, and L. A. Neimark, "Relocation of Molten Material to the TMI-2 Lower Head," *Nuclear Safety*, **87**(1):269-279, July-December 1994.

3.5 Molten Pours onto the Lower Head

Stage 5 begins with the movement of molten fuel-bearing debris into the lower plenum of the reactor vessel. It ends with failure of the reactor pressure vessel and the discharge of fuel debris to the containment. Reactor pressure vessel failure could result from weakening of the lower head or its penetrations due to contact with hot debris. Alternatively, vessel failure could result from an energetic interaction of molten fuel with residual water in the lower plenum. This section discusses accident progression scenarios in the absence of energetic fuel-coolant interactions. The implications of energetic fuel-coolant interactions (steam explosions) are discussed in Section 3.6.

3.5.1 TMI-2 Molten Pour

Relocation of approximately 19.2 metric tonnes of molten core material into the lower head of the reactor vessel occurred between 224 and 226 minutes. This was confirmed by several indicators: a primary system pressure increase of 290 psi (2 MPa), increases in out-of-core source-range neutron detector count rates, alarms of in-core self-powered neutron detectors (SPNDs), alarms of in-core thermocouples, and post-accident measurements of incore thermocouple loop resistances.

The debris configuration that resulted from relocation is depicted in Figure 3.5-1. The crust failure appears to have been in the upper half of the consolidated region near the core periphery. Two mechanisms have been postulated for crust failure. First, continued heating of the molten pool could have lead to melting of the supporting crust, which was thinnest on the top (1 cm versus 10 to 15 cm on the bottom) where heat transfer was greater. Second, at about 220 minutes the pressurizer block valve was opened resulting in a decrease in the reactor coolant pressure of 70 psi (0.5 MPa) between 220 and 240 min.

Post-accident examinations of the eastern half of the core region and lower vessel internals show that the molten pour started on the eastern side of the core. Figure 3.5-2 shows a cross section of the internal structures surrounding the core region. The primary path from the core region was radially outward through a hole melted in the R6 wall of the core former. The core barrel appears to have experienced local surface ablation in this region as indicated in Figure 3.5-3.[1]

Post-accident probings found approximately 4.2 tonnes of solidified fuel debris in the gap between the vertical core former wall and the core barrel at depths depicted in Figure 3.5-3. Another 5.8 tonnes are estimated to have solidified in the core support assembly region. About 19.2 tonnes relocated onto the lower head of the reactor vessel. Examinations of flow holes in the horizontal baffle plates between the core former and the core barrel indicate that nearly the whole volume between plates 6 and 7 filled with molten corium that flowed from the initial core former meltthrough location. The majority of the molten corium then flowed downward through flow holes in plate 7 and ultimately into the reactor vessel lower head.

The lower core support assembly consists of a number of plates and a forging as shown in Figure 3.5-4. There were multiple flow paths through the core support assembly to the lower head. Figure 3.5-5 indicates where solidified material was found in the area between the lower grid and the flow distributor plate, between the flow distributor plate and the grid forging, and in flow holes of the grid forging.[2] The presence of solidified material indicates that molten material flowed through or adjacent to these locations. On this basis, most of the melt flowed down to the elliptical flow distributor on the eastern periphery in the R6/7 and P4/5 areas. Visual examinations indicated that some melt flowed around the perimeter of the core support assembly structures before moving downward.

Figure 3.5-6 indicates the locations in the elliptical flow distributor where solidified material was observed in or above a flow hole.[2] The flow holes indicated in Figure 3.5-6 agree well with those indicated in Figure 3.5-5. In particular, locations H-15, K-15, L-15 indicate flow on both figures, and flow location C-14 in Figure 3.5-5 is near locations D-13 and D-14 in Figure 3.5-6. The melt appears to have dropped onto the lower head from several different locations around the periphery of the elliptical flow distributor.

As the melt moved downward from the core region, heat was lost to the vertical core former, to the core barrel, to the horizontal baffle plates, to the lower core support assembly, and to water that filled the lower plenum. Minimal damage observed to the elliptical flow distributor suggests that the initial material reaching the lower head was relatively cool. It is possible that the material was mobile at temperatures below the solidus temperature of (U,Zr) O_2 owing to the presence of phases with higher metal content and lower melting temperatures.

Rapid steam production occurred as a result of heat transfer from the molten core material to water in the lower head. Nothing in the recorded data or post accident core conditions suggests an energetic steam explosion (see Section 3.6) occurred as the tons of molten core material relocated into the lower plenum with the reactor vessel nearly full of water.

Figures 3.5-7 and 3.5-8 depict the ultimate hard debris layer that formed in the lower head.[2] The layer depths were established by mechanical probing during defueling operations. The steep cliff-like profile around the periphery of the hard layer indicates rapid freezing of relatively cold debris. A high initial temperature or remelting would have resulted in a flatter profile near the periphery. On the other hand, it is now clear that high temperature melt existed and caused some damage in the more central regions of the lower head (see Section 3.5.4).

3.5.2 Alternative Melt Flow Scenarios

In core melt scenarios involving the formation of blockage in the core region, configurations similar to that at TMI-2 are postulated. The formation of a molten pool contained within a crucible-like bottom crust is envisioned with unmelted ceramic (UO_2) and metallic material either adding to the pool from above or forming a rubble bed above an upper crust as at TMI-2.

The size of the molten region grew due to continued addition of decay heat (reduced by the loss of volatile fission products during liquefaction). With a total loss of coolant injection, the residual water level could drop below the bottom of the active core and structures supporting the mass of the crust and melt could weaken as depicted in Figure 3.5-9. Given a failure of the core support structures or a breakthrough of suspended melt as occurred at TMI-2, substantial quantities of melt could suddenly plunge into the residual water in the lower plenum. On the other hand, a massive, coherent pour of molten material is not the only scenario that can be envisioned. Local crust failure could result in a narrow continuous pour over a fraction of a minute to several minutes. Alternatively, if there were little residual water present, a strong crust might not form in the core region. In this case the discharge of molten material from the core might occur in a narrow discontinuous stream or streams distributed over the duration of the core meltdown.

The rate of formation of liquefied fuel is slow compared to all but the very slowest discharge rates. Thus, if a large fraction of the core is liquefied at the onset of discharge, a larger amount might be discharged. Conversely, if only a small fraction is liquefied at the onset of discharge, much smaller discharge rates would result.

3.5.3 Debris on TMI-2 Lower Head

During the TMI-2 defueling, the solidified layer of debris in the lower head was found to be very hard. It had to be broken apart by dropping a 300 lb (136 kg) hammer from an elevation of 20 ft (6.1 m). Once the material was broken into pieces, there was virtually no adherence to the lower head itself. Representative samples of the solidified layer were obtained for examination. Because the hard layer had to be broken into pieces, however, information regarding variability in debris properties with depth could not be obtained. Results of physical and radiochemical examinations, which are discussed in detail elsewhere,[3] are summarized below.

The debris was generally a dull grey ceramic with some areas of yellow (probably hexavalent uranium). The average density of the samples was 8.7±0.4 g/cm^3. By comparison, the density of UO_2 fuel pellets is about 10.8 g/cm^3. The average porosity for all samples was 18±11%, reflecting a very wide range. As indicated in Table 3.5-1, the elemental composition of the debris was found to be very similar to that in the original core, but with slightly more uranium and slightly less zirconium.

Figure 3.5-10 shows cross-sectional views of one sample with apparently connected pores in the longitudinal sections. Such interconnected pores were observed in many of the samples and may have been caused by bubbling of steam or structural material vapors through the melt when it froze. As indicated in Figure 3.5-11, sçanning electron microscope examinations revealed a light uranium-rich $(U,Zr)O_2$ phase away from the pores. A dark, zirconium-rich $(Zr,U)O_2$ phase was often found adjacent to the pores. Based on the time required for such visible phase separation to occur, the debris cooling time was estimated to be from 3 to 72 hours. The lack of complete phase separation implies a cooling time toward the lower end of this range. As discussed later, however, tests of metal samples from the lower head and analyses of potential vessel failure modes imply a much shorter (~30 min.)

quenching time. This apparent discrepancy has not yet been explained.

Dissolution techniques were used to measure the retention fractions of several key radionuclides in the debris. The analyses indicated that only small fractions of volatile radionuclides like Cs-137 were retained, but most of the low volatility radionuclides were retained. The decay heat generation rate in the debris on the lower head was estimated to be 0.13 watts per gram (w/g) of uranium just after the molten pour.[3] This compares to 0.18 w/g of uranium if all radionuclides had been retained.

3.5.4 Hotspot in TMI-2 Lower Head

The condition of the TMI-2 incore instrument nozzles following debris removal from the lower head is depicted in Figure 3.5-12. As indicated by the section view in Figure 3.5-8, some nozzles had been completely buried in solidified debris but showed absolutely no damage. Other nozzles were partially melted, and nine nozzles (E-7, E-9, F-7, F-8, G-5, G-6, G-9, H-5, and H-8) were completely melted off. The following explanation accounts for these various degrees of damage.

The portion of the molten pour that initially contacted the lower head is believed to have been substantially cooler than material that reached the lower head later. The initial material lost more heat to the core baffle and former plates, the core barrel, the lower core support assembly, and the water that filled the lower plenum. The lower head itself provided an additional heat sink.

The initial cooler material fell to the lower head from several different locations and is believed to have rapidly frozen to form a cup-shaped basal crust structure that protected lower head and nozzles in these areas. Hotter material flowed downward across the top of this insulating crust. Unprotected nozzles in the flow paths of the hotter material were melted off. The height at which a nozzle melted off indicates the depth of the insulating crust that surrounded the nozzle. The protective crust thickness was negligible at location E-9, ~15 cm at location H-5, and ~25 cm at location M-9 (see Figure 3.5-12).

In February 1990, 14 nozzles, 2 guide tubes, and 15 lower head steel samples, were removed from the TMI-2 vessel. Figure 3.5-13 shows the locations of these samples. (The stubs of nozzles E-9, F-7, F-8, G-6, and G-9 were too short to be removed.) Figure 3.5-14 shows the as-removed appearance of six nozzles. The 15 lower head steel samples extended about half way through the 5.6 inch (14.2 cm) thick vessel. Figure 3.5-15 illustrates the prism shape of the vessel material samples. Significant insights regarding potential lower head failure modes were obtained based on tests and analyses performed on these samples. It was determined that an elliptical hot spot (approximately 1×0.8 m) formed where the insulating crust thickness was negligible. This hot spot is depicted in Figure 3.5-16.[4] Within the hot spot temperatures from ~800 to 1100°C (1472 to 2012°F) persisted for approximately 30 minutes. Cooling then occurred rapidly (10-100°C/min.).[5] Outside the hot, spot, lower head temperatures remained below the 727°C (1341°F) austenitic to ferritic transition temperature; however, some areas may have been close to this temperature. The temperature gradient through the lower head was 20 to 40°C/cm.

3.5.5 Early Views of Lower Head Failure

As mentioned in Sections 3.3.5 and 3.4.6 and illustrated in Figure 3.3-8, the strength of steel decreases rapidly as its temperature exceeds 1000°F (538°C), which is far less than the steel melting point. Early investigators focused on global weakening accompanied by large plastic deformations of the entire lower head as the most likely vessel failure mode. If large fractions of the core were postulated to be molten in the lower head, estimates of the time required for failure varied from 22 min. to 40 min., depending on whether the vessel was assumed to be pressurized or not.[6]

The 80 minute maximum duration with total loss of coolant injection given in Table 3.3-1 for Stage 5 results from combining the maximum estimated time-to-breach for the reactor vessel (40 minutes) with a scenario in which the molten core material flowing into the lower head is initially quenched by the water remaining there and must then reheat to cause vessel failure.

In a 1981 risk assessment of the Zion plant, an alternative mechanism for lower head failure was identified.[7] Local meltthrough was postulated to occur at an incore instrument tube penetration. The time to failure identified for this mode was 5 to 7 minutes, independent of relative pressure.

3.5.6 Lower Head Failure Modes Analyzed for TMI-2

The preceding lower head failure analyses do not apply to the TMI-2 accident where only a limited mass (~19.2 tonnes) of molten core debris relocated to the lower head. The TMI-2 lower head did not fail in spite of the hot spot that existed for about half an hour. In 1994, analyses were performed to investigate what modes of failure might have occurred had the accident proceeded further without efficient cooling of debris in the lower head. As illustrated in Figure 3.5-17, four temperature-related failure modes were analyzed.

Tube Rupture - The tube rupture mechanism shown in Figure 3.5-17a would result from a combination of high pressure and elevated ex-vessel tube temperatures caused by penetration of hot debris through the tube to ex-vessel locations. Data from some of the TMI-2 instrument nozzles were used to calibrate a melt-penetration model. Model predictions indicate that molten fuel did not penetrate through the instrument tubes to locations below the lower head. Ex-vessel tube rupture was therefore not a significant threat at TMI-2.

Weld Failure, Tube Ejection - Failure of a penetration tube weld (Figure 3.5-17b) could result from attack and sustained heating by debris surrounding a tube in combination with high reactor coolant system pressure. At TMI-2, metallurgical evidence indicates that the Inconel penetration welds did not melt.[8] Analysis results obtained in 1994 indicated that this failure mode would not have occurred first at TMI-2. Results of a subsequent lower head failure experiment (see Section 3.5.7) show, however, that deformation of the lower head can indeed cause penetration welds to fail first.

Global Failure by Uniform Heating - Based on the TMI-2 debris composition, it is likely that the molten material reached temperatures greater than 2600°C (4712°F) in the central core region before relocation. The temperature of the debris when it reached the lower head is not known; however, it reached the lower head in a molten state, and results of the debris sample examinations suggest slow cooling. Consequently, analysts examined the potential for vessel failure due to prolonged uniform heating by the debris that reached the lower head. Heat transfer from the debris to the lower head was modeled as depicted in Figure 3.5-17c. With no allowance for rapid cooling of the debris, global failure of the lower head was predicted to occur within 1.7 to 2.3 hours of the molten pour.[9]

Local Failure by Peaked Heating - Calculations were also performed to assess the margin to failure due to the high temperatures in the hot spot. The existence of the hot spot was simulated by imposing surrounding (background) temperatures consistent with a lower rate of debris to vessel heat transfer as depicted in Figure 3.5-17d. When the hot spot temperatures were imposed with a background temperature of only 327°C (621°F), the vessel was predicted to survive. When the hot spot temperatures were imposed with a background temperature near the 727°C (1341°F) ferritic to austenitic steel transition temperature, lower head failure was predicted to occur 1.5 hours after the molten pour.

3.5.7 Lower Head Failure Experiments and Analyses

The analyses of material samples and failure modes described in the preceding sections do not fully explain the known outcome of the TMI-2 accident (the vessel did not fail). The hypothesis that rapid cooling of debris by water prevented lower head failure is examined in Section 3.5.8. To assess the validity of lower head failure models, the NRC sponsored a series of Lower Head Failure (LHF) experiments and analyses,[10] which are discussed in this section.

The LHF experiments were performed using 1-to-4.85 linear scale models of a typical PWR lower head. The test vessel was basically a scaled version of the lower part of a TMI-like reactor pressure vessel without the vessel skirt. Linear scaling was used to preserve the membrane stress. The prototypic material for U.S. PWRs (SA533B1) was used to preserve the material behavior. The heat flux, which was applied using internal radiant heaters, was scaled by the linear scale factor to preserve the creep and failure time. As a result of the heat flux scaling, the throughwall temperature differential decreased by the square of the scaling factor, and the throughwall temperature difference was typically about 10 K (18°F).

To be useful for model validation, the experiments were designed with well-characterized initial and boundary conditions and with sufficiently detailed measurements of temperature, pressure, and displacement histories. Maps of the vessel shape (including wall thickness) were obtained before and after each test.

A series of eight experiments was conducted. The test conditions were selected to examine the effects of spatial heat flux distribution, pressure, and construction features on lower head deformation and failure. Three temperature distributions were used: uniform, center-peaked, and edge-peaked. A uniform distribution might occur in scenarios where the core melt gradually relocated to the lower head. Center-peaked distributions are representative of the hot spot that occurred at TMI-2. Edge-peaked distributions simulate the presence of a convecting molten pool. All of the experiments were conducted at a pressure of 10 MPa (1450 psig) except LHF-7, which was conducted at 5 MPa (775 psig). A pictorial summary of all eight LHF experiments is presented in Figure 3.5-18. Table 3.5-2 summarizes the test conditions and key results of all the experiments.

In all of the experiments large deformations in the geometry of the lower head were observed following the onset of creep. The temperature for the onset of creep for experiments conducted at 10 MPa was fairly consistent, ranging from 935 K to 997 K (1223°F to 1335°F). The temperature at which the lower head failed in the 10 MPa experiments was also fairly consistent, ranging from 1006 K to 1114 K (1351°F to 1546°F). In LHF-5, which was the only test with penetrations installed in the lower head, failure occurred prematurely by leakage around circumferential welds that connected the penetrations to the surrounding vessel. The diameter of the penetration through holes increased by as much as a factor of two indicating how global head deformations can impact the stress state in penetration welds.

In LHF-4, a leak developed causing the vessel pressure to decrease to 7.7 MPa (1117 psig). The pressure was increased back to 10 MPa rapidly while the vessel temperature was just under 1000 K (1340°F), which is above the previously observed temperature for the onset of creep. The vessel deformation rate immediately increased, and the vessel failed catastrophically. This illustrates how repressurization at elevated temperature can cause lower head failure.

LHF-7 was a replicate of LHF-1, except the test pressure was reduced from 10 MPa to 5 MPa. The overall deformation of LHF-7 was comparable to that of LHF-1, but the vessel failure was different. Lowering the driving pressure elevated the temperature for the onset of creep and the temperature for vessel failure. While all experiments at 10 MPa had severe necking and a thickness reduction of about a factor of 10 at the failure location, the thickness reduction for LHF-7 was only a factor of two.

LHF-6 was designed to investigate the susceptibility of vessel welds, but the welds were not challenged and LHF-6 was essentially an exact replicate of LHF-1. Similarly, in spite of slight difference in the location of the edge-peaked heat flux, LHF-8 was essentially an exact replicate of LHF-3.

Generally, the tests show that regions of weakness (reduced thickness or elevated temperature) are most likely to fail. The uniform heat flux failures typically occurred in regions of reduced wall thickness. For cases where there was localized heating, failure always occurred in regions of maximum temperature. The difference in load-carrying capability need not be very large. The failure region in LHF-1 was less than 5% thinner than the surrounding region.

The repeatability of the LHF tests and model comparisons to the test results suggest that with adequate information (heating rates and patterns, pressure transients, vessel thickness profiles, material properties, and penetration characteristics) modeling of the mode and timing of lower head failure may be possible. However, the LHF experiments constitute an incomplete data base with respect to possible in-vessel pressures, pressure transients, and through-wall temperature drops. They also suggest the need for better characterization of vessel material properties. Consequently, although the heating rates and patterns and the pressure history at TMI-2 are fairly well documented; it remains to be demonstrated that state-of-the-art models would produce TMI-2 predictions that are in agreement with the intact end-state of the TMI-2 lower head.

Lower head failure predictions for hypothetical severe accidents are even more problematic. Details regarding plant-specific lower head thickness and contour variations, welds, and penetrations are seldom available to severe accident analysts, and the ability to model debris relocation from the core region to the lower head, the resulting debris configuration, the composition and properties of the debris, and the associated heating rates and patterns is quite limited. Finally, as discussed in Section 3.5.8, quenching mechanisms that could prevent lower head failure if water is present or reintroduced are poorly understood.

One thing is certain: if water is unavailable, or if lower head damage proceeds too far before water is reintroduced, lower head failure due to creep can occur.

3.5.8 Debris Coolability

Debris cooling experiments performed before the TMI-2 reactor pressure vessel investigations did not focus on water cooling of molten debris. Instead, they focused on determining conditions under which water covered beds of internally heated solid particles reach dryout. Dryout occurs when debris to coolant heat transfer rates are high and steam flow rates out of the debris bed prevent sufficient water from reaching the bed interior as illustrated in Figure 3.5-19.

Such experiments and models developed from them indicate some key factors affecting the coolability of debris beds.[11] These factors include the bed power, the bed configuration, and particle sizes. The higher the power generated in a bed, the more difficult the bed is to cool. The bed power at which some part of a flooded bed drys out is called the dryout power. If flooded from above, deeper debris beds tend to be less coolable than shallow debris beds of the same volume.

Figure 3.5-20 shows the impact of particle size on the dryout heat flux (dryout power divided by top surface area of the bed) for beds flooded from above.[12] In beds of smaller particles, the surface area for heat transfer is larger, and therefore the vapor generation rates are increased relative to water ingress rates. Many particle sizes are possible during a severe accident, ranging from fractions of millimeters up to centimeter size and larger. There is no one exact particle size that defines a threshold for coolability. However particle sizes of a few millimeters and smaller, which could result from steam explosions (see Section 3.6), are most likely to be noncoolable.

A deep bed, sufficiently small or stratified particle sizes, and/or a small coolant fraction could produce dryout in the bed even after it is initially quenched.[13] Forced circulation of coolant through some possible configurations of in-vessel debris would be required to prevent dryout. Maintaining forced circulation was considered to be of paramount importance once it was re-established at TMI-2.

Even with forced circulation, melting in the interior of a large debris bed could occur, and quenched or partially quenched debris could remelt even with forced circulation. Natural processes (such as capillary flow) tend to cause a melting debris bed to crumble. That is, melt flows through the open porosity toward the debris bed boundary where it freezes and forms a crust. If the crust is a poor conductor (e.g., an oxide), then very little of the energy is transferred out of the bed. A molten pool would form and very high temperatures could be attained in the melt. Upward radiative heat transfer could cause melting of vessel upper internal structures, which would fall and increase the metallic content of debris in the lower head. Models have been developed to analyze debris bed heatup, remelting, and lower head response.[14]

Cooling of lower head debris at TMI-2 may have occurred in two ways. To explain why temperatures surrounding the hot spot were low enough to preclude local failure, a slow cooling mode has been postulated in which channels or cracks in the debris allowed for infusion of water that cooled the debris near the channels but left interior portions hot. To explain the cooling rates observed in the metallurgical samples a rapid cooling mode has been postulated in which gaps or channels between the lower debris crust and the lower head allowed relatively high flow rates of coolant to the hot spot. Water ingress between the lower crust and the vessel might be facilitated by deformation of the lower head; however, there were no observable deformations in the geometry of the TMI-2 lower head.

A mass-energy balance on the reactor coolant system was performed based on plant data regarding letdown, relief valve, and makeup flow rates following the molten pour. The results, though not precise, confirm that a decrease in debris internal energy occurred in the 2 hours following the molten pour. This supports the hypothesis that debris cooling occurred at a rate faster than indicated by the physical appearance of the debris samples.[8]

Even if one accepts the unanticipated cooling mechanisms that seem to have occurred at TMI-2, more debris in the lower head, hotter debris in the lower head, failure to keep the debris covered by water, or late introduction of water can lead to global or local temperature-induced failure of the lower head in hypothesized severe accidents.

3.5.9 Advanced Design Concepts

Several studies have been conducted to examine the potential for maintaining core and structural debris within the reactor vessel by flooding the containment to the extent that water covers the outer surface of the lower portion of the reactor vessel.[15,16,17] In general, experiments have shown that the required wall cooling could be accomplished without departure from nucleate boiling at the outer wall surface.[16,17] Nevertheless, there are many practical difficulties from the standpoint of providing the volume of water that would be necessary to invoke this strategy in an assured and timely manner because existing plants were not designed to provide such a flooding capability (see also Section 3.7.7).

Advanced designs such as the Westinghouse AP600 have implemented design features aimed at assuring in-vessel retention of molten debris. First steps have been taken to allow vessel depressurization thereby decreasing the differential pressure loads imposed on the lower head. Second, the lower head has been designed without penetrations so failure mechanisms associated with such penetrations are precluded. Finally, the reactor cavity can be flooded with water, so that heat transfer through the lower head to surrounding water can be used to prevent lower head failure due to creep rupture.[18]

Table 3.5-1 Average TMI-2 Lower Head Debris Composition by Quadrant (wt%)[a]

Element	Southeast	Southwest	Northeast	Original TMI-2 Core[b]
U	72.3	70.8	68.2	65.8
Zr	14.1	15.2	15.2	18.0
In	0.28	[c]	[c]	0.3
Cr	0.33	0.52	0.52	1.0
Fe	0.74	0.93	0.93	3.0
Mn	0.03	0.28	0.028	0.8
Ni	0.099	0.81	0.10	0.9
Total[d]	87.8	84.3	85.1	92.14

[a] Extracted from Reference 1, which cautions that because of the small number of samples examined these data should be used with caution.

[b] Composition of original TMI-2 core is computed in Reference 1.

[c] Below analytic detection limit. Elements Sn, Ag, Al, Mo, and Nb were also below their analytic detection limits. Detection limits vary from element to element; however, a nominal value is approximately 0.1 wt%.

[d] The total is for measurable constituents. Oxygen was not measured.

Table 3.5-2 Summary of lower head failure experimental results

Test	Heat Flux Distrib.	Test Press. (MPa)	T_{in} (K)	T_f (K)	RPV Features	Failure size/initiation location overall strain/Wall thickness at failure
LHF-1	Uniform	10	935	1038	None	49 cm x 25 cm oval, 1.66 m FSE /66° 33%/3 mm
LHF-2	Center Peaked	10	958	1010	None	4 cm x 7 cm oval, 0.23 m FSE/77° 35%/3 mm
LHF-3	Edge Peaked	10	980	1006	None	3.8 cm wide by 55 cm tear, 0.63 m FSE/33.5° 11%/3 mm
LHF-4	Uniform	10	949	977	30 scaled penetrations between 55° and 90° (bottom center) latitude	Penetration weld failure at weld/base-metal interface with less than 1 mm separation. Holes for penetration doubled in size.
LHF-5	Edge Peaked	7.7-10	997	1114	9 scaled penetrations between 41° and 80° latitude	Vessel unzipped, 3.5 m FSE
LHF-6	Uniform	10	949	1052	vessel with typical welded construction consisting of a bottom dish and a 4-segment upper torus.	17.8 cm x 10 cm oval, 0.63 m FSE/ 74°29%/4 mm
LHF-7	Uniform	5	992	1200	None	Latitudinal rip 1.6 mm wide and 29 cm long, 0.32 m FSE/30%13 mm
LHF-8	Edge Peaked	10	967	1041	None	1.2 cm wide by 31.7 cm tear, 0.28 m FSE/25° 10%/5mm

T_{in} = Temperature for creep initiation, T_f = Vessel failure temperature
FSE = full scale equivalent hole diameter

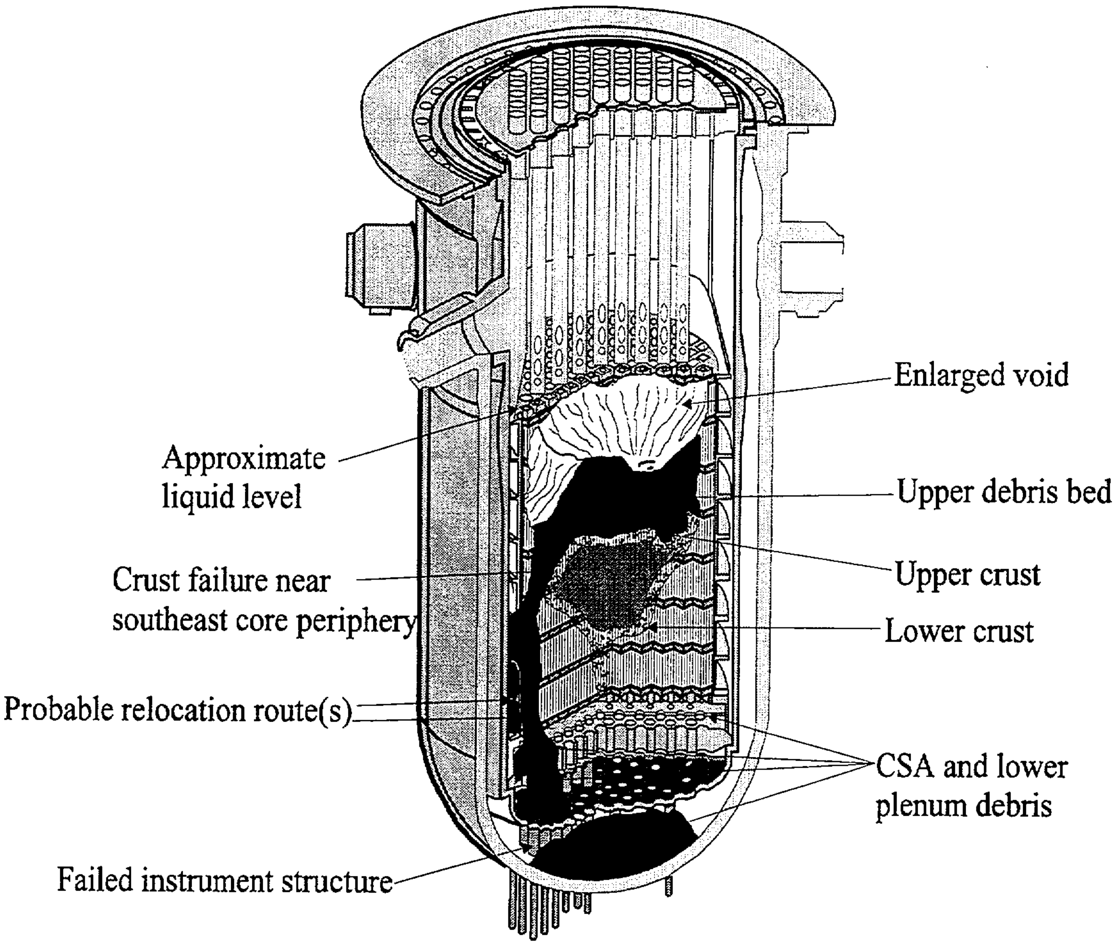

Enlarged void
Approximate liquid level
Upper debris bed
Crust failure near southeast core periphery
Upper crust
Lower crust
Probable relocation route(s)
CSA and lower plenum debris
Failed instrument structure

Figure 3.5-1 Final TMI-2 debris configuration

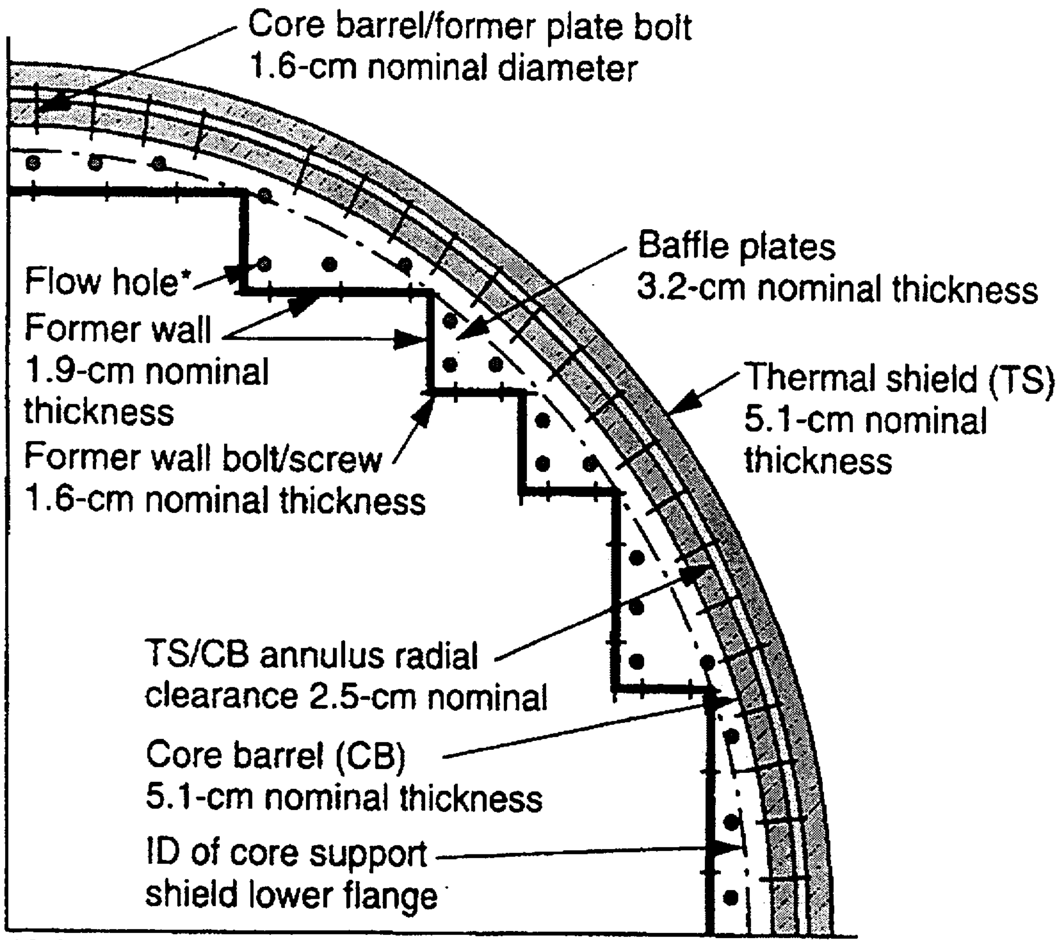


Figure 3.5-2 TMI-2 structures surrounding the core

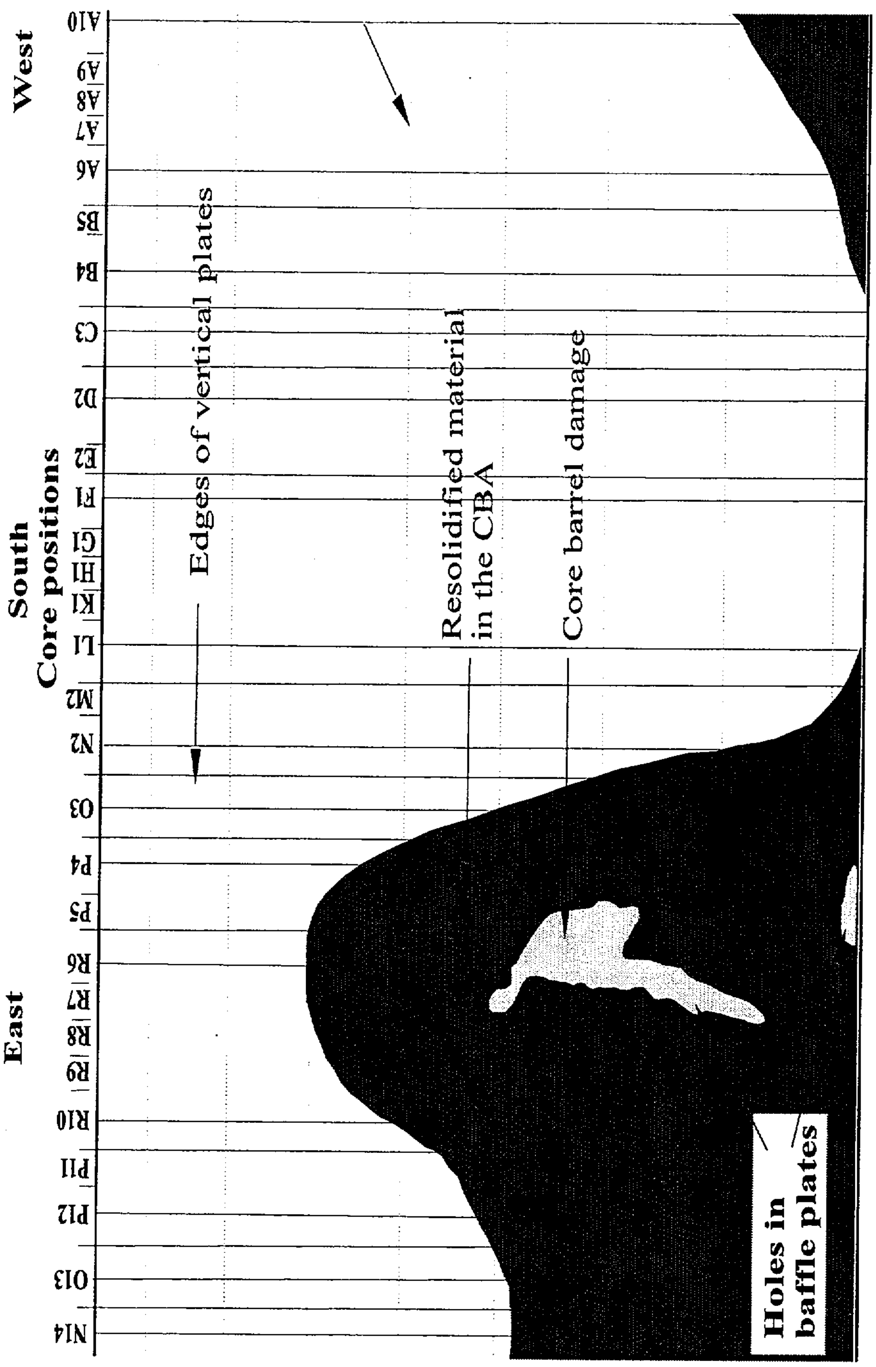


Figure 3.5-3 Fuel debris profile inside TMI-2 core barrel assembly (CBA laid flat)

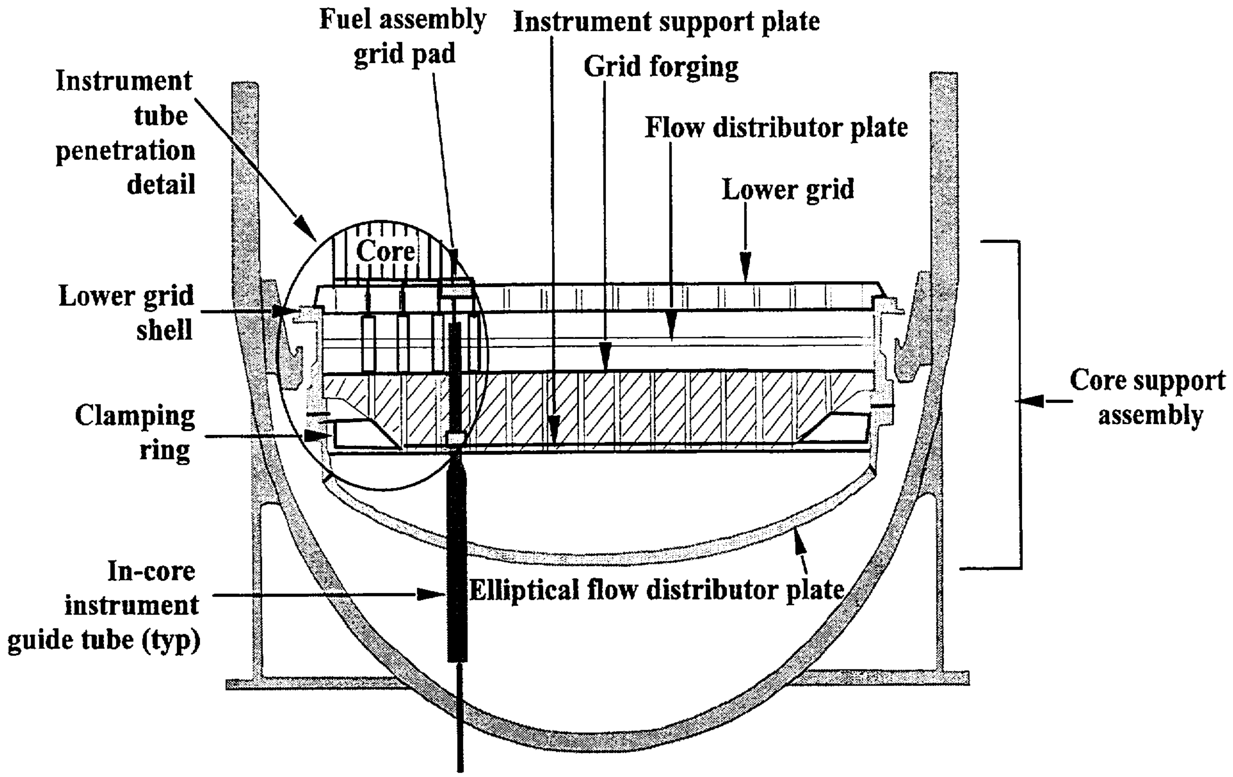


Figure 3.5-4 TMI-2 core support assembly

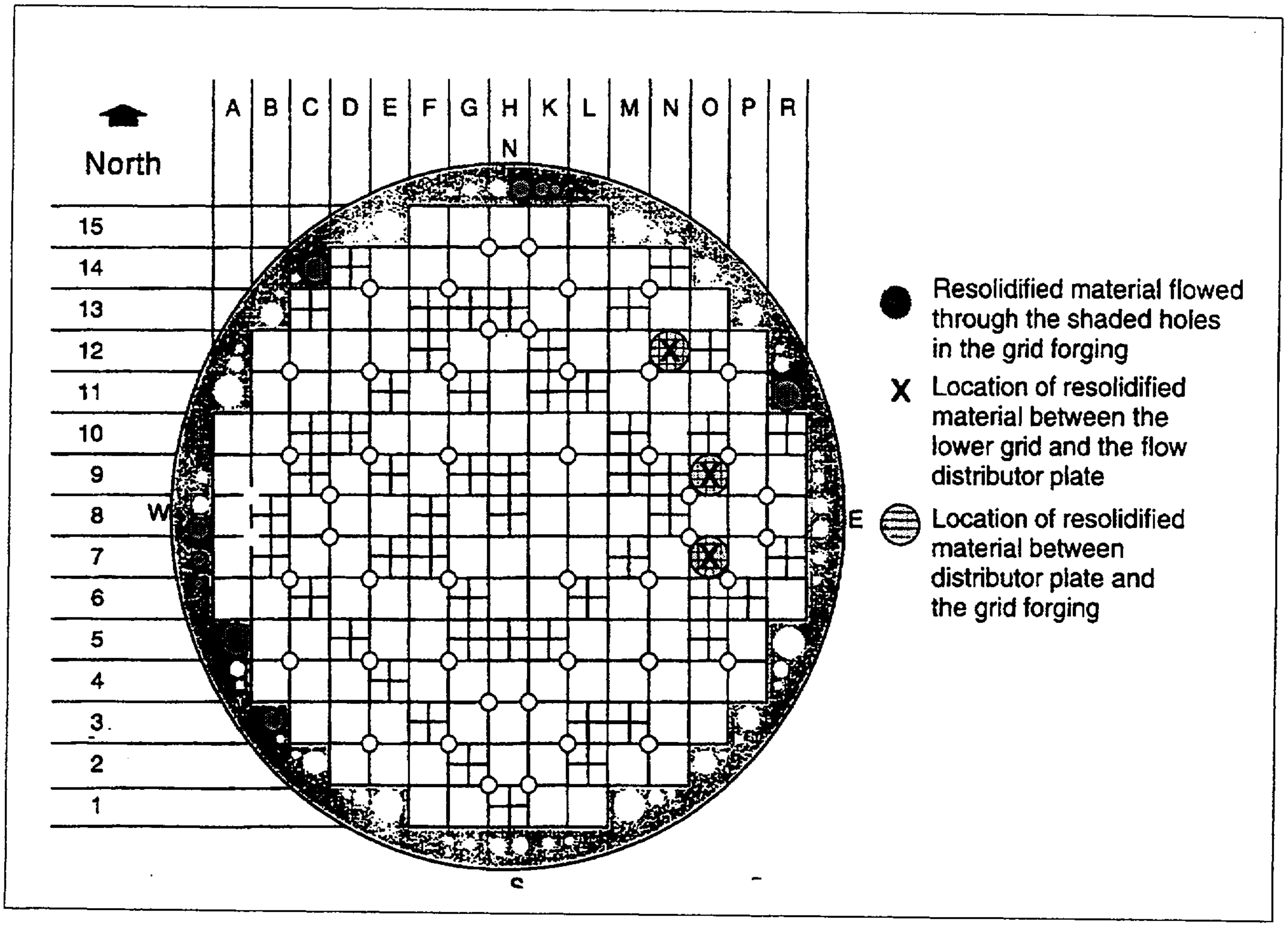

North
A
B
C
D
E
F
G
H
K
L
M
N
O
P
R
N
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
W
E
S
● Resolidified material flowed through the shaded holes in the grid forging
X Location of resolidified material between the lower grid and the flow distributor plate
⊜ Location of resolidified material between distributor plate and the grid forging

Figure 3.5-5 Locations of solidified material in TMI-2 core support assembly

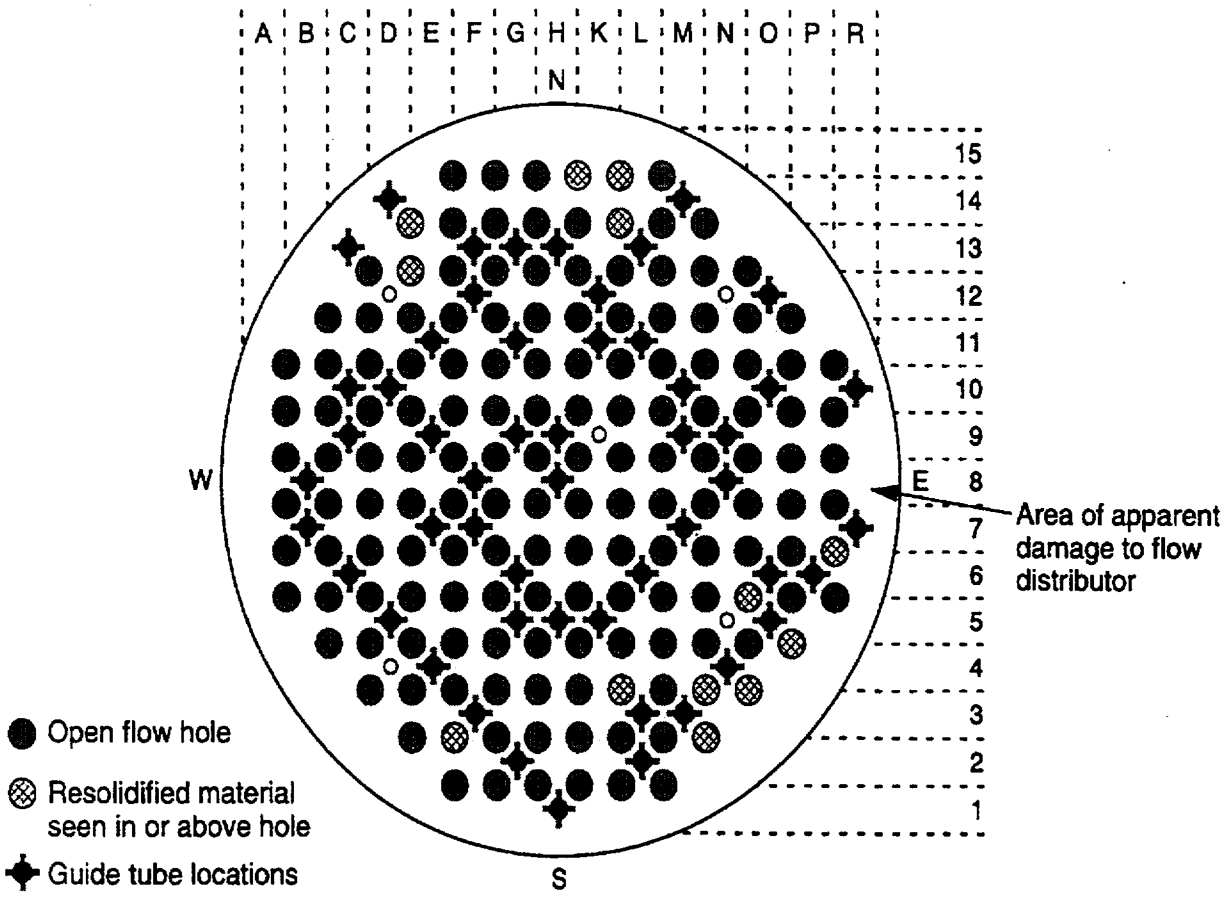

A
B
C
D
E
F
G
H
K
L
M
N
O
P
R
N
W
E
S
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
Area of apparent damage to flow distributor
● Open flow hole
▨ Resolidified material seen in or above hole
✦ Guide tube locations

Figure 3.5-6 Locations of solidified material TMI-2 elliptical flow distributor

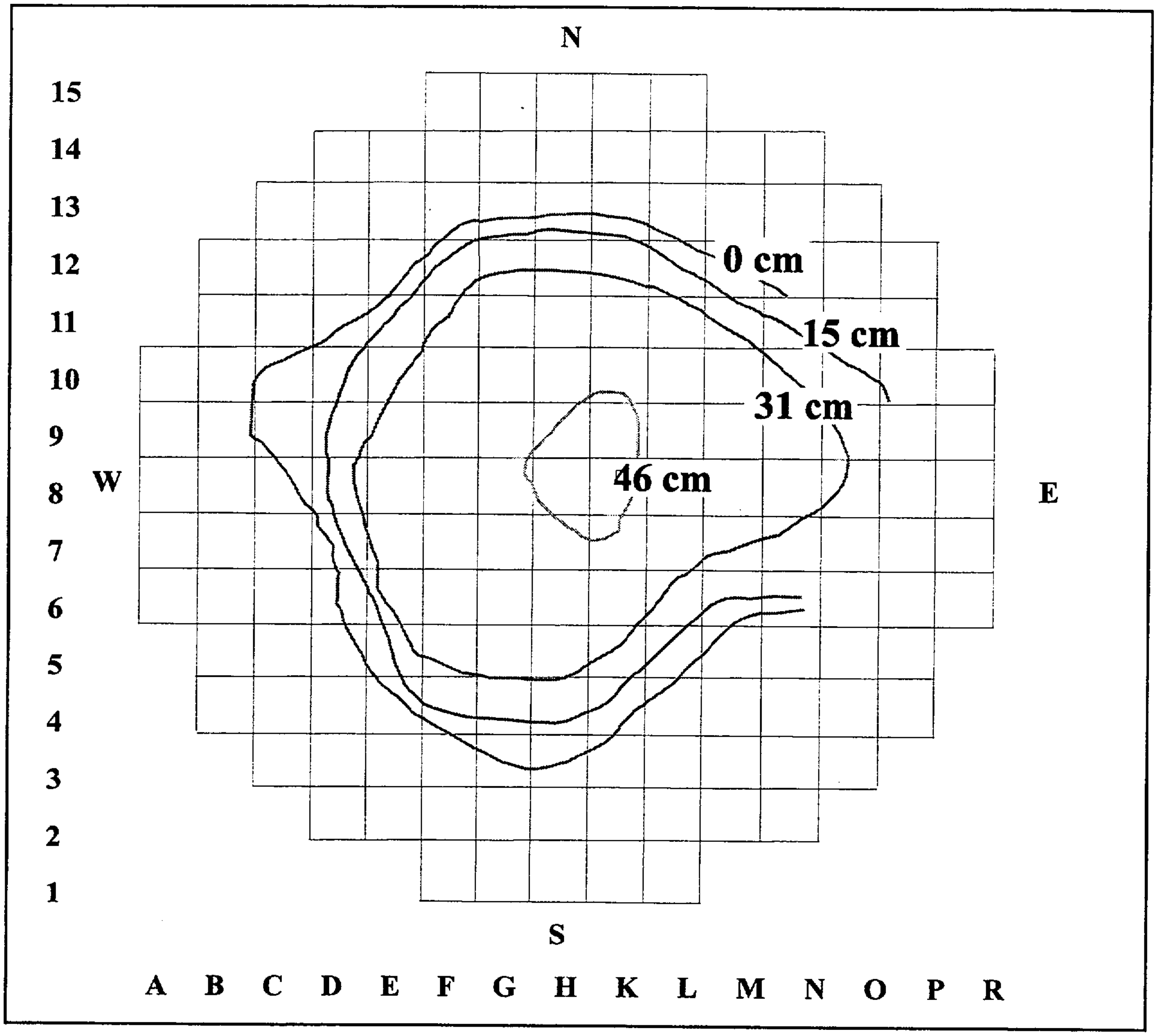


Figure 3.5-7 TMI-2 hard layer debris depths in lower head

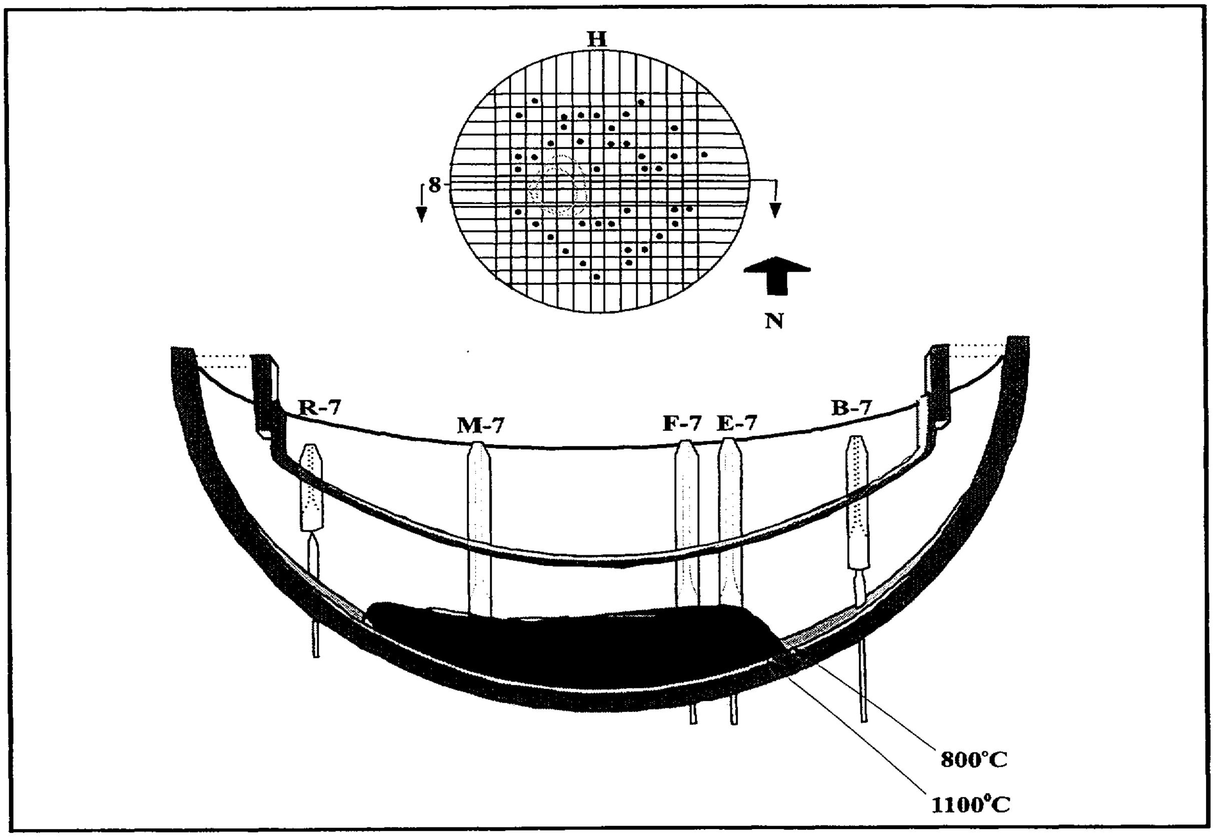


Figure 3.5-8TMI-2 lower-head cross section of hard debris, row 7

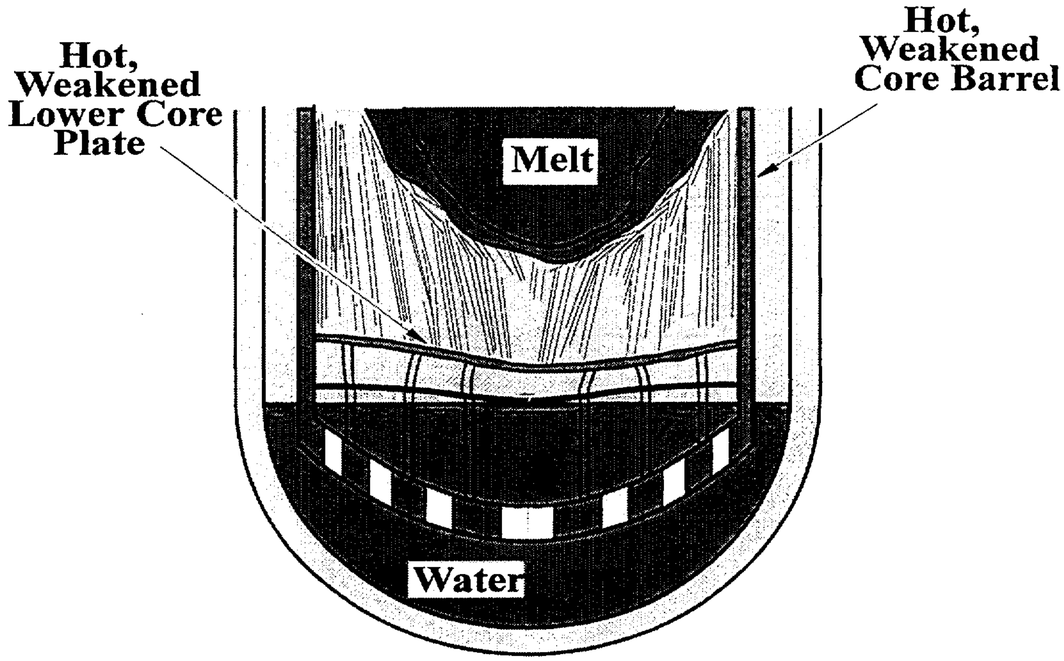


Figure 3.5-9 Visualization of the downward progress of a coherent molten mass as the below-core structures weaken

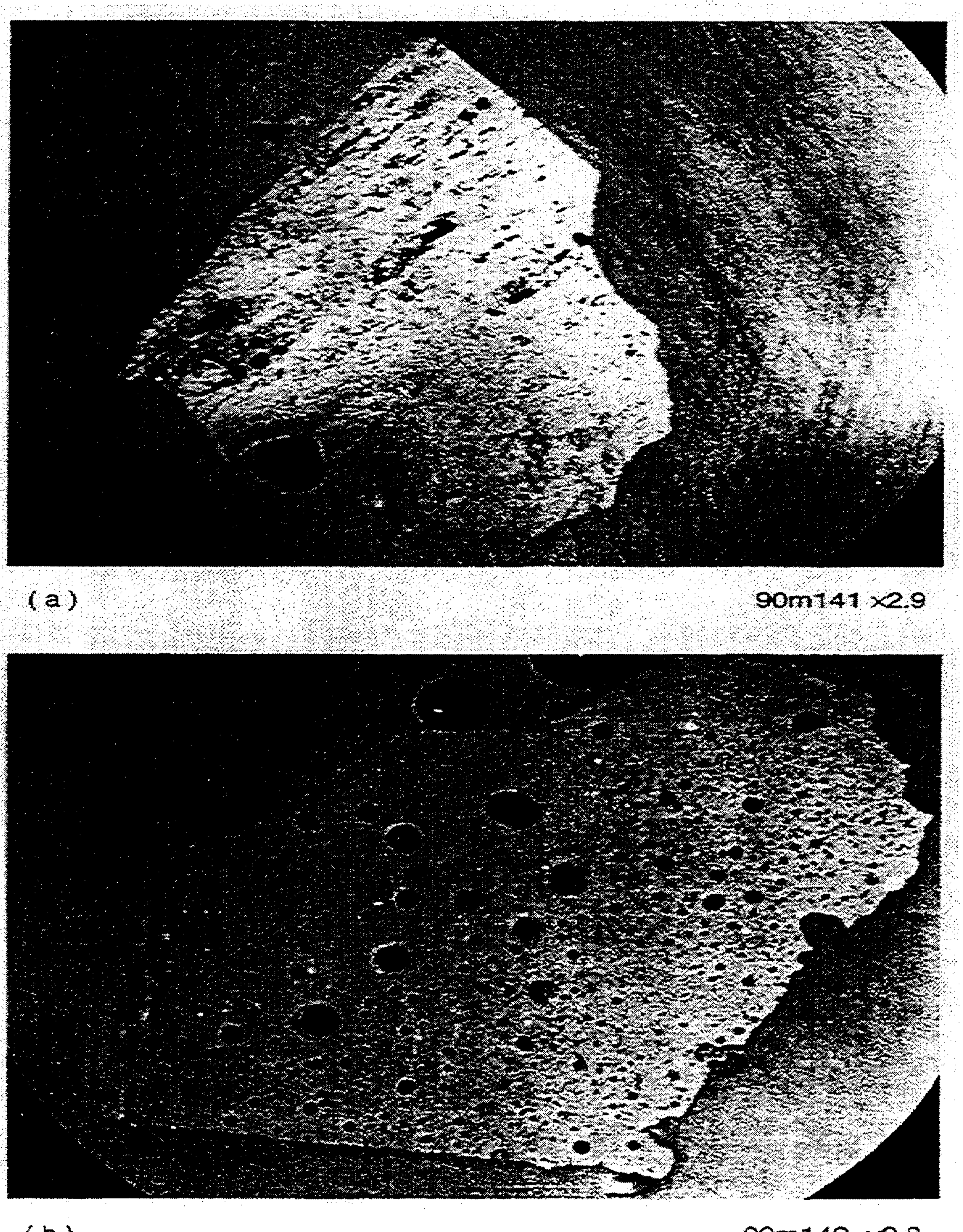


Figure 3.5-10 Cross-sectional views of TMI-2 hard layer debris sample

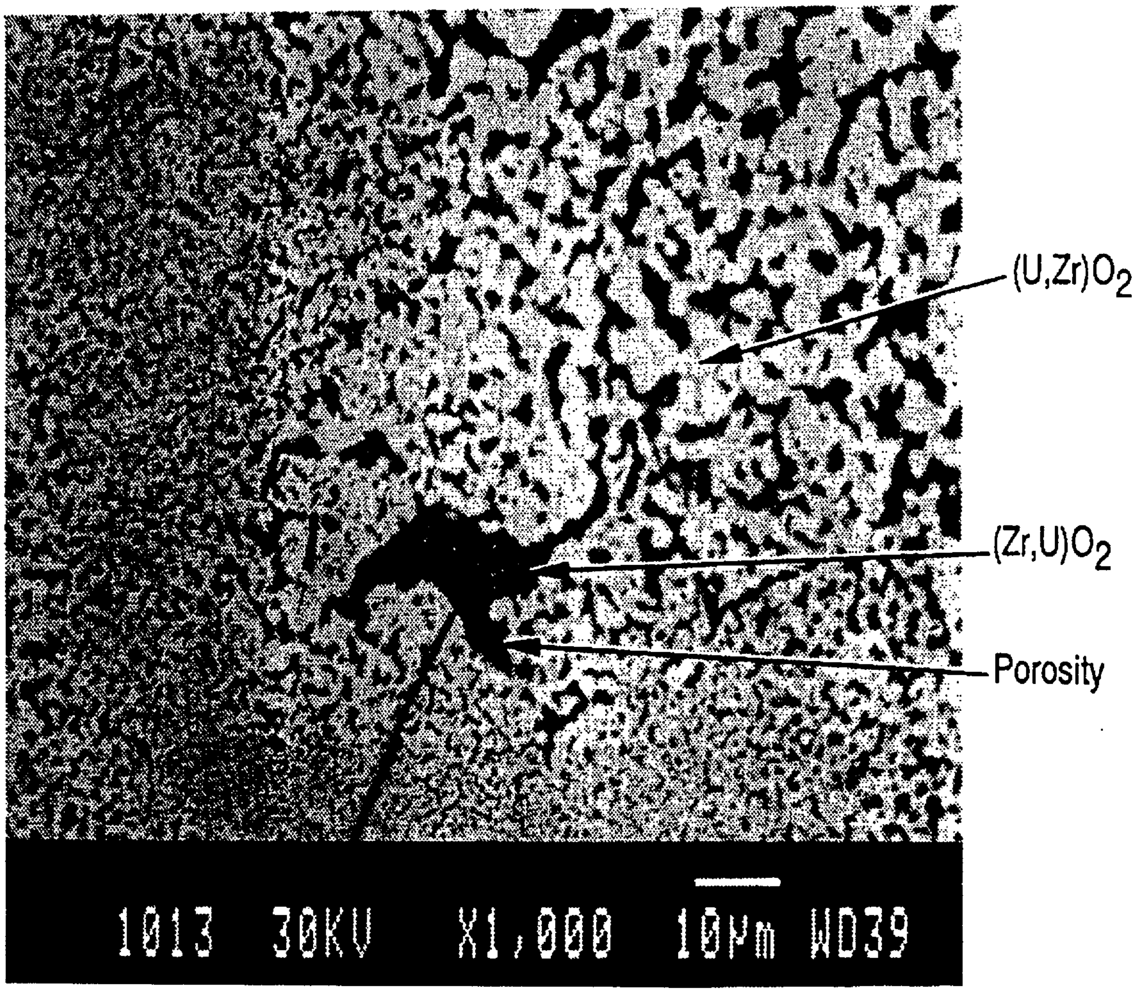


Figure 3.5-11 Scanning electron microscope image of two phase region in TMI-2 hard layer debris sample

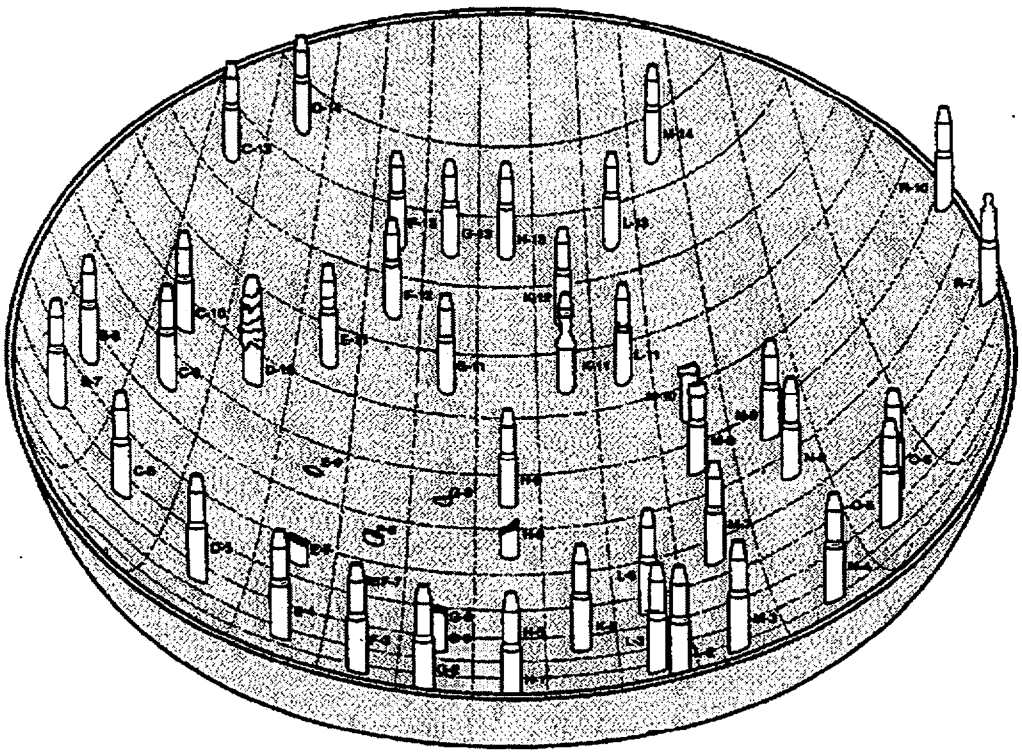


Figure 3.5-12 TMI-2 nozzle damage profile

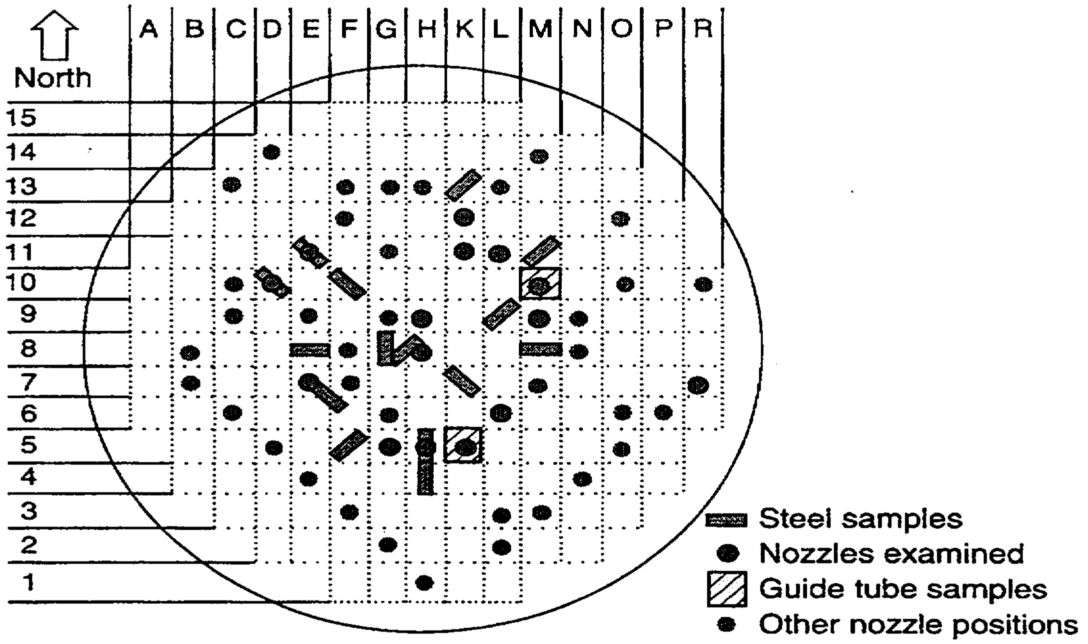


Figure 3.5-13 Location of lower-head steel, nozzle, and guide tube samples

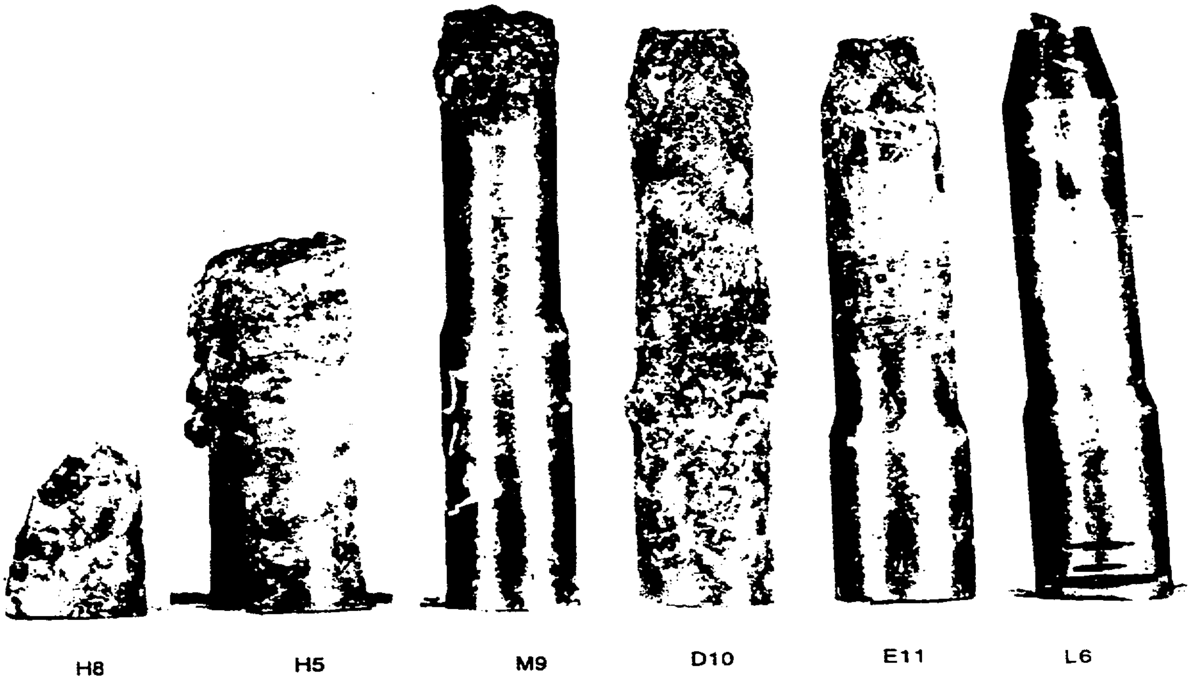


Figure 3.5-14 As-removed appearance of six TMI-2 nozzles

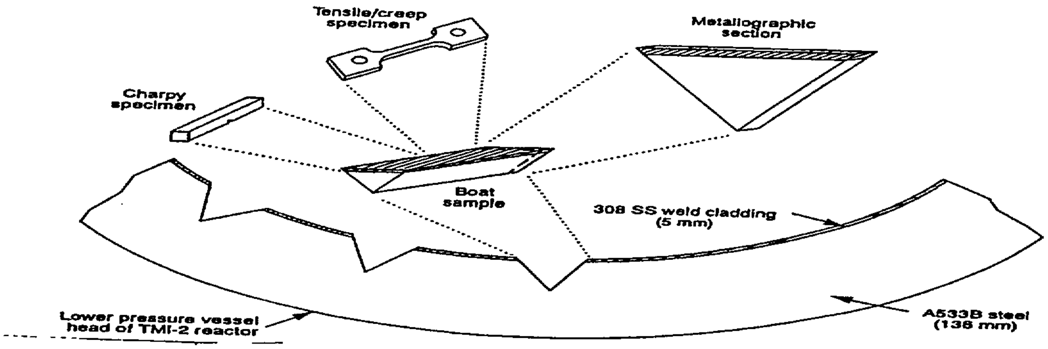


Figure 3.5-15 Schematic of sample taken from TMI-2 lower head

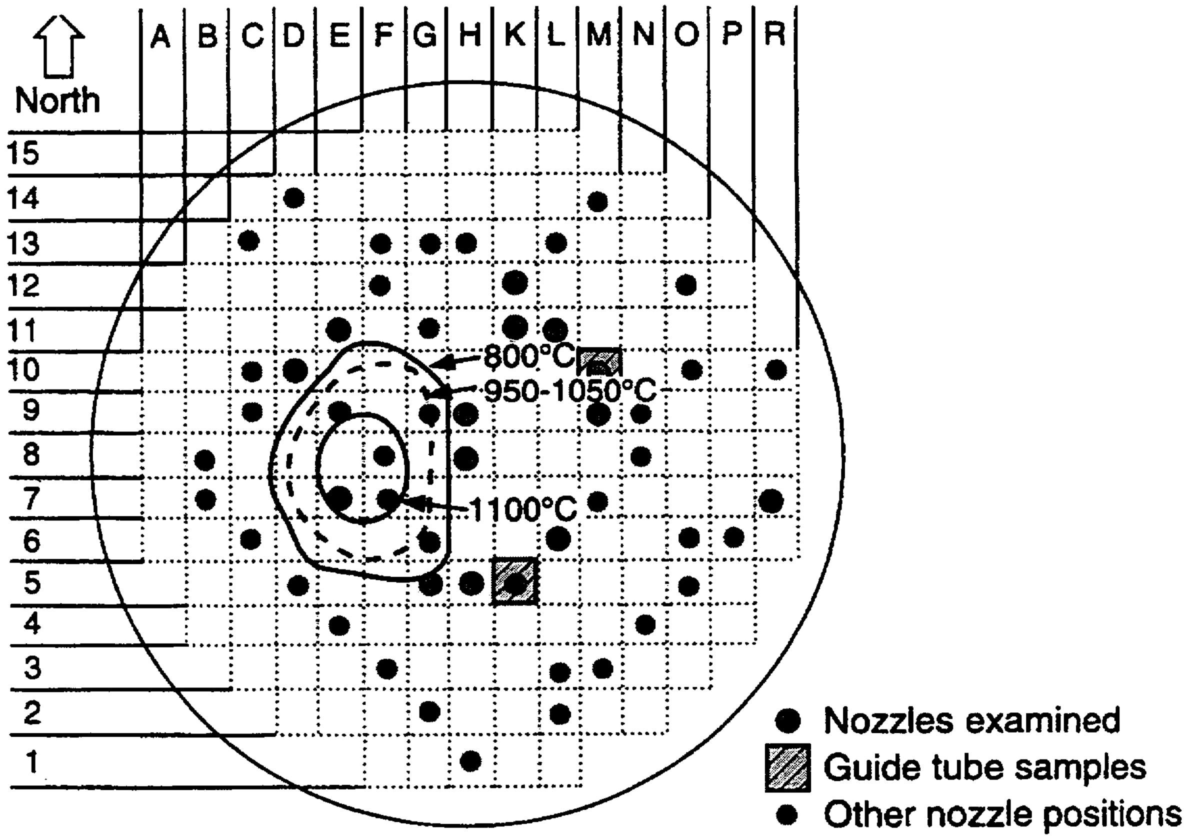


Figure 3.5-16 Lower-head hot spot and nozzle guide tube locations

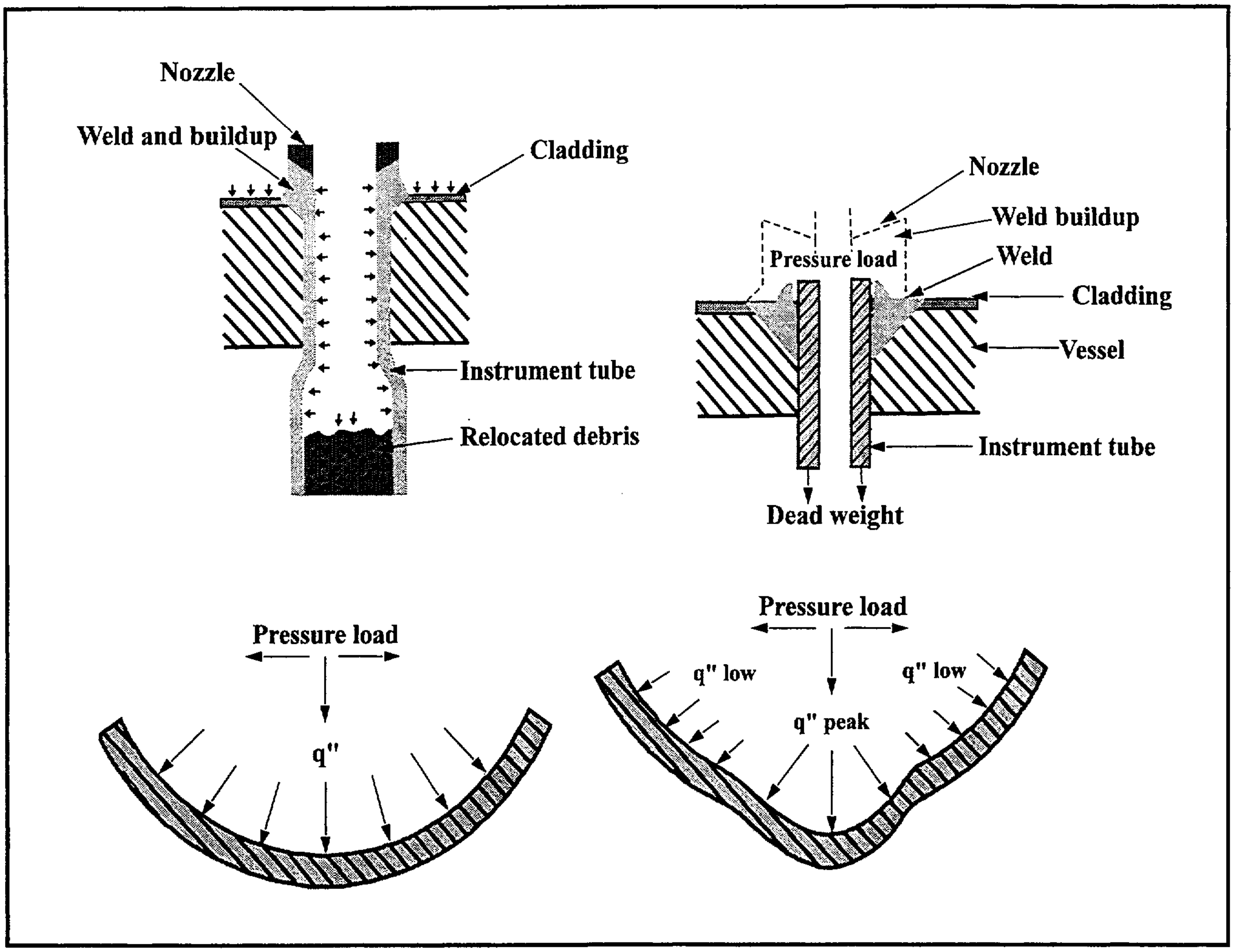


Figure 3.5-17 Failure mechanism considered in TMI-2 analyses:
(a) tube rupture
(b) weld failure–tube ejection
(c) global vessel failure, and
(d) localized vessel failure

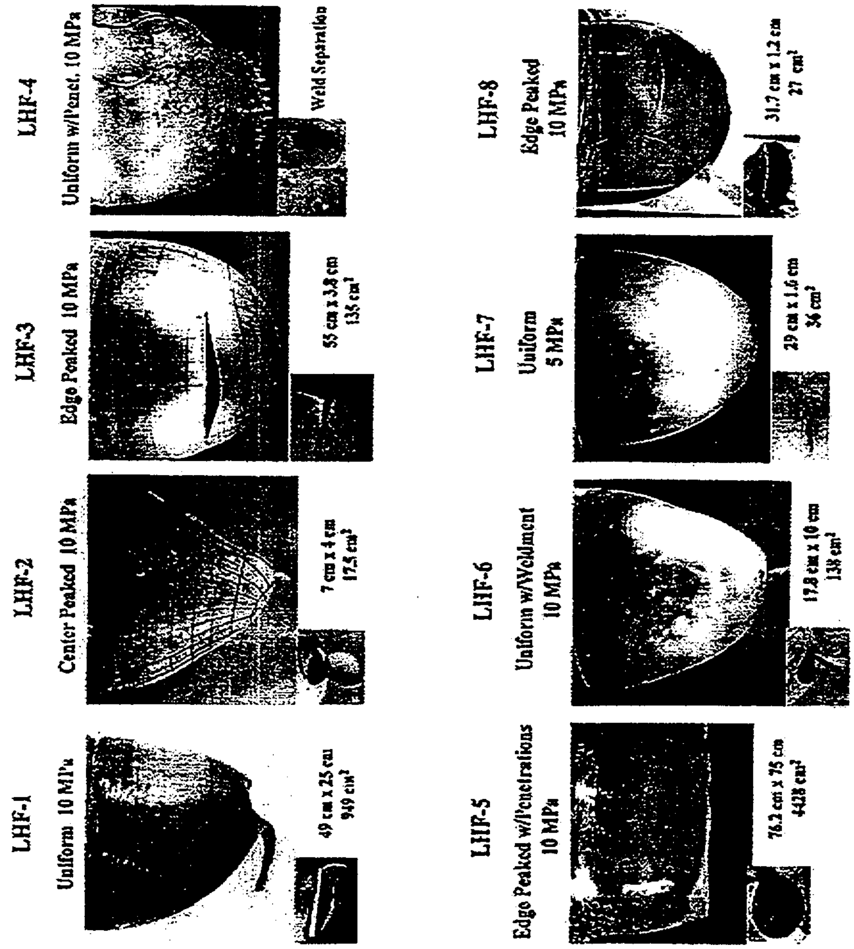


Figure 3.5-18 Pictorial summary of the completed lower head failure tests (Figure ES-1 of NUREG/CR-5582, SAND98-2047)

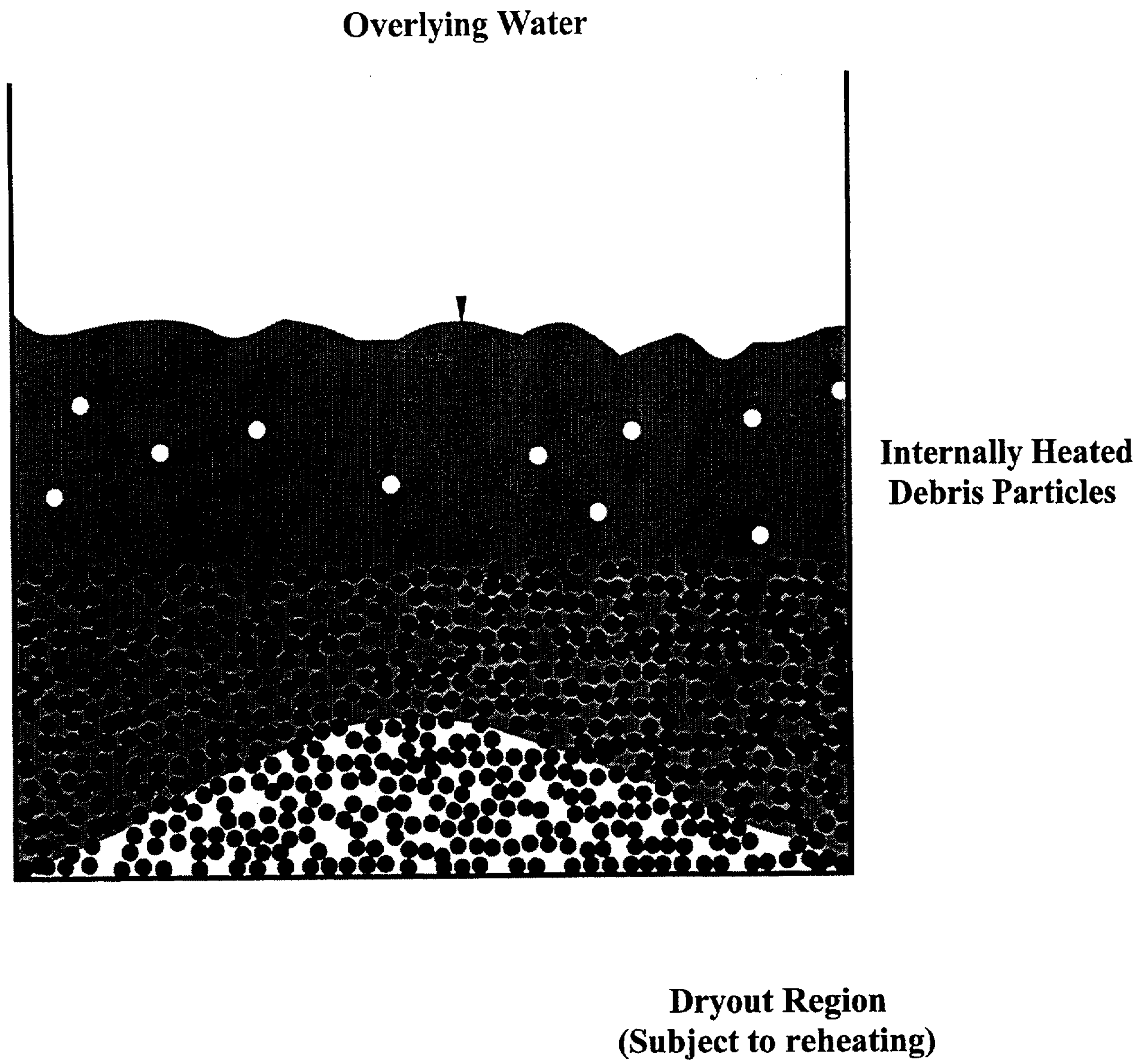

Overlying Water
Internally Heated Debris Particles
Dryout Region (Subject to reheating)

Figure 3.5-19 Typical debris bed dryout experiment

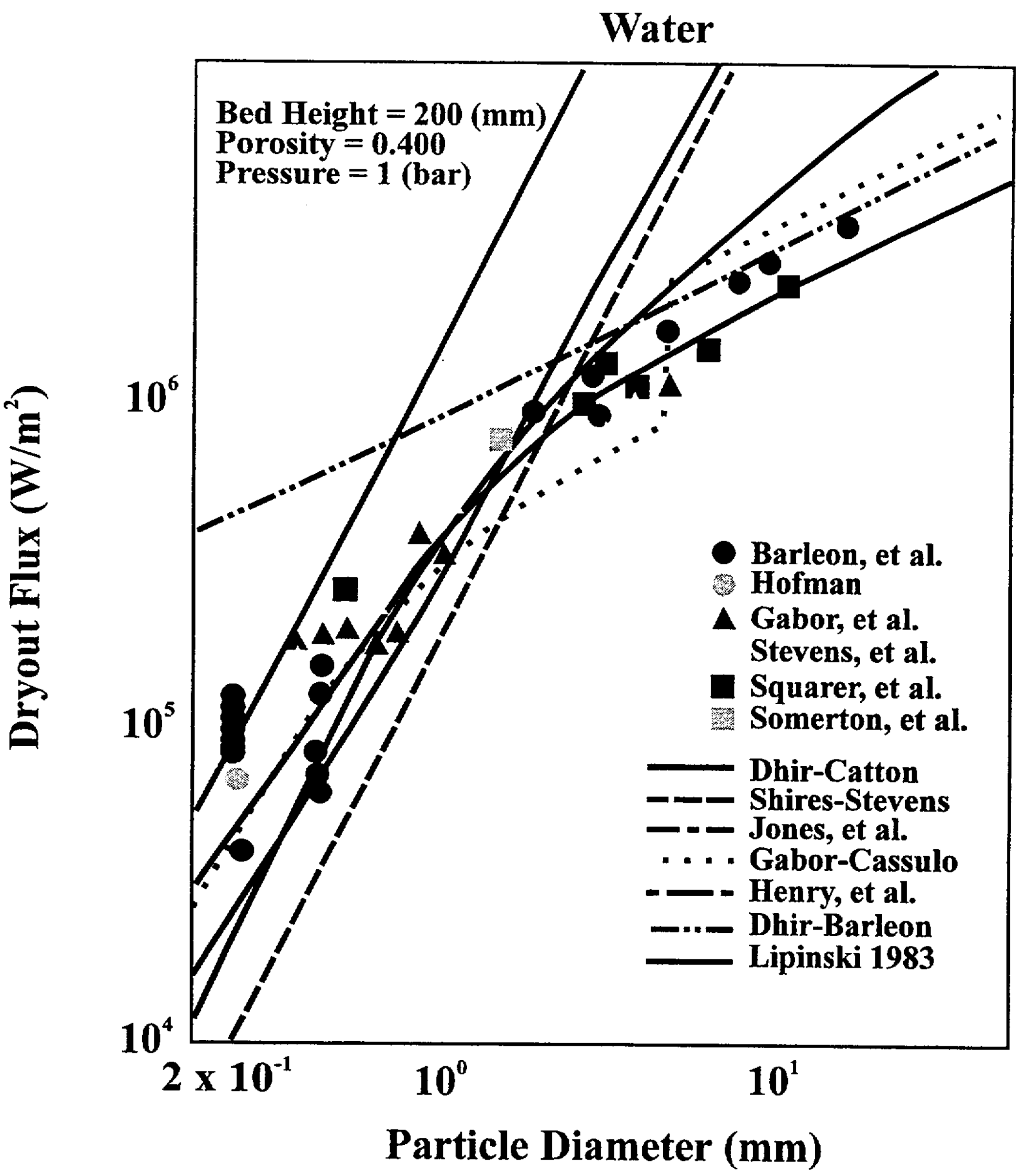


Figure 3.5-20 Debris bed dryout heat flux versus particle diameter for water

References for Section 3.5

1. J. R. Wolf, D. W. Akers, and L. A. Neimark, "Relocation of Molten Material to the TMI-2 Lower Head," *Nuclear Safety*, Vol. 35(2), 269-279, July-December 1994.

2. V. R. Fricke, "Quick-Look Inspection Results," GPU Technical Report TPO/TMI-026, Rev. 0, December 1982.

3. D. W. Akers and B. K. Schuetz, "Physical and Radiochemical Examinations of Debris from the TMI-2 Lower Head," *Nuclear Safety*, Vol. 35, No. 2, July-December 1994.

4. G. E. Korth, "Peak Accident Temperatures of the TMI-2 Lower Pressure Vessel Head," *Three Mile Island Reactor Pressure Vessel Investigation Project Achievements and Significant Results*, Organisation for Economic Co-operation and Development, Paris, France, October 1994.

5. D. R. Diercks and G. E. Korth, "Results of Metallographic Examinations and Mechanical Tests of Pressure Vessel Samples from the TMI-2 Lower Head," *Nuclear Safety*, Vol. 35, No. 2, 301-312, July-December 1994.

6. F. A. Kulacki, "Estimates of Failure Time for LWR and LMFBR Vessels Following a Core Meltdown Accident," Ohio State University, Department of Mechanical Engineering, USNRC contract AT-(49-24)-0149 Report, February 1976.

7. Commonwealth Edison Company, "Zion Probabilistic Safety Study," Chicago, IL 1981.

8. D. R. Diercks and L. A. Neimark, "Results of Mechanical Tests and Supplementary Microstructural Examinations of the TMI-2 Lower Head Samples," NUREG/CR-6187 (ANL-94/8) [TMI V(93)AL02], June 1993.

9. J. Rempe, L. Stickler, S. Chavez, G. Thinnes, R. Witt, and M. Corradini, "Margin-to-Failure Calculations for the TMI-2 Vessel," *Nuclear Safety*, Vol. 35, No. 2, July-December 1994.

10. T. Y. Chu, M. M. Pilch, J. H. Bentz, J. S. Ludwigsen, W-Y Lu, and L. L. Humphries, "Lower Head Failure Experiments and Analyses," NUREG/CR-5582, SAND98-2047.

11. R. J. Lipinski, "A Coolability Model for Postaccident Nuclear Reactor Debris," *Nuclear Technology*, 65, pp. 53-66, 1980.

12. R. Lipinski, "Debris Bed Dryout," Appendix 3.2-B of *Thermal-Hydraulic Process Modeling in Risk Analysis: An Assessment of the Relevant Systems, Structures, and Phenomena,* NUREG/CR-3986, SAND84-1219, August 1984.

13. K. R. Boldt et al., "SNL-LWR Severe Core-Damage Phenomenology Program, LWR Degraded Core Coolability Program, Vol. 2," NUREG/CR-2725, SAND82-1115.

14. S. A. Hodge, C. R. Hyman, R. L. Sanders "BWR Lower Plenum Debris Bed (BH) Package Reference Manual," *MELCOR Computer Code Manuals*, NUREG/CR-6119, SAND93-2185, Vol. 2, March 1995.

15. S. A. Hodge, J. C. Cleveland, T. S. Kress, and M. Petek, “Identification and Assessment of BWR In-Vessel Strategies,” NUREG/CR-5869, ORNL/TM-12080, October 1992.

16. R. E. Henry and H. K. Fauske, "External Cooling of a Reactor Vessel Under Severe Accident Conditions," *Nuclear Engineering Design*, 139, pp. 31-43, 1993.

17. R. E. Henry et al., "Cooling of Core Debris Within the Reactor Vessel Lower Head," *Nuclear Technology*, 101, pp.385-399, 1993.

18. T.G. Theofanous and M.L. Corradini, “The containment of Severe Accidents in the Advanced Passive Light Water Reactors,” Agenzia Nazionale per la Protezione del'Ambiente, March 1995.

3.6 In-Vessel Fuel-Coolant Interactions

When molten core material (fuel) comes into contact with liquid water (coolant), a variety of different fuel-coolant interactions (FCIs) can occur. The FCIs can range from quiescent boiling to explosive fragmentation of the fuel with rapid steam generation. An explosion caused by the rapid fragmentation of fuel and vaporization of water due to heat transfer from the fragmented fuel is called a steam explosion. If the melt contains unoxidized metals, exothermic metal-water reactions can accompany the fuel coolant interaction, resulting in enhanced energy release and the generation of hydrogen. The nature of the FCI determines the rates of steam and hydrogen production and the potential for damaging the reactor vessel or containment building. Much theoretical and experimental research has been devoted to FCIs over the last three decades. This research is summarized in several review articles.[1,2,3,4,5]

3.6.1 Steam Explosions

Steam explosions occur when heat is transferred from the melt to water on a very short time scale (approximately 1 msec.). Steam explosions have occurred ever since man began to work with molten metals. The first known written record of such an explosion appears in the Canterbury Tales of the 14th century.[6] Destructive steam explosions have occurred in aluminum, steel, and copper foundries; arc-melting facilities; paper mills; granulation plants; and (some believe) Chernobyl.[7,8,9,10,11]

The four major stages of a steam explosion are:

1. Initial *coarse mixing* of melt and water during which heat transfer is generally characterized by stable film boiling (Figure 3.6-1),
2. a *triggering* event that causes local destabilization of film boiling and local fragmentation of melt into small drops, on the order of 0.01 to 0.1 mm in diameter,
3. *propagation* of the region of rapid heat transfer through the coarse mixture, and
4. explosive *expansion* driven by steam at high pressure.

In the absence of a triggering event, a nonexplosive FCI would occur. Coarse mixing would result in some quenching of the melt with associated steam and hydrogen production.

3.6.2 Conditions Affecting Steam Explosions

The probability and magnitude of steam explosions depend on various initial and boundary conditions, including:

- mass, composition, and temp-erature of the molten material,
- water mass, depth, and temperature,
- vessel geometry, degree of confinement, and the presence and nature of flow restrictions and other structures,
- fuel-coolant contact mode, in particular, for melts poured into water, the melt entry velocity and pour diameter,
- the ambient pressure,

- the timing and strength of any external trigger that might be applied (e.g. in an experiment, not a reactor accident).

Intermediate conditions that strongly influence the probability and magnitude of steam explosions include:

- the extent of coarse mixing (drop sizes and surface areas),

- the rate of heat production by the exothermic oxidation of molten metals and partially oxidized materials by the surrounding coolant, and

- the occurrence, timing, and strength of a spontaneous trigger (see below).

During mixing, some of the molten drops may spontaneously fragment into much smaller drops, on the order of 0.01 to 0.1 mm in diameter. This local fragmentation event is generally called a trigger. It may be produced by natural oscillations in the vapor film about the drop leading to fuel-coolant contact, or it may be induced by shock waves from falling objects, contact of the fuel with the bottom surface, entrance of the fuel into a region of colder water, or by turbulence generated in part of the mixing region. If the fragmentation is rapid enough, local shock waves can be produced, which can cause neighboring drops to fragment. If such a chain reaction escalates, a steam explosion can result.

Steam explosions can occur for a variety of high-temperature molten materials including uranium and its oxides. Spontaneous (no external trigger) steam explosions have been observed for aluminum, iron, tin, and associated oxides in all possible contact modes including melt pours, stratified water over melt, and reflooding. High ambient pressure and low water subcooling have been shown to reduce the probability of spontaneous steam explosions at experimental scales; however, explosions can still occur if the necessary triggers are available.

Experimentally measured conversion ratios (the work done divided by the thermal energy available) range from zero to values approaching the thermodynamic limit. Explosion pressures have been measured over the range of tens of bars to 2 kilobars. Steam explosion computer codes have predicted that pressures of many kilobars are possible for strong steam explosions.

Significant rates of hydrogen production have been observed for both explosive and nonexplosive interactions. Much finer fragments produced in explosive interactions can potentially lead to more rapid production of steam and hydrogen. The actual hydrogen production rate, however, is a result of two competing processes. The large surface-to volume ratio of the molten drop tends to increase the rate of heat transfer from the drop to water, but it also tends to increase the rate of exothermic oxidation, which adds energy to the drop and hot hydrogen gas to the vapor film surrounding the drop. The occurrence of a steam explosion as opposed to a nonexplosive interaction is generally thought to favor increased hydrogen production, especially when the melt is metallic as in foundries.

3.6.3 Limitations on In-Vessel FCIs

A rough estimate of the potential for energy release from in-vessel FCIs (excluding Zr oxidation) can easily be computed by calculating the energy that would have to be transferred to water in order to quench the entire core. For example, a typical PWR core might contain 10^5 kg of UO_2 and 2×10^4 kg Zr. Assume that all of this material (plus 10^4 kg Fe to allow for structural material in the melt) is liquefied at 4712°F (2600°C = 2873K), below the UO_2 melt temperature of 5180°F (2860°C = 3133K). The decrease in sensible and latent heat required to quench this melt to 212°F (100°C = 373K), which is the saturation temperature for water at atmospheric pressure is approximately 170 GJ (a steam explosion of 1 to 1.5 GJ could fail the reactor vessel lower head). A 170 GJ steam explosion would require the evaporation of approximately 75,000 kg or 75 m^3 of saturated water at atmospheric pressure.

In reality, the energy transferred from core materials to residual water would be less than 170 GJ for two reasons:

1. The volume of residual in-vessel water would be limited, in the absence of ECC restoration, and

2. lower melt temperatures and/or higher in-vessel pressures, which would be anticipated in most severe accident scenarios, would reduce the temperature difference between molten core materials and residual in-vessel water.

Figure 3.6-2 illustrates the limited capacity for in-vessel FCI energy releases at various pressures in a PWR if the residual water is limited to 29 m^3, which is approximately the volume below the lower core plate of a Westinghouse PWR. Table 3.6-1 shows the corresponding limitations of the mass of core material that could be quenched.[12] In general, BWR lower plenums are larger and hold more water relative to the mass of the core. Considerations with respect to the potential for debris quenching in a BWR lower plenum are discussed in Section 3.7.6.

Reactor vessel lower plenums, particularly in BWRs, contain significant quantities of structural materials as illustrated in Figures 3.1-5 and 3.1-9. Such structures could restrict the volumes of melt and/or water participating in FCIs at a given time. Table 3.6-2 provides some data on features and geometry that characterize these flow restrictions.[13]

It should be noted that the preceding estimates ignore the potential contribution to FCI energy releases associated with oxidizing metallic Zr contained in the melt. As noted in Subsection 3.3, quantities of unoxidized zirconium are likely to be involved in the core-liquefaction processes. Mixing of this metallic phase at high temperatures with the water in the lower plenum would promote rapid oxidation of the zirconium, depending primarily upon the degree to which fragmentation of the melt provides large increases in the interfacial surface area. The heat of reaction for Zr oxidation is approximately 6.5 MJ/kg of Zr reacted. If only 1% of the Zr typically contained in a PWR core (2×10^4 kg) were oxidized during in-vessel FCIs, an additional 1.3 GJ would be released. Regardless of the exact outcome, the addition of reaction energy and liberation of a quantity of hydrogen by the oxidation of zirconium during the melt-water interaction phase seems likely.

3.6.4 In-Vessel FCI Scenarios

In assessing the impact of in-vessel FCIs on accident progression, three alternative scenarios can be postulated:

1. No steam explosion but violent boiling, which may partially or totally quench the core debris, depending on the quantity of water available and the agglomeration of the debris.

2. One or more relatively low-yield steam explosions and nonexplosive quenching until the whole of the molten mass of fuel has been fragmented or all of the water evaporates.

3. A large steam explosion involving a significant fraction of the melt, triggered either spontaneously or by a low-yield steam explosion.

Because of the resultant disruption (and possible dispersal) of internal structures and residual core materials, the occurrence of even a relatively low-yield steam explosion could significantly alter the subsequent progression of damage.

3.6.5 Alpha Mode Containment Failure

Energetically, it is possible that a large in-vessel steam explosion could cause (a) breach of the reactor vessel,[14] or (b) breach of the reactor vessel and generation of containment-failing missiles.[15] Either event would completely alter the course of the accident by causing the immediate ejection of fuel and fission products from the reactor vessel. The second would result in nearly simultaneous venting of the containment. The possibility of these events accounts for the nil minimum duration for Stage 5 given in Table 3.1-1.

The Reactor Safety Study (RSS) first identified the possibility that a large-scale in-vessel steam explosion could result in containment failure. This is commonly referred to as the alpha mode of containment failure. The RSS took the alpha mode failure probability to be 0.01, although the uncertainty in this probability was acknowledged by also providing a pessimistic estimate of 0.1.[12]

Since the RSS, there has been considerable experimental research performed on fuel-coolant interactions at small to intermediate scales (50 mg to 157 kg). Early experiments investigated steam explosion efficiencies and various aspects of triggering in geometries that were open to the atmosphere. This early work is summarized in three review papers.[2,3,4]

A 1984 study showed that conversion ratios less than 5.3% and masses of actively participating molten core less than 5000 kg, as suggested by several mixing models,[16,17] imply an alpha mode failure probability of 0.0001 or less. However, some argued that the possibility of larger conversion ratios or larger masses actively participating could not be excluded and that the uncertainty in the alpha-mode containment failure probability was therefore large.[18]

In 1985 the first NRC-sponsored Steam Explosion Review Group (SERG-1) assessed the probability of alpha mode failure for NUREG-1150.[19] The SERG-1 pessimistic failure probability was 0.1, unchanged from the pessimistic estimate of the RSS. The NUREG-1150 alpha mode failure probabilities are listed in Table 3.6-3.

NRC-funded FCI research after the initial SERG-1 workshop sought to enhance the technical basis of the alpha mode failure estimates given by the experts, and reduce uncertainties in the estimates. Numerous experiments were conducted from 1985 through 1995 in both U.S. and European facilities. A review of these experiments is provided in a recent paper.[5] The experiments demonstrate that steam voiding around hot debris particles causes the mixing region to be depleted of water in part as a result of its vaporization due to rapid melt-to-coolant heat transfer, and, in part due to displacement of remaining water mass away from the interfacial region. Depletion is even more pronounced in the case of adjacent simultaneous pours as occurred through multiple holes in the elliptical flow distributor at TMI-2.

In June 1995 the NRC convened the SERG-2 workshop to reassess the alpha mode failure issue and to evaluate the current understanding of other FCI issues of potential risk significance. As illustrated in Table 3.6-4, all but two of the 11 SERG-2 experts concluded that the alpha mode failure issue is essentially resolved, meaning that this mode of failure is of very low probability, that it is of little or no significance to the overall risk from nuclear power plants, and that further research is not likely to change this conclusion.

The SERG-2 experts based their judgements regarding the likelihood of alpha mode failure largely on experimentally substantiated arguments favoring limits to mixing. There is a consensus among the experts that the triggering process is poorly understood due largely to its inherently random nature. Assumptions regarding triggering under accident conditions tend, therefore, to be conservative. Triggering is postulated at the worst time during premixing, leading to trigger amplification or shock wave propagation.

It should be emphasized, however, that in experiments performed with prototypic reactor melts interacting with saturated to subcooled water at an ambient pressure of nominally 0.1 MPa, only one or two cases exhibited weak steam explosions either at high melt-to-coolant volume ratios or at high subcooling, and only when an external trigger was used. In contrast, many more cases using iron-alumina thermite and iron oxide as melt simulants produced strong steam explosions at a wide range of melt-to-coolant volume ratios, much lower subcooling to almost saturated conditions, with or without trigger.

3.6.6 Vessel Breach by an In-Vessel Steam Explosion and Related Issues

The steam-explosion energy required to fail the bottom head of a PWR has been estimated to be between 1 GJ and 1.5 GJ. That is, a steam explosion need not involve large quantities of melt or water in order to yield such energies. In one study of PWR in-vessel steam explosions, failing the bottom head by an in-vessel steam explosion was found to be much more likely (probability of 0.2 versus 0.0001) than alpha mode failure.[20] Figure 3.6-4 illustrates this mode of vessel breach, which has the potential for driving particulate debris from the reactor cavity, resuspending radioactive aerosols previously plated out within the reactor coolant system, and forming additional aerosols during the explosion.

Steam explosion research has been conducted at several research facilities to address several issues including the possibility of lower head failure due to an in-vessel steam explosion, the potential for significant structural damage due to a steam explosion in the reactor cavity (see Section 4.3), pressure s,uppression effects on triggering, and effects of melt composition and melt-coolant-confinement geometry on both triggering and energetics of steam explosions. Table.3.6-5 provides summary information on four current steam explosion research facilities.[5]

The current level of understanding of the propagation phase of a steam explosion is adequate for estimating the net energy transfer to the coolant and hence, estimating the alpha mode failure probability. Understanding of shock loading of lower head and reactor cavity structures requires more rigorous treatment for which detailed two or even three-dimensional propagation phase models may be required.

3.6.7 Impact of Melt Discharge from Vessel

Four modes of discharge of core materials from the vessel can be postulated:

1. Massive failure of the vessel by an in-vessel explosion,
2. a pressure-driven melt jet,
3. gravity-driven pour of a large molten mass,
4. continuous dripping of core materials not involved in the initial release.

These modes of melt discharge are depicted in Figures 3.6-4 through 3.6-7.

The mode of vessel breach can strongly influence the timing and nature of potential loads imposed on containment. In 1984, the NRC sponsored Containment Loads Working Group identified the fact that pressurized dispersal of high-temperature melt into containment at the time of vessel breach (Figure 3.6-5), could result in rapid direct heating and exothermic chemical reactions within the containment atmosphere and pose a severe threat to containment integrity. On the other hand, if the vessel is depressurized, molten material would simply flow into the reactor cavity by gravity (Figure 3.6-6), although if water were present in the reactor cavity significant loads on containment could result from ex-vessel fuel coolant interactions or from the additional hydrogen generated in such interactions. In general, BWR containment drywells are relatively small, and, hence, special procedures are provided to assure that the reactor vessel would be depressurized under severe accident conditions.

The initial geometry and potential for cooling of ex-vessel debris, as well as the nature of interactions between core materials and concrete, are strongly influenced by the mode of vessel breach. The mode of melt discharge into containment also has a strong influence on the resulting concentrations of fission products, particularly in aerosol form, in the containment. Ex-vessel phenomena are discussed in Chapter 4.

Following either a pressurized ejection or a gravity-driven pour of melt from the vessel, a significant fraction of core materials may remain unmelted in the core region. Without coolant, much of this material may subsequently melt and drop out of the vessel in small amounts over a period of hours. This mode of discharge is illustrated in Figure 3.6-7. If there is water below the vessel, the dripping mass may prolong ex-vessel fuel-coolant or core-concrete interactions. If the hot leg or surge line had failed earlier natural circulation could be established with flow from the reactor cavity up through the reactor vessel and out the failed pipe. The ingress of air from containment following vessel breach could cause additional expthermic oxidation of hot in-vessel debris. This would, in turn, lead to additional releases of radionuclides to containment. All such possibilities would affect the magnitude of the radiological release given late containment failure.

Table 3.6-1 Fractions of core mixture[*] that can be quenched in below-core water for a typical PWR[**]

	Saturated Water Pressure			
	Atmospheric	800 psia (5.5 MPa)	1595 psia (11 MPa)	2465 psi (17 MPa)
ΔT = 2700°F (1500°C) No Freeze	0.79	0.44	0.31	0.17
ΔT = 3600°F (2000°C) No Freeze	0.59	0.33	0.23	0.13
ΔT = 4500°F (2500°C) Freeze	0.37	0.21	0.14	0.08

[*] 10^5 kg UO_2 + 2×10^4 kg Zr + 10 ^{4} kg steel

[**] in 29 m ^{3} of water

Table 3.6-2 Lower plenum features of a Westinghouse PWR

Feature	Approx. Thickness (mm)	Water Volume to Next Feature (m^3)	Energy to Evaporate Water (GJ)[**]
Lower Core Plate	50	6.6	4.6
Diffuser Plate	37	14.1[*]	9.8
Bottom Support Plate	220	7.7[*]	5.4
Reactor Vessel Bottom	132	0	--

[*] Ratio of these two volumes approximate; sum (21.8 m^3) is volume of lower hemisphere.

[**] Based on a pressure of 2500 psia (17.2 MPa).

Table 3.6-3 NUREG-1150 alpha mode failure probabilities

	Plant	System Pressure	Lower Bound	Mean	Upper Bound
BWRs	Grand Gulf	High Low	0 0	1.0×10^{-3} 1.0×10^{-2}	0.1 1.0
	Peach Bottom	High Low	1.0×10^{-8} 1.0×10^{-7}	1.0×10^{-3} 1.0×10^{-2}	0.1 1.0
PWRs	Sequoyah	High Low	0 0	8.5×10^{-4} 8.5×10^{-3}	0.1 1.0
	Surry	High Low	0 0	9.1×10^{-4} 9.1×10^{-3}	0.1 1.0

Table 3.6-4 Alpha mode failure probability estimates (given a core melt accident)

Participant	SERG-1[a] (1985)	SERG-2 (1995)	View on Status of Alpha Mode Failure Issue
Bankoff	$< 10^{-4}$	$< 10^{-5}$	Resolved from risk perspective
Berthoud	--	$< 10^{-3}$	No statement on resolution
Cho	< RSS[a]	$< 10^{-3}$	Resolved from risk perspective
Corradini	10^{-4} - 10^{-2}	$< 10^{-4}$	Resolved from risk perspective
Fauske	Vanishingly small	Vanishingly small	Resolved from risk perspective
Fletcher	--	$< 10^{-4}$	Resolved from risk perspective
Henry	--	Vanishingly small	Resolved from risk perspective
Jacobs	--	Probably low likelihood	Not resolved from risk perspective
Sehgal	--	$< 10^{-2}$	Resolved from risk perspective
Theofanous	$< 10^{-4}$	Physically unreasonable	Resolved from risk perspective
Turland	--	$< 10^{-3}$	Resolved from risk perspective

[a] Reactor Safety Study (RSS) best estimate 10^{-2}; NUREG-1150 consensus estimate 10^{-2} at low reactor coolant system pressure, 10^{-3} at high reactor coolant system pressure.

Table 3.6-5 Fuel coolant interaction experimental facility characteristics

Facility	FARO	KROTOS	WFCI	ZREX
Location	Joint Research Center, Ispra		The University of Wisconsin	Argonne National Laboratory
Areas of Interest	Premixing, quenching, propagation, energetics, and debris coolability		Conditions favoring and suppressing energetic FCI	Chemical augmentation of FCI due to metals in the melt
Test Section Diameter (cm)	4.7 - 15	0.95 - 2.0	0.87 - 2.0	1.0
Melt Jet Diameter (cm)	1	0.3 - 0.5	0.3	0.25 - 0.5
Water Depth (cm)	50 - 200	1000	1000	1000
Pressure (MPa)	0.1 - 5.0	0.1 - 1.0	0.1	0.1
Melt	UO_2-ZrO_2 w/ & w/o Zr and stainless steel (SS)	UO_2-ZrO_2 or Al_2O_3	Sn, FeO, or Fe_3O_4	Zr w/ or w/o ZrO_2
Melt Mass (kg)	18 - 250	1.4 - 6.0	0.8 - 4.5	0.2 - 1.0

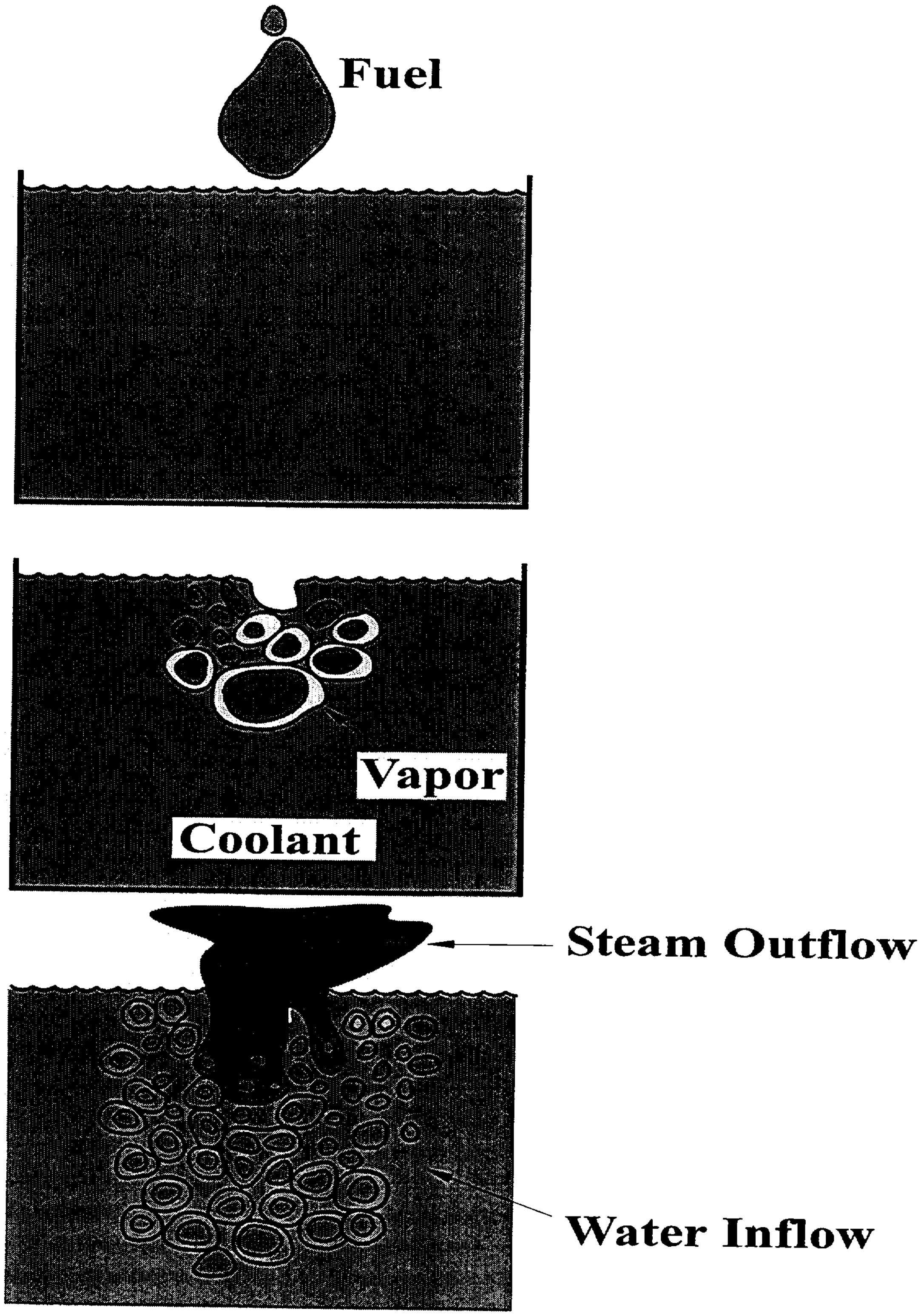


Figure 3.6-1 Progression of fuel-coolant mixing

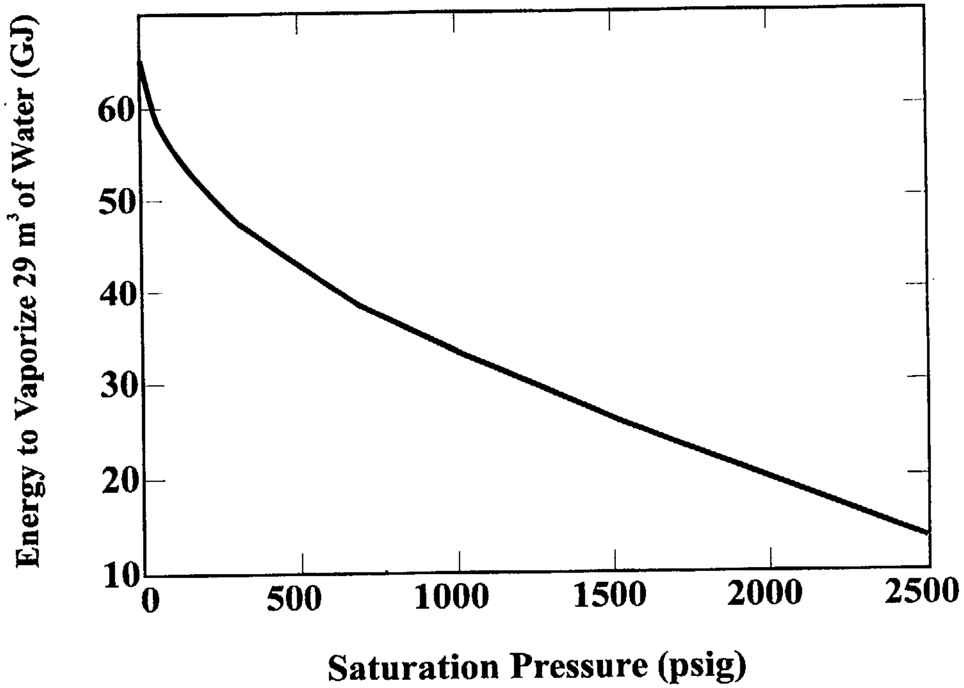


Figure 3.6-2 Energy required to vaporize 29 m^3 for water versus saturation pressure

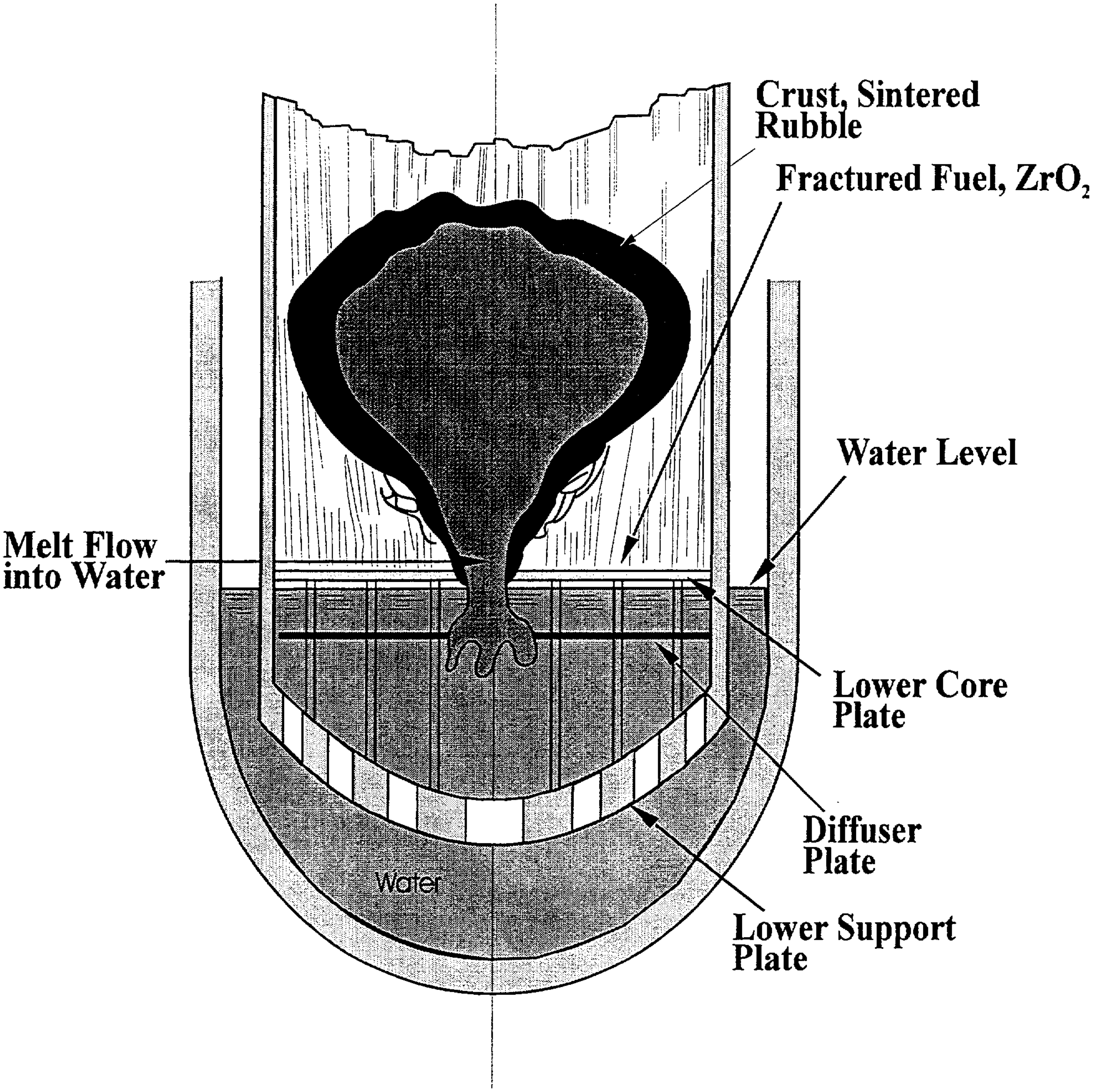


Figure 3.6-3 Melt pour into lower plenum by failure of core plate

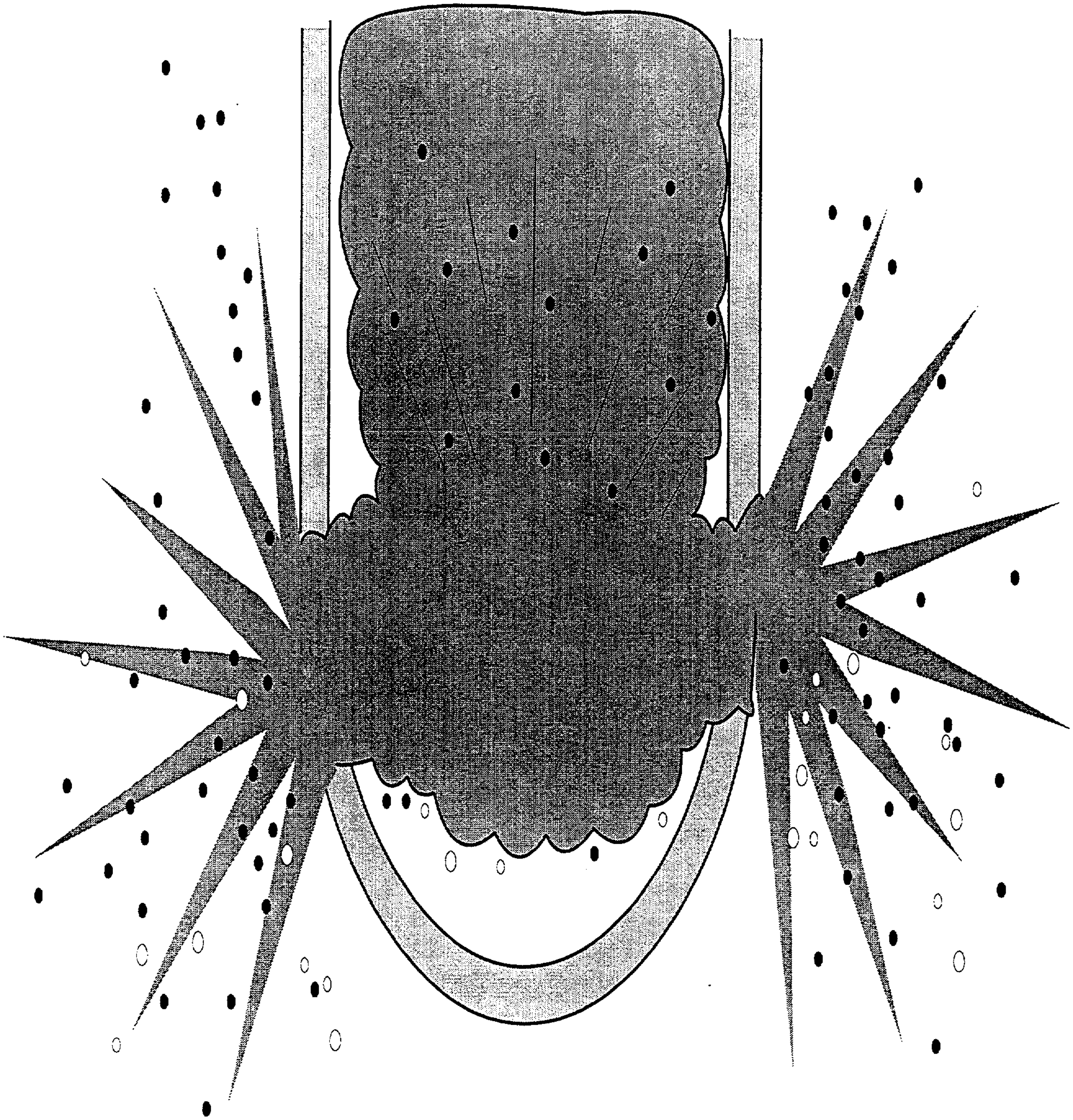


Figure 3.6-4 Vessel failure from steam explosion

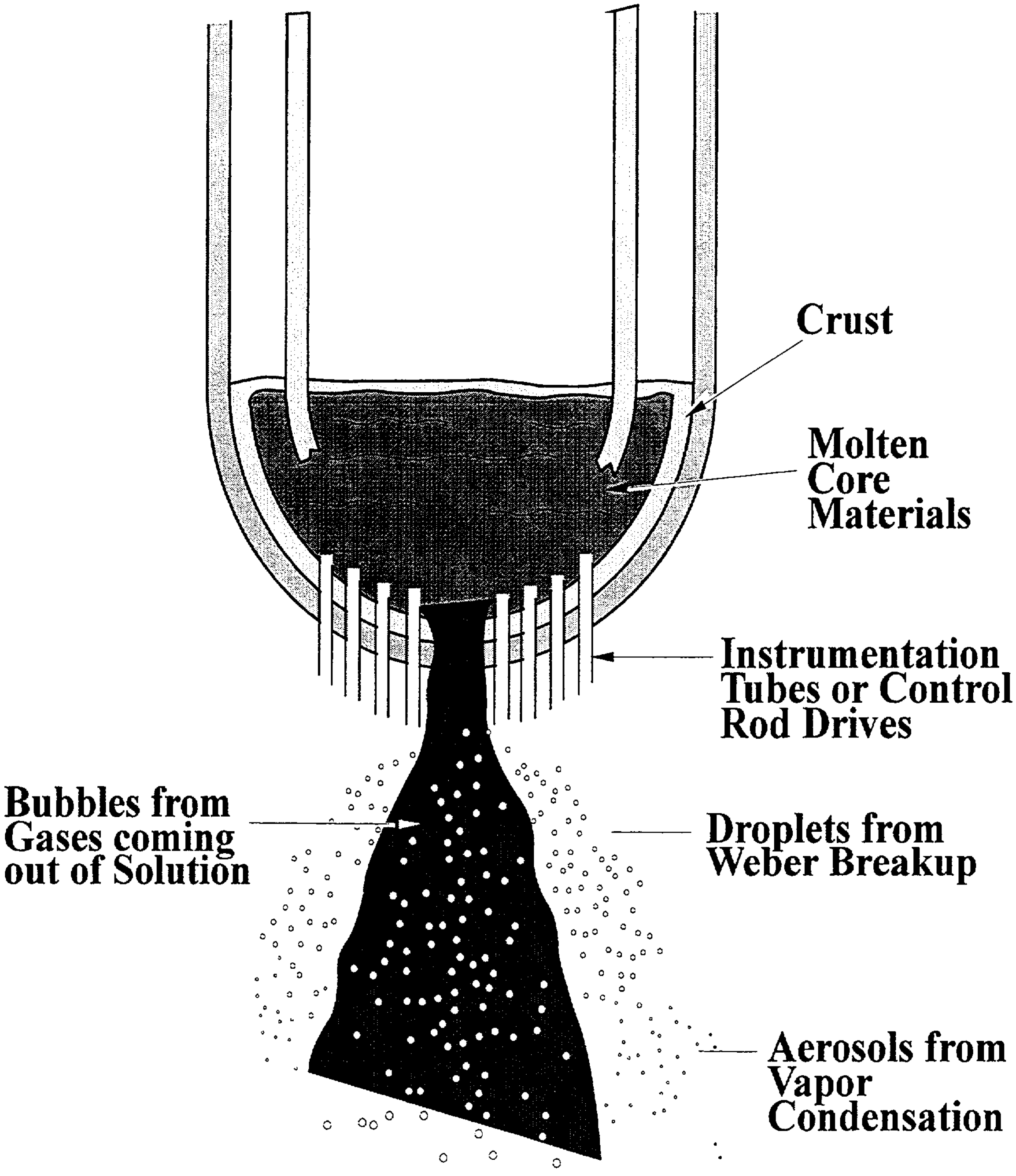

Crust
Molten Core Materials
Instrumentation Tubes or Control Rod Drives
Bubbles from Gases coming out of Solution
Droplets from Weber Breakup
Aerosols from Vapor Condensation

Figure 3.6-5 High pressure melt release from bottom of reactor vessel

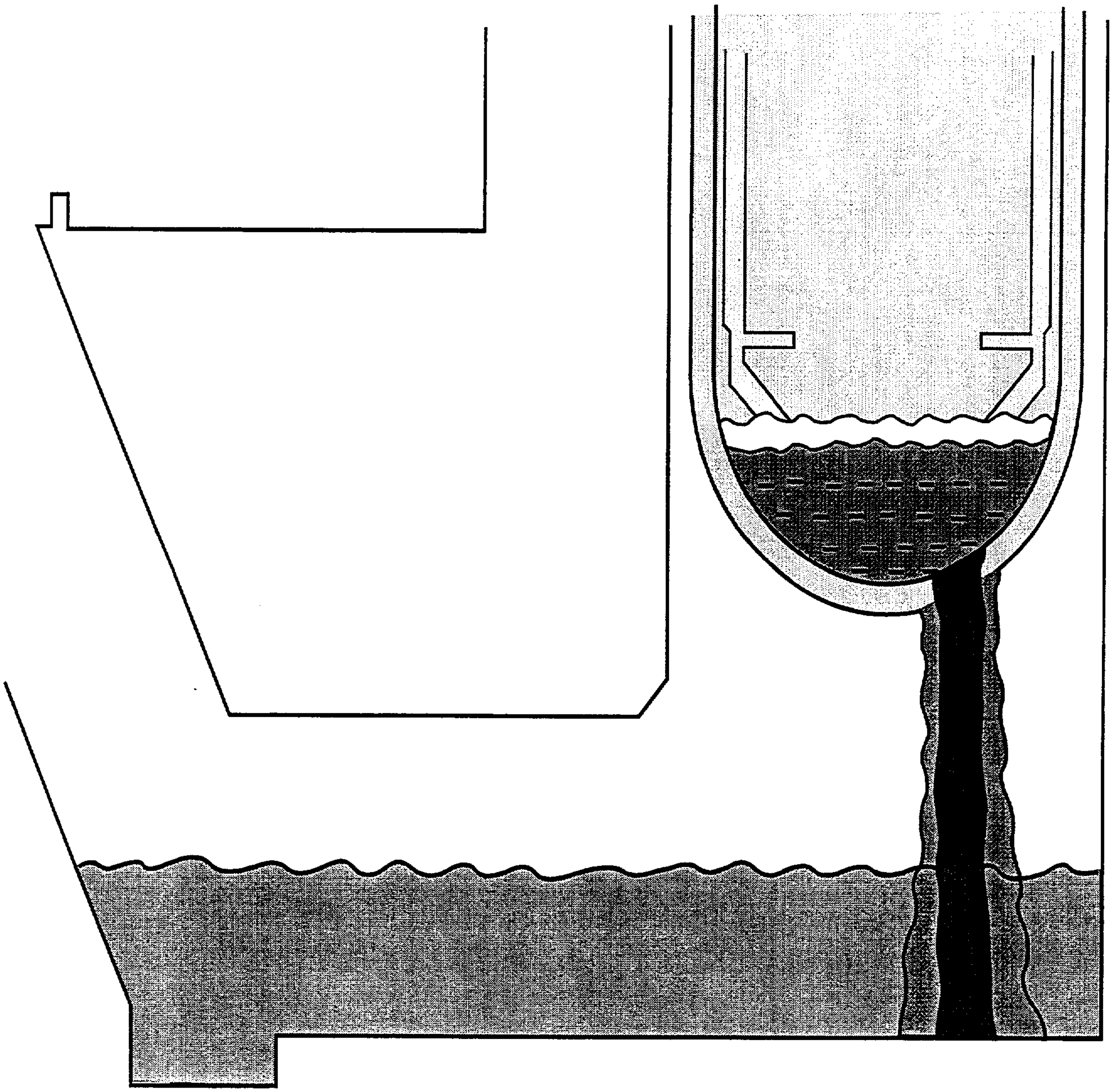


Figure 3.6-6   Low pressure melt release from bottom of reactor vessel

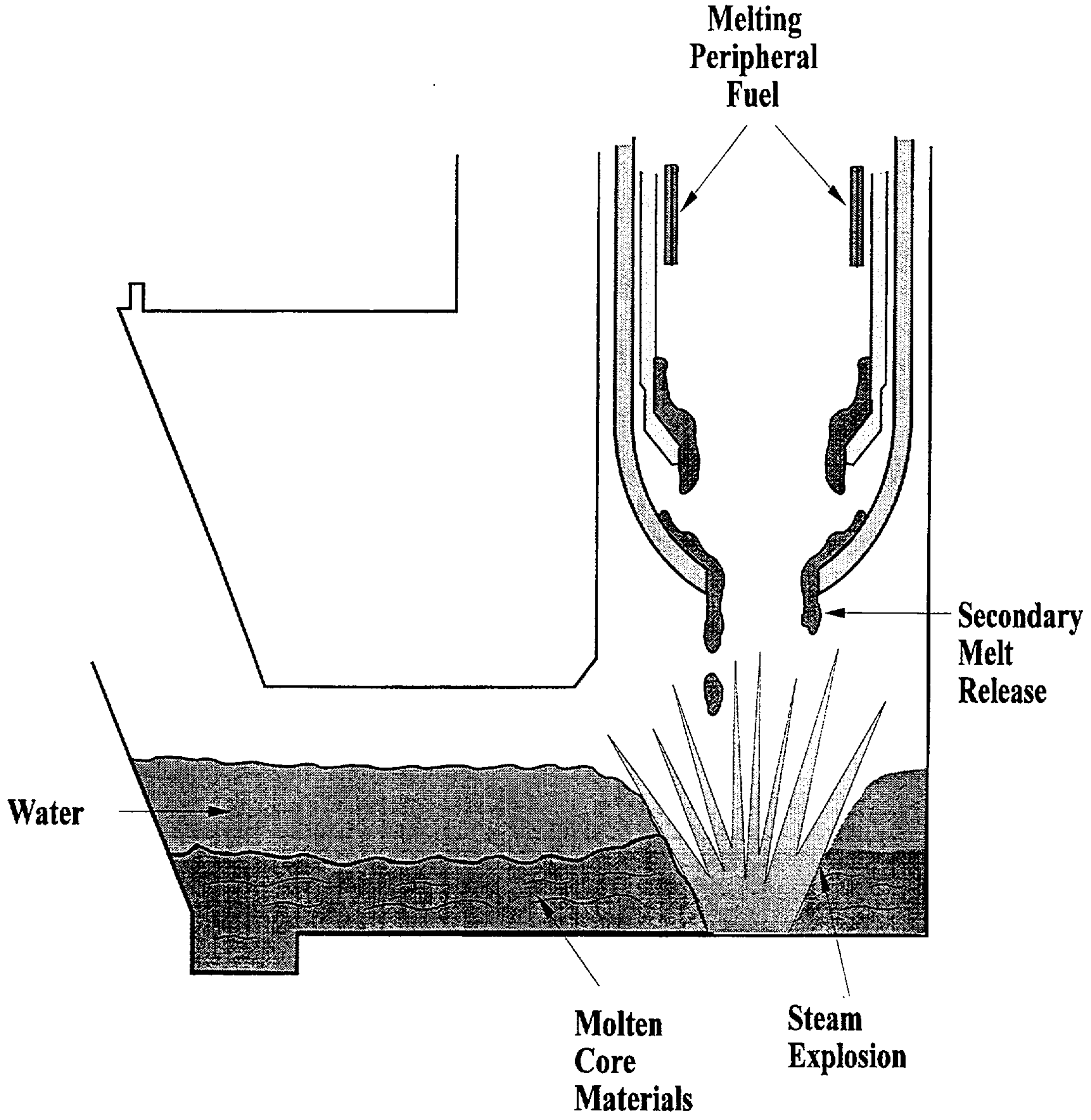


Figure 3.6-7 Secondary melt release in a Zion-type PWR reactor cavity

References for Section 3.6

1. R. C. Reid, "Rapid Phase Transitions from Liquid to Vapor," *Advances in Chemical Engineering*, 12, pp. 105-208, 1983.

2. M. L. Corradini, et al., "Vapor Explosions in Light Water Reactors: A Review Theory and Modeling," *Progress in Nuclear Energy,* 22(1), pp.1-117, 1988.

3. M. L. Corradini, "Vapor Explosions: A Review of Experiments for Accident Analysis," *Nuclear Safety,* 32(3), pp. 337-362, 1991.

4. D. F. Fletcher, "A Review of the Available Information on the Triggering Stage of a Steam Explosion," *Nuclear Safety,* 35(1), pp. 36-57, 1994.

5. S. Basu and T. P. Speis, "An overview of fuel-coolant interactions (FCI) research at NRC," *Proceedings of the 23rd Water Reactor Safety Information Meeting*, Vol. 2, pp. 187-210, October 23-25, 1995.

6. G. Chaucer, "The Canon's Yeoman's Tale," in *Canterbury Tales*, Garden City Publishing Company, Inc., Garden City, NewYork, 1934.

7. M. Berman, "Thermodynamic and Fluid-Dynamic Modelling of Two-Phase Propagating Explosions," *Workshop on the Causes and Prevention of Melt-Water Interactions,* Sandia National Laboratories, Albuquerque, New Mexico, July 29, 1988.

8. M. Berman et al., "Chernobyl: Where Do We Go From Here," Discussions of Steam Explosions at Chernobyl, *Proceedings of the Conference -by-Computer*, Nuclear Publications, McGraw-Hill, New York, New York, September 29-October 17, 1986.

9. W. Sweet, "Chernobyl, What Really Happened," *Technology Review*, pp. 43-52, July, 1989.

10. F. Reisch, "Chernobyl - the Initiating Event?" *Nuclear News*, December 1987.

11. A. W. Cronenberg, "Recent Developments in the Understanding of Energetic Molten Fuel-Coolant Interactions," *Nuclear Safety*, 22(3), pp. 319-337, May-June 1980.

12. J. B. Rivard et al., "Identification of Severe Accident Uncertainties," NUREG/CR-3440, SAND83-1689, September 1984.

13. J. B. Rivard, "Review of In-Vessel Meltdown Models," NUREG/CR-1493, SAND80-0455, July 1980.

14. J. H. Gittus et al., "PWR Degraded Core Analysis," ND-R-610(S), United Kingdom Atomic Energy Authority, Springfields, UK, 1982.

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

16. T. G. Theofanous and M. Saito, "An Assessment of Class 9 (Core-Melt) Accidents for PWR Dry Containment Systems," *Nuclear Engineering Design,* pp. 301-332, 1981.

17. M. L. Corradini and G. A. Moses, "A Dynamic Model for Fuel-Coolant Mixing," *Proceedings from the International Meeting on LWR Severe Accident Evaluation*, Cambridge, Massachusetts, August 1983.

18. M. Berman, "Molten-Core Coolant Interactions Program," *Proceedingsfrom the 12th Water Reactor Safety Research Information Meeting*, 1984.

19. U.S. Nuclear Regulatory Commission, "A Review of the Current Understanding of the Potential for Containment Failure Arising from In-Vessel Steam Explosions," NUREG-1116, 1985.

20. M. Berman, D. V. Swenson, and A. J. Wickett, "An Uncertainty Study of PWR Steam Explosions," NUREG/CR-3369, SAND83-1438, May 1984.