WASH - 1400 - App-1
(NUREG-75/014 - App-1)

Reactor Safety Study

An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants

Appendix I

United States Nuclear Regulatory Commission

October 1975

DISCLAIMER

WASH–1400
(NUREG-75/014)

ACCIDENT DEFINITION
and
USE OF EVENT TREES

APPENDIX I
to
REACTOR SAFETY STUDY

U.S. NUCLEAR REGULATORY COMMISSION
OCTOBER 1975

Appendix I

Table of Contents

Table of Contents (Continued)

Table of Contents (Continued)

List of Tables

List of Tables (Continued)

List of Figures

List of Figures (Continued)

Section 1

Accident Definition and Use of Event Trees

INTRODUCTION AND SUMMARY

Nuclear power plant operating experience to date is not sufficient to completely support risk assessment involving low probability accidents on a purely actuarial basis.[1] Quantitative risk estimation therefore requires an analytic methodology that evaluates the factors contributing to risk:

a. The probability and magnitude of the release of radioactivity from the facility.

b. The likelihood and characteristics of various meteorological conditions and other physical factors that can affect the dispersion of the radioactivity in the environment.

c. The distribution of population that can be affected by the accident.

A combination of event trees and fault trees was used in this study to provide information on the first of the above factors. This information was then used as an input to the consequence model described in Appendix VI. In general the approach used in this study has been to make more realistic, as opposed to traditionally conservative, estimates of both the likelihood and the magnitude of potential accidents. Of course, in areas where information was insufficient for realistic estimates, appropriate levels of conservatism were used to prevent underestimation of risks.

Some failures in a nuclear power plant, such as a break in the piping of the reactor coolant system, can potentially lead to a wide range of accidents, each of which is composed of a series of events called an accident sequence.

Each sequence depends not only on the particular initiating event but also on the success or failure of various systems installed in the plant to perform mitigating functions. for instance, a pipe break in the reactor coolant system results in a loss-of-coolant accident (LOCA).[2] To respond to such an accident, plants are provided with various engineered safety features (ESFs) such as emergency core cooling systems, fission product removal systems, and containment. With all ESFs operating at their minimum design basis, the accident sequence resulting from a coolant pipe break is the design basis accident (DBA) LOCA defined in the AEC's reactor licensing process, and the consequences are quite small. With any one or all of the ESFs not performing their designed function, a broad spectrum of accident sequences can occur, each with a probability and consequences dependent on the operability state of the various ESFs.

In conventional safety analyses, a suitable design basis, including redundancy, is specified to assure a minimum level of operability of ESFs, and the likelihood or consequences of total failure of ESFs are not considered further. In this study all failures are considered possible, but appropriate probabilities are assigned to them. Thus, many potential accident sequences are described in the following discussions as if they will surely occur, with no reservations expressed as to their likelihood or significance. However, most of these sequences have such low probability that they do not contribute to the overall risk from reactor accidents. In fact, in order to make an overall risk assessment, a major task of this study was to identify the sequences that are the dominant contributors to risk.

In this study the initial failures or initiating events that could lead to significant consequences were examined to varying degrees. Those that seemed to contribute significantly to potential risks were analyzed in considerable detail; those that did not, received less detailed consideration. This is discussed more fully in section 3 of this appendix.

In considering the wide range of accident sequences that can occur following an initiating event, one needs a precise way of recording each significant sequence and defining the relationships between the operability states of the various ESFs and the effects of these operability states on the possible se-

---

[1] A discussion of the meaning of risk is presented in section 2 of the Reactor Safety Study Report.

[2] See Appendix IX for a description of a LOCA.

quences. One also needs a way of relating the probabilities of occurrence of the various accident sequences to their consequences. An explicit method is to use event trees, which are a modified form of the decision trees used in decision analysis (Ref. 1). Probabilistic techniques of this type have been developed over the past decade by applied mathematicians primarily for application to problems of decision making (typically in business), where the ultimate outcome of immediate actions is uncertain because of the influence of future events. Since reactor safety systems are largely automated so that the sequence of initiating events plus safety system responses involves few decisions, the term event trees is more appropriate than decision trees in studies of reactor accidents.

In section 2 of this appendix, the methodology used in event tree development is illustrated with a LOCA used as an example. Then the importance of the interrelationship between ESF functions and the systems provided to perform them is discussed. The need for and development of containment event trees is also covered. Finally, the utilization of event trees in risk assessment and their contribution in limiting the number of common mode failures requiring study is discussed.[1]

Section 3 of this appendix describes the approach taken to help ensure completeness of coverage of all significant accidents in the study. Section 4 covers accidents involving the reactor core, LOCA's, and transient events. The event trees for each of the LOCA types and for transients are discussed. Section 5 covers accidents involving fuel and radioactivity in locations other than the core such as in refueling, in the spent storage pool, etc. Table I 1-1 is a foldout glossary of terms and is located at the end of this section.

---

[1] In a simplified way, common mode failures can be thought of as multiple failures caused by a single event or failure. (See Appendix IV).

References

1. Raiffa, H., "Introductory Lectures on Making Choices Under Uncertainty," Addison-Wesley, 1968.

TABLE I 1-1 GLOSSARY OF TERMS

General

BWR - Boiling Water Reactor
DBA - Design Basis Accident
ESF - Engineered Safety Feature
EP - Electric Power
LOCA - Loss-of-Coolant Accident
PB - Pipe Break
PWR - Pressurized Water Reactor
RCS - Reactor Coolant System
RWST - Refueling Water Storage Tank
TE - Transient Event

ESF Functions

CI - Containment Integrity
ECC - Emergency Core Cooling
ECI - Emergency Coolant Injection
ECF - Emergency Cooling Function
ECR - Emergency Coolant Recirculation
PAHR - Post Accident Heat Removal
PARR - Post Accident Radioactivity Removal
RT - Reactor Trip

ESF Systems

PWR

ACC - Accumulators
AFWS - Auxiliary Feedwater System
CL - Containment Leakage
CLCS - Consequence Limiting Control System
CHRS - Containment Heat Removal System
CSIS - Containment Spray Injection System
CSRS - Containment Spray Recirculation System
CVCS - Chemical Volume Control System
HPIS - High Pressure Injection System
HPRS - High Pressure Recirculation System
LPIS - Low Pressure Injection System
LPRS - Low Pressure Recirculation System
PCS - Power Conversion System
NaOH - Sodium Hydroxide
RPS - Reactor Protection System
SICS - Safety Injection Control System

BWR

ADS - Automatic Depressurization System
CL - Containment Leakage
CSIS - Core Spray Injection System
CSRS - Core Spray Recirculation System
HPCIS - High Pressure Coolant Injection System
HPSWS - High Pressure Service Water System
LPCIS - Low Pressure Coolant Injection System
LPCRS - Low Pressure Coolant Recirculation System
RCICS - Reactor Core Isolation Cooling System
RHRS - Residual Heat Removal System
RPS - Reactor Protection System
SBGTS - Standby Gas Treatment System
SC - Secondary Confinement
SHA - Sodium Hydroxide Addition

Containment Event Tree Terms

CR - Containment Rupture
VSE - Steam Explosion in Vessel
CSE - Steam Explosion in Containment
OP - Overpressure of Containment
B - Burning of Hydrogen in Containment
MT - Core Melt Through of Containment
VS - Vapor Suppression

(ESF-XXX) - Damage to ESF due to XXX
Example: ESF-VSE and ESF-CSE

(CR-XXX) - Containment rupture due to XXX
Example: CR-VSE and CR-CSE

Section 2

Event Tree Methodology

The discussions in this section cover in some detail the principles followed in the development of event trees and the role of these trees in the risk assessment performed in this study. In section 2.1 the principles are illustrated by development of functional event trees for LOCA. In section 2.2 the development of containment event trees is shown. In section 2.3 the contribution of these trees to the risk assessment is illustrated. Section 2.4 discusses the contribution of event trees to the study of common mode failures.

2.1 LOCA FUNCTIONAL EVENT TREE DEVELOPMENT

Some simple event trees are presented here to illustrate the logic followed in the development of event trees in this study. These trees are concerned with a LOCA in a typical power reactor. Some of them are presented solely to illustrate the methodology and were not otherwise used in this study. The final functional event trees shown in Figs. I 2-6 and I 2-8 although not used in the study per se, are valid representations of the ESF functional interrelationships and as such are precursors of the actual LOCA trees in which ESF systems replace ESF functional headings.

In considering the events involved in a LOCA after the pipe break that is the initiating event, one must consider the functions that the ESFs are required to perform. Regardless of the design details of a particular reactor, the ESFs perform a uniform set of functions illustrated in Fig. I 2-9 which cover:[1]

a. Reactor shutdown or "trip" (RT) to stop significant power generation due to the fission process during the LOCA.

b. Emergency core cooling (ECC) to cool the core to keep the release of radioactivity from the fuel into the containment at low levels.

c. Post accident radioactivity removal (PARR) to remove from the containment atmosphere the radioactivity that could be released from the core.

d. Post accident heat removal (PAHR) to remove the core decay heat from the containment to prevent its overpressure.

e. Containment integrity (CI) to prevent the radioactivity not removed by PARR from being dispersed into the environment.

The drawing of an event tree (Fig. I 2-1) is started by indicating these functions, i.e., RT, ECC, PARR, PAHR, and CI, together with the initiating event, pipe break (PB), as event tree headings, in roughly chronological order. It proceeds from left to right by the addition under each heading of branches corresponding to two alternatives: successful performance of function (upper branch) and failure (lower branch). After the tree is drawn, paths across it can be traced by choosing a branch under each successive heading. Each path corresponds to an accident sequence. Six headings, five of which have two alternatives, result in a 2^{n-1} (where n = 6) event tree representing 32 accident sequences, designated S1 to S32. In Fig. I 2-1, S1 illustrates the DBA LOCA defined in the regulatory process.

When more headings are used because ESF systems replace the functional headings, the number of sequences can be quite large. Analysis of individual sequences indicates that many of them are illogical or meaningless and can be eliminated. In the process of increasing the detail in the headings and eliminating the unneeded sequences, continuing attention must be given to the order of the headings. Tree development is facilitated when the order corresponds generally to the logic of the accident

[1] Note that one ESF function required in the regulatory process, the handling of postaccident hydrogen generation has been omitted from this discussion on the basis that it has no significant impact on the overall risk assessment being performed. If the core does not melt, the containment building can be purged to prevent combustible hydrogen mixtures from occurring without releasing significant amounts of radioactivity; if the core does melt, more hydrogen is generated by the resulting metal-water reactions than the postaccident hydrogen system can handle.

process, i.e., when the headings whose failure affects the failure of others are located early in the tree. The rationale for the order in Fig. I 2-1 is as follows:

a. RT is listed first because failure to shut down the fission process during a LOCA could result in high core temperatures and thus nullify the effectiveness of ECC even if cooling water were provided.[1]

b. ECC is listed next because cooling determines whether or not the core will melt. If it does not, the consequences of pipe break will be very small; but if the core does melt, the potential consequences can be large and are strongly affected by PARR, PAHR, and CI.

c. PARR comes after ECC because its function is to remove any radioactivity released from the fuel into the containment.

d. PAHR is put just before CI because the containment has failure modes that depend on the performance of PAHR (as well as on ECC).

The form of the tree does not imply independence among failure events. Dependent as well as independent events can be handled provided the dependencies are appropriately defined.

The following discussion indicates how trees are expanded by inclusion of more detailed headings and reduced by elimination of sequences that are illogical or meaningless in terms of functional and operational relationships. Thus the event tree development process, like many of the other processes in this study, can be thought of as a filter into which all the elements involved in the matter under study are fed. The filtering action consists of eliminating all extraneous material so that the remaining elements are those that contribute to the risk and can then be quantitatively evaluated.

First, RT is eliminated from Fig. I 2-1 to simplify the later discussions and because (as shown below) it is not required in some cases.

---

[1]This aspect of RT is involved and depends on pipe break size and reactor type. Actual LOCA trees developed later in this appendix demonstrate how to handle RT correctly in specific situations.

This results in Fig. I 2-2, which is not very useful since extraneous sequences have not yet been eliminated.

Further development of the event tree requires analysis of the physical processes, such as core melting or overpressurization of the containment, that could occur when one (or more) of the functions is not performed. The analysis must include consideration not only of functional interrelationships but also of the interrelated operational factors involved with the physical systems provided to perform the functions. Such analyses are important also in the study of common mode failures because they define, if properly done, the only significant logically permissible sequences (i.e., those that appear in the event trees) and eliminate all others. Common mode failures need be considered only for the sequences remaining in the completed event tree.[1]

Development of the event tree to the form shown in Fig. I 2-2 was done without considering the following important topics:

a. The time dependent performance requirements for the physical systems needed to perform the various ESF functions.

b. ESF functional interrelationships such that failure of one function eliminates the need for another.

c. ESF functional failures producing physical processes that cause other functions to fail.

d. The effect of accident characteristics such as pipe break size and location on the event tree and on the operability requirements for the systems providing ECC.

The process for eliminating unnecessary sequences is discussed in the following sections.

2.1.1 TIME DEPENDENT FUNCTIONAL PERFORMANCE RELATIONSHIPS

The effect of the failure of one or more functions on the remaining functions varies with time after the initiating event. In the initial period after the pipe break (~1/2 to 1 hr.), all branches of the tree are permitted because functional interrelationships do not yet

---

[1]See section 2.4 and Appendix IV for further discussion of common mode failures.

exist. Functional interrelationships can come about only after this period because of the times involved in the physical processes resulting from failures in the initial period and because of performance requirements that change with time. If times beyond the initial period are considered, it is necessary to modify the event tree of Fig. I 2-2 to indicate these types of time dependent relationships.

In considering ECC, the performance requirements are seen to change greatly with time. The initial few minutes after pipe break are most demanding in that ECC must provide high flow rates at relatively high pressures to refill the core in the presence of blowdown of the reactor coolant system and at high levels of core decay heat. Once the core has been reflooded with cold water, the flow and pressure requirements are much reduced. The configuration of the physical systems required for successful performance also changes significantly with time.

It is therefore convenient to separate ECC into two discrete time phases: an emergency cooling injection mode (designated ECI) to cover the initial period, and a long-term recirculation mode (ECR) for the rest of the time (Fig. I 2-3). ECR is located between PAHR and CI on the tree because failure of PAHR causes failure of ECR, and failure of ECR causes failure of CI. The use of ECI and ECR in this tree illustrates considerations that pertain to the time dependent functional performance relationships between ECC physical systems and the ECC function.

2.1.2 FUNCTIONAL INTERRELATIONSHIPS

Other types of functional interrelationships are also found in the event tree. One type is such that a failure in one function eliminates the need for another. For instance, if ECI fails, the core will melt, and whether ECR functions or not becomes unimportant since it can no longer prevent the melt. The effect of this on event tree construction is to eliminate the ECR choices in sequences S17 to S32 of Fig. I 2-3 and to produce sequences S17 to S24 of Fig. I 2-4.

Another type of functional interrelationship is seen when the failure of a function causes other functional failures due to physical processes taking place. In general, these physical processes introduce a time delay between the failures that can be important in assessing consequences. In Fig. I 2-4, sequences S17 to S24 involve ECI failure. Without ECI, the core will melt and CI will surely fail; therefore, no CI choices should be shown in these sequences. It might be inferred, since failure of PAHR will result in overpressure and failure of CI, that PAHR choices should not be shown since ECI failure also causes failure of CI. However, PAHR affects the modes and timing of containment failure, as discussed below. Thus the PAHR alternatives should remain, and sequences S17 to S24 of Fig. I 2-4 reduce to sequences S9 to S12 of Fig. I 2-5.

Sequences S1 to S16 of Fig. I 2-4 assume availability of ECI and therefore no core melt in the initial period. However, if ECR were to fail, the core would melt and CI would fail; therefore, no CI alternatives should be shown where ECR has failed. If PAHR were to fail, then CI and ECR would both ultimately fail; the first because of overpressure and the second because the ECC water would get hot enough to cause pump cavitation. Thus, with PAHR failed, no ECR or CI alternatives should be shown, and sequences S1 to S16 of Fig. I 2-4 reduce to sequences S1 to S8 of Fig. I 2-5.

Figures I 2-3 and I 2-4 illustrate the initial period following pipe break when functional interrelations are not important and the later period when they come into play. Note that the logic used in developing Fig. I 2-5 allowed elimination only of the logically impermissible choices, and the number of sequences was thus reduced from 32 in Fig. I 2-3 to 12 in Fig. I 2-5.

Note that each sequence in Fig. I 2-5 may really denote one or more possible sequences depending on the timing of the various failures indicated in the tree. There are also timing and operational interrelationships between the functions shown in Fig. I 2-5 and the physical systems provided to perform the functions. To handle these hidden sequence possibilities within the sequences shown, sequence descriptions must be written that specify the significant differences. These are discussed below in connection with the actual event trees used in the study.

In addition to interrelationships between functions, there are interrelationships between functions and the ESF systems provided to perform them, called functionability-operability interrelationships. There are also interrelationships between the operability of one system and that of others, called

operability-operability interrelationships.

2.1.3 FUNCTIONABILITY AND OPERABILITY INTERRELATIONSHIPS

To advance beyond the functional event trees so far shown, one must consider explicitly the relationships between the functions to be performed and the respective physical systems provided to perform them. This is necessary in order to quantify the probability of success or failure at each branch of the tree. Since few actuarial data exist on the failure probabilities of these functions, estimates must be made by using reliability techniques. The failure probabilities of the various systems, and hence of their functions, can be calculated. This was done mainly by using fault trees.[1]

Table I 2-1 has as column headings the functions involved in event trees. In each column are listed the systems provided in the pressurized-water reactor (PWR) and the boiling-water reactor (BWR) to perform the function. The systems are described in Appendix II and are illustrated in Figs. I 2-10 and 2-11. Some examples of functionability-operability and operability-operability interrelationships are treated in the analysis.

Note that Table I 2-1 is only illustrative, since not all applicable interrelationships can be shown in a simple format, but it does show several examples of interest. The actual event trees and their sequence descriptions presented below provide a system for considering all significant interrelationships.

2.1.3.1 Functionability-Operability Interrelationships.

Table I 2-1 shows that, for the PWR:

a. Operation of both the containment spray recirculation system (CSRS) and the containment heat removal system (CHRS) are needed for PAHR to succeed; inoperability of either or both will cause failure.

b. Operation of the CSR system affects PARR also. In the initial period after LOCA, the containment spray injection system (CSIS) alone or with sodium hydroxide (NaOH) addition (SHA) can perform PARR, although with different but quite high efficiencies. Operation of the CSR system during this period would improve PARR somewhat. However, should core melting occur at some later time, due, say, to failure of ECR, the CSIS system would no longer be available because its water supply would have been expended in about an hour. If the CSR system were not operating at this time, PARR would fail when most needed.

c. Since CSR system failure causes PAHR to fail also, the result will be CI failure due to overpressure by steam. Furthermore, CSR system failure will also cause ECR failure since the low pressure recirculation system (LPRS) pumps will cavitate and cease to pump water to cool the core after CI fails.

Table I 2-1 shows that, for the BWR:

a. Operation of the low pressure coolant recirculation system (LPCRS) and the high pressure service water system (HPSWS) are both needed for PAHR to succeed; inoperability of either or both will result in failure.

b. If the containment leakage rate is relatively low (less than 100% per day), failure of the HPSW system will cause failure of CI due to overpressure by steam.[1]

c. Failure of the HPSW system will cause failure of the LPCR system by one of two routes:

   1. The loss of containment pressure due to failure of the HPSW system will cause the core spray recirculation system (CSRS) and LPCR system pumps to cavitate and cease to pump water for core cooling.

   2. If the containment leakage rate is greater than 100% per day, the torus water will ultimately get so hot that the CSRS and LPCRS pumps will cavitate and cease to pump water to keep the core cool.

---

[1] See Appendix II.

[1] Containment leakage is measured in percent of the contained free volume per day.

d. As noted above, failure of the HPSW system causes failure of CI. This influences PARR because failure of CI releases sufficient energy to cause failure of the blowout panels on the secondary containment (SC). Without SC, the radioactivity escaping from the failed containment cannot be released through the standby gas treatment system (SBGTS).

2.1.3.2 Operability-Operability Interrelationships.

An example of an operability-operability interrelationship involves Electric Power (EP). The ESFs that perform ECI, PARR, PAHR, and ECR functions all depend on the availability of EP. If EP were to fail, all the ESF systems associated with the above functions would fail. Unavailability of EP clearly represents a common mode failure of great importance. The electric power systems of nuclear power plants are therefore provided with a great amount of redundancy. Because of its importance, EP availability should appear explicitly on the LOCA event tree; this is shown in Fig. I 2-6, which is the same as Fig. I 2-5 except that EP failure has been added as sequence 13.

Less apparent interrelationships of this type are brought out in the analysis of event trees when two or more ESF fault trees are combined as required by some particular accident sequences. For instance, a common control system is provided for automatic initiation of operation of the PARR and PAHR systems. Should this control system fail, the PARR and PAHR systems could also fail. The relationships of the control systems to the performance of applicable ESF systems are included in the fault trees for the systems involved; the interrelationships of the control systems signals with more than one system are treated when the system fault trees are combined in specific accident sequences as defined by the event trees.

Perhaps a more direct example is the interrelationship between the low pressure injection system (LPIS), the high pressure injection system (HPIS), and the CSI system in the PWR. All these systems have the refueling water storage tank (RWST) as their water supply. Thus the fault tree for each of these systems includes the RWST and its failure modes. When the trees are combined as required by various event tree accident sequences, the RWST appears as a single failure that can affect the systems being combined. Components such as the RWST obviously represent potential common mode failures since their failure may contribute to the overall probability of occurrence of a particular accident sequence. Thus the systematic search for important interrelationships and the identification of potential common mode failures is greatly aided by the event tree and fault tree development and by their quantitative assessment (see Appendix II and IV).

2.1.4 PIPE BREAK LOCATION, PIPE BREAK SIZE, AND ECC SYSTEM OPERABILITY REQUIREMENTS

As mentioned earlier, it is also necessary to consider pipe break location, pipe break size, and the level of operability required of the redundant systems involved in ECCS. Since many hundreds (if not thousands) of combinations would result from consideration of all possibilities for these three factors, some reductions in choice are needed to make the analysis manageable. However, care must be taken not to eliminate possibilities that involve relatively high probabilities or large consequences since this would result in underestimation of the risks involved. The general approach taken throughout this study, in this as well as other areas, was to retain any choice that could be regarded as a significant contribution to the final risk assessment.

For example, with regard to break location, in general two types are of interest. In the PWR, the cold leg break is more demanding on ECC system performance than the hot leg break; in the BWR, the recirculation line break is more demanding than the steam line break. One approach would be to develop different pipe break trees for the two locations. This might be required if the failure probability were different for the two pipe locations. However, since available data on pipe failures are imprecise, only a single probability with a wide error band could be assigned for pipe failure occurring in the applicable segments of the reactor coolant system. Therefore, for ECC analysis, the break was assumed to occur in the location giving the most severe demand on the ECC systems.

With regard to break size, the combinations of ECC systems required to perform the ECC function differ for small breaks and for large breaks; some of the plant systems involved also differ. For instance, in the PWR, reactor trip (RT) is not necessary after a large pipe break because blowdown of the reactor

coolant system is so rapid that appreciable energy due to fission is not added to the core. Further, the ECC water added is borated so that the reactor will remain shut down even if RT fails. However, after a small LOCA, blowdown is slow enough that RT is needed to prevent addition of significant fission heat to the core during the blowdown. If RT did not occur, the effectiveness of ECC would be impaired. For these reasons different event trees were developed for large and small pipe breaks (discussed as follows).

For each physical system provided to perform the various post LOCA functions, the degree of system operability required for success had to be defined. For most ESF systems in a nuclear power plant, redundancy is provided which permits certain components to fail or to be out of service without impairing the ability of the system to perform its intended function. Further, if the system is degraded to such an extent that its performance is somewhat less than normally required for success, the system may still be capable of performing the required function depending on the margin incorporated in the design. In this study, system operability success is defined as the degree of performance required by the AEC Regulatory Staff, estimated with conservative assumptions. This approach is considered to be somewhat conservative in that some potentially successful levels of system operation are considered to be failures.

For example, for the PWR plant under study, four independent trains of equipment are incorporated in the CSRS, whereas, according to the Regulatory Staff, only two are used to satisfy the PAHR function. Thus in our study it was assumed that less than two CSR trains operating would lead to loss of PAHR, and the probability of CSRS failure was computed on that basis. However, there would actually be significant removal of heat with only one CSRS train operating. Since the probability of CSRS failure by loss of three trains is greater than by loss of all trains, some potential success paths have conservatively been assumed to result in failure.

With regard to ECI, the assumption in this study is that any situation involving calculated fuel cladding temperatures in excess of the AEC's Interim Acceptance Criteria results in complete core meltdown (see Fig. I 2-7) (Ref. 1). Note that, because of the redundancy provided in ESF systems to meet the requirements of the AEC's General Design Criteria, less than 100% (in fact about 50%) of the installed full flow capability satisfies the conservatively stated AEC rules for acceptable ECI performance (Ref. 2). This implies that some success level, full or partial, is possible at lower ECI flows (which have a higher probability of being provided) and thus more equipment failures could be tolerated. To avoid complex ECC performance calculations, all such potential successes are listed as failures. Although this approach is conservative and results in overestimation of risks, it was the only one feasible because of the state of the art of ECC performance calculations. The adequacy of ECC to cool the core, which was discussed extensively at the AEC's Emergency Core Cooling Rule Making Hearing and was the subject of an AEC order, December 28, 1973, will be addressed later (Ref. 3). It will be handled by inserting into later forms of the large LOCA event tree a heading for emergency cooling functionability (ECF). Factors contributing to ECF and the sensitivity of the ECF contribution to the overall risk assessment are discussed in Appendix V.

2.1.5 FUNCTIONAL LOCA EVENT TREES FOR WATER POWER REACTORS

The event trees presented so far have illustrated the logic involved in event tree development. Slight further modifications lead to actual functional event trees for a LOCA in pressurized water and boiling water power reactors. The major modification needed is appropriate inclusion of the RT function. Other minor modifications are discussed in later sections.

The correct representation of RT in the event tree depends on the following considerations:

a. Since RT occurs automatically with loss of EP in both types of reactors, it is proper to place the RT heading after EP.

b. The purpose of RT is to halt generation of heat by the fission process during the LOCA.

c. In the PWR, RT does not in general affect the course of a LOCA, since ECC water is borated and therefore prevents the fission process from restarting even if RT fails. Thus RT is not needed in the large LOCA event tree. However, if the pipe break is small, the blowdown is slow

and the fission process can generate significant heat after normal heat removal has stopped. RT is therefore needed in the small LOCA event tree since it prevents the core from overheating during plant blowdown.

d. In the BWR, ECC water is not borated and its addition would not prevent the fission process from restarting if RT failed. RT is therefore needed in the BWR LOCA trees for all break sizes.

In line with consideration c above, Fig. I 2-6 is a functional event tree directly applicable to a large LOCA in a PWR. Addition of RT results in another tree (Fig. I 2-8) directly applicable to a small LOCA in the PWR and to both small and large LOCAs in the BWR. The added sequences are S13 to S16, in which the success and failure paths for ECI and ECR are omitted because, since RT failure is assumed to result in core melt, their availability is irrelevant. The assumption of core melt with failure of RT following a pipe break is conservative because it is not clear when or if core melting will occur. What will occur in the BWR, for example, when ECC water is added, is "chugging," i.e., as water is added to the core, fission restarts and generates enough power to blow the water out of the core and thereby stop the fission process. Gravity returns the water to the core, and the cycle is repeated. How long "chugging" could continue without damage to the core is difficult to assess, but some time may be available for manual RT. The difficulties of assessment led to the conservative assumption that failure of RT would result in core melt.

The event trees above were presented to illustrate the thought processes involved in developing the LOCA trees used in this study. The actual LOCA trees were not made in such a detailed step-by-step process but were drawn more directly, with iterations, and with the many interactions examined to assure completeness and adequacy. Note, however, that functional trees in Figs. I 2-6 and I 2-8 can be converted directly into LOCA trees related to actual plant systems by substituting the appropriate systems from Table I 2-1 for the headings in the figures. Care is needed in grouping some systems, such as those associated with ECC, to keep the tree to a manageable size. Further small adjustments needed for CI and other system interrelationships are discussed below.

2.1.6 NEED FOR CONTAINMENT EVENT TREES

Before proceeding further, the best way of handling containment integrity (CI) on the event tree must be considered. During a LOCA, CI can fail by two basic mechanisms: (1) the containment can fail to isolate (i.e., close its normally open valves to keep leakage rate low), and (2) as mentioned earlier, many physical processes that may occur following core melt or PAHR failure can cause rupture of CI. A significant number of headings would be needed on the LOCA event tree to describe all the various failure modes. It is therefore convenient to construct a separate containment event tree whose input consists of the sequences on the LOCA tree that cause core melt (see next section). The resulting two small and closely coupled trees are easier to handle than a single large tree having up to 200 sequences.

2.2 CONTAINMENT EVENT TREES

2.2.1 GENERAL DISCUSSION OF CONTAINMENT EVENTS

The assessment of possible consequences of reactor accident sequences requires estimation to type, quantity, and rate and time of release of radioactivity from the containment to the environment. Various potential LOCA sequences were identified above in terms of possible ESF functional failures. Most of these sequences, although of low probability (as shown below), lead to core melt and subsequent loss of containment integrity. A detailed analysis of the physical phenomena resulting from core melt and causing loss of CI is given in Appendix VIII.

The central role of the CI function in determining the amount of radioactivity released in an accident sequence makes it important to identify and analyze the various modes of containment failure. This is more conveniently approached through development of a separate containment event tree. The sequences on such a tree may be treated as continuations of the LOCA trees, core melt sequences, which are regarded as "inputs" to the containment tree.

The LOCA tree generally defines as a function of time after pipe break the spectrum of probabilities and amounts of radioactivity in the containment atmosphere, whereas the containment tree defines, as a function of time, for each LOCA tree sequence, the probabilities and amounts of radioactivity released to the environment. The containment event

trees presented below are applicable not only to LOCA sequences but to most sequences involving core melt,[1] regardless of the type of initiating event, if the physical processes set in motion by the core melt are the same.

The variation in modes of containment failure is most significantly affected by physical processes capable of large energy releases into the containment. The potential of such energy releases to cause further damage by missiles or high pressure must be examined with regard not only to potential containment rupture but also to possible damage to ESFs such as those needed for PARR and PAHR, whose continued operation might affect the course of a particular accident sequence.

Before outlining meaningful accident sequences involving containment failure modes, containment failure must be clarified. The purpose of containment is to provide a barrier to the release of radioactivity under post-accident conditions. Containment failure can occur basically in three ways: (1) excessive leakage due to lack of adequate isolation of the containment atmosphere from the external environment, and (2) gross rupture due to physical processes resulting from core meltdown, which allows rapid release of radioactivity, and (3) overpressure rupture which precedes the core meltdown processes.

The subsequent discussions on containment failure focus on the first two ways above where the core meltdown is occurring prior to gross containment rupture or during the time when inadequate isolation has occurred. Item (3) represents particular sequences where the containment ruptures through overpressure prior to core meltdown; then because core cooling systems are rendered inoperable by the overpressure failure, meltdown occurs with excessive leakage via the ruptured containment. In the latter case, the release of radioactivity occurs somewhat continuously and depends on the driving forces developed by the meltdown processes.

[1]In some cases such as pressure vessel rupture, the violence of the initiating event can result in direct coupling to containment failure so that use of a containment tree would not be appropriate.

All the above containment-failure mode possibilities were examined as part of the study.[1]

While it is nearly impossible to obtain zero containment leakage, the leakage rates are minimized by three aspects of containment design: (1) a continuously welded steel membrane with carefully designed penetrations, (2) isolation of the containment atmosphere, by valves and controls, from external systems that are isolated from the environment and can withstand containment pressures, and (3) isolation, by valves and controls, of the few systems that could potentially interconnect the containment atmosphere and the environment.

In normal operation, the containment atmosphere is isolated from the environment, with a few exceptions. The containment building has many electrical and piping penetrations for supplying services to the reactor and taking output steam to the turbine. The piping contains fluids or gases and air, and it is connected to "closed" systems outside the containment that are isolated from the environment. When a LOCA occurs, although the containment atmosphere is already largely isolated from the external environment, the isolation valves of the penetrations to the "closed" systems receive signals to close. The purpose is not really to achieve isolation from the environment, but rather to eliminate whatever leakage would occur through seals, gaskets, and the like in these "closed" systems. The so-called containment isolation system is really a containment leakage-control (CLC) system, with the following exceptions:

a. The PWR has two small (2-in. dia.) vacuum pump line penetrations each having two isolation valves outside containment that are called upon to close when LOCA occurs. However, both of these penetrations ultimately connect to a common vacuum pump exhaust line. In this line is a normally open valve which is designed to trip closed on a high radiation signal. Thus failure to isolate for each of these penetrations would involve failure of three valves to close.

b. The BWR has 26-in. dia. main steam lines that connect the reactor vessel to the main turbine and condens-

[1]See Appendices V and VIII

er. Each line has two isolation valves, one inside and one outside containment, that have to close. These are backed up by the turbine stop valve. Failure of containment to isolate would involve failure of at least two containment isolation valves in the same steam line plus failure of the turbine stop valve to close.

c. Also for the BWR, there are three equipment cooling loops in the drywell that are "closed" to drywell atmosphere. However, it is fairly likely that the LOCA itself will fail one or more of these loops and cause it to be open to containment atmosphere. The cooling loops (two chilled water and one reactor building cooling water) are not completely closed to secondary containment external to the drywell. In the three loops the only significant opening to secondary containment is the two inch vent in the reactor building cooling water head tank.

   Protection against leakage is based on maintaining the integrity of the closed loops inside the drywell backed up by the optional closing of valves outside the drywell by the operator.

d. Additionally in the BWR there are drywell equipment and flood drains that connect sump pumps in the drywell to vented tanks in the secondary containment through dual two inch isolation valves that are occasionally opened for pump operation. The valves are given isolation signals when the LOCA occurs and closure of either valve in a line will insure isolation.

Thus, were the CLCS of the PWR to fail, the leakage rate for the containment atmosphere to external environment could be equivalent to that due to about a 3-in. dia. hole. As shown below, this by itself would not be enough excess leakage to be classed as a containment failure. For the BWR, on the other hand, if the steam line isolation valves and the turbine stop valve failed to close, the containment pressure could rupture the main condenser and thus provide a path to the outside atmosphere. Failures in the BWR cooling loops or drain lines, the former the more probable, would result in two inch openings to secondary containment.

Containment failure in terms of gross rupture was defined above as involving rapid release of the containment atmosphere to the environment. Containment rupture has been conservatively treated in risk assessment, the assumption being that violation of containment integrity by some physical process resulting from core melt is a gross rupture rather than an increase in leak rate. For each reactor, the specific assumption has been that gross rupture occurs if containment pressure reaches about twice design pressure.[1]

Containment failure due to excessive leakage is harder to define. Clearly there is a spectrum of containment leakage rates with their associated probabilities. However, to define how containment leakage affects accident sequences on the event trees, three factors must be considered: (1) the effect of containment leakage on the operability of various ESFs; (2) the competition for post-accident radioactivity between removal systems and the leakage to the environment, and (3) the relationship of leakage to physical processes, such as pressure buildup, occurring during the accident sequence. These are discussed below.

In developing the containment event tree, the first step is to define headings representing possible events that can significantly affect modes of containment failure or the resulting releases. Containment leakage (CL) is one such heading. Other headings are defined according to one of the two results, rupture of containment (CR-...) or damage, without CR, to mitigating ESFs (ESF-...) together with the appropriate causal mechanisms. By analyzing the physical processes accompanying or resulting from core melt, one can identify the following potential mechanisms of interest:

a. CL may affect physical processes within the containment and thus affect modes of rupture, operation of ESFs, or consequences of accident sequences.

b. A steam explosion in the reactor vessel (VSE), which could occur by interaction of finely dispersed molten fuel with water, could release sufficient energy to result in CR-VSE or ESF-VSE.

---

[1] See Appendix VIII for the specific pressure levels used and the technical bases underlying this assumption.

c. A steam explosion within containment (CSE), which could occur if molten core material contacted water, could release sufficient energy to result in CR-CSE or ESF-CSE.

d. Overpressure (OP) of containment may result from generation of noncondensable gases, hydrogen and carbon dioxide, by metal-water reactions or by interaction of molten core material with concrete; OP may result also from lack of heat removal capability. CR-OP or ESF-OP could result.

e. Damage to containment due to the explosion or burning (B) of hydrogen generated by the reactions between molten materials and water could result in CR-B or ESF-B.

f. Melt-through (MT) may lead to violation of CI, if some other process has not already done so, since the molten core material will penetrate through the bottom of the containment structure.[1] The result would be CR-MT.

Each possible heading must be examined in terms of the characteristics of the specific reactor to determine whether or not it represents an event that should appear on the tree for that reactor.

2.2.1.1 Containment Leakage.

a. The potential effects of leakage during accident conditions involve more considerations for the BWR than for the PWR. There are interrelationships between leakage rate, containment pressure, and the performance of systems carrying out ECR and PARR functions. Leakage also affects the potential for containment rupture due to physical processes occurring during the low probability accident sequences involving ESF failures. The interrelationships of interest are as follows:

- Leakage and Containment Failure. Two physical processes that could potentially rupture the containment are generation of noncondensible gases by reaction between metal and water or molten fuel and concrete, and generation of steam pressure due to loss of post-accident heat removal from the containment. However, if containment pressures are relieved by sufficient leakage, then overpressurization will not occur. Analysis indicates that a leakage path equivalent to about a 1-in. dia. hole (about 100% per day leak rate) will prevent containment overpressure. Since CL of that size will be on the LOCA tree (see below), the particular LOCA accident sequence will determine whether or not such overpressure will occur.

- Leakage and ECR. If the leakage rate is greater than about that from a 1-in. hole and also the HPSW system fails, then the LPCR and CSR system pumps will ultimately cavitate and fail. Since these systems are more conveniently shown on the LOCA tree than on the containment tree, they should be preceded by a leakage heading on the BWR LOCA tree to show the necessary interrelationships. Thus each accident sequence on the LOCA event tree will indicate whether the leakage path in the containment is smaller or larger than the equivalent of a 1-in. dia. hole.

- Leakage and PARR. The BWR is provided with multiple PARR features (see Fig. I 2-11 and Table I 2-1). PARR is achieved within containment by a vapor suppression (VS) system. As steam and gases are forced through the torus water after the LOCA, a limited amount of radioactivity is retained in this pool. Therefore in assessing the consequences one should distinguish between leakage from the containment drywell, which allows the containment contents to escape without the retention action of the pool, and leakage from the containment wetwell, which allows exit only after some scrubbing. This leak location is most conveniently shown on the containment event tree.

In addition to the VS system, PARR capability in the BWR is provided also by outside containment. The reactor building, or secondary

[1] It is assumed that in every case of core melt, regardless of the mode of containment failure, the nonvolatile portion of the core will always melt through the bottom of the containment. See Appendix VIII for analyses and discussion on the melt-through event.

confinement (SC), surrounds the containment and forms a pathway for radioactivity released from the containment to go to the standby gas treatment system (SBGTS), which provides for filtration and elevated release through a stack.

The SBGTS will be ineffective if integrity of SC is not maintained (i.e., if the integrity of the pathway is destroyed). Analysis indicates that if the CL rate exceeds the equivalent of that due to a hole about 6 in. in diameter (about 3600% per day at LOCA blowdown pressure), SC integrity will be violated and the SBGTS will be ineffective.[1] SC and SBGTS (as shown below) will be located on the containment event tree, and CL in the 5-in. dia. equivalent range should precede them on that tree.

b. For the PWR, leakage can affect the physical processes leading to potential containment rupture. At a sufficient rate, leakage prevents the burning of hydrogen by keeping its concentration in the containment below that required for combustion. At about the same rate, it also prevents overpressure which would result if containment heat removal were to fail. Analysis indicates that the penetration of containment required to attain this rate would be equivalent to a hole about 4 in. in diameter[1] (giving a leakage rate of about 200% per day at LOCA blowdown pressure).

   For the PWR, since CL has no significant interrelationships with operability of ESFs, CL is conveniently shown on the containment tree.

2.2.1.2 CR-VSE, ESF-VSE.

When the core melts, there is some potential for a steam explosion, but it would require efficient interactions of the molten fuel with the water in the vessel.[2] An explosion small enough not to rupture the reactor vessel has no potential interrelationships with mitigating ESFs or containment. An explosion large enough to rupture the reactor vessel but not the containment has potential interrelationships with ESFs having PARR and PAHR functions within the containment, whose continued operation is of interest, because of the energy released into the intact containment. An explosion large enough to rupture the reactor vessel and the containment has no such ESF interrelationships because all the volatile radioactivity will be quickly released from the containment.

In the BWR, the space between the reactor vessel and the containment is small; therefore, any steam explosion rupturing the reactor vessel would almost certainly rupture the containment also because of the missiles due to vessel rupture. Once the containment ruptures, the ESFs within containment are of no further interest; the ESFs outside containment will fail as a result of CR because SC cannot withstand the energy release.[1]

In the PWR, the PARR and PAHR ESFs (i.e., CSRS) pumps, pipes, and heat exchangers within the containment are quite well shielded by massive structures from potential missiles generated by vessel rupture; therefore, they are not likely to be damaged by vessel rupture due to a steam explosion.

Based on the foregoing, for both the PWR and the BWR, CR-VSE should appear on the containment event trees but ESF-VSE need not.

2.2.1.3 CR-CSE, ESF-CSE.

If a steam explosion does not occur in the reactor vessel, the decay heat in the core is sufficient to melt the bottom of the vessel and allow core material to fall to the bottom of the containment.[2] Here again, there is some potential for a steam explosion.

For the PWR, the likelihood is low:

a. If the steam explosion occurred after the spray (CSIS and CSRS) and CHRS had been operating, the containment pressure would be low, and the thermal energy released in the

---

[1] See Appendix VIII.

[2] A steam explosion might be precluded if the reactor vessel contained no water, but the probability of having no water in the vessel is considered to be negligibly low.

---

[1] The bulk of the secondary containment building is reinforced concrete, but its upper level is covered with fragile siding that would be blown out by slight pressures.

[2] See Appendix VIII.

explosion could be absorbed without resulting overpressure.[1]

b. If the sprays had not operated, the reactor cavity would contain little water, and the likelihood of a large steam explosion would be low.

c. If a steam explosion did occur, the massive structure (vessel, reactor cavity, crane support walls, etc.) would offer significant protection to the containment and ESFs against missiles that might be generated.

Since the likelihood of a steam explosion in the containment is low and since the likelihood of its damaging the containment or ESFs is also low, CR-CSE and ESF-CSE need not be considered for the PWR.

For the BWR, the containment, having a relatively small free volume, has some likelihood of rupturing should a steam explosion occur; therefore, CR-VSE should appear on the containment tree. ESF-CSE need not appear because the remaining effective PARR ESFs (the secondary confinement) would no longer serve a useful purpose since the most likely path to containment failure would be overpressure by the generation of noncondensible gases.

2.2.1.4 CR-OP, ESF-OP.

The buildup of pressure within containment has two potential sources: generation of steam pressure by decay heat from the molten core and generation of noncondensible gases. The first can occur only if the capability for heat removal from containment, PAHR, has been lost. The second involves hydrogen, formed by water reacting with zirconium and steel, and carbon dioxide, formed by molten fuel interacting with the concrete in the containment floor.

For the PWR, analysis has shown that noncondensibles cannot cause overpressure in the containment because of its large volume.[1] Loss of PAHR, however, can lead to potential containment rupture; therefore, CR-OP must be included in the containment tree, its occurrence depending on whether PAHR has failed in the LOCA sequence being followed.

Since loss of PAHR leads to high containment pressure, the only mitigating ESF that could continue to operate is the CSR system, which would provide radioactivity removal capability. By the time high pressure was experienced, however, the PARR function provided by the CSRS would have been largely completed. Therefore ESF-OP is of no interest and should not appear on the PWR trees.

For the BWR, both sources of overpressure lead to potential modes of containment failure. Analysis indicates that, should CR-VSE or CR-CSE not occur, then LOCA sequences involving core melt would inevitably lead to failure by overpressure from one or both sources (steam or gas pressure) unless leakage were sufficient to keep pressure below the point of rupture. Since effective PAR ESFs are not located within the containment and would not be affected by pressure below that inducing rupture, ESF-OP is not an applicable heading for the BWR tree, CR-OP, however, is a required heading, the principal mechanism of rupture (steam or noncondensables) being determined by the LOCA sequence.

2.2.1.5 CR-B, ESF-B.

Hydrogen has been discussed as a source of pressure; it also has the potential to burn or to explode.

For the PWR, containment rupture due to hydrogen burning is possible, and CR-B is a heading for the containment event tree. The likelihood of a hydrogen explosion within the containment is negligibly low because all processes leading to large-scale hydrogen generation are accompanied by generation of enough steam to dilute the hydrogen below its explosive concentration.[1]

Passive components of mitigating ESFs (CSRS) are located within PWR containment, and redundant pumps are located outside. Analysis has shown that inside components are well shielded from flame impingement. On the basis of component location, therefore, ESF-B can be eliminated from the PWR tree.

For the BWR, as noted above, in the absence of CR-VSE or CR-CSE, an overpressure induced CR must result from

[1]See Appendix VIII.

[1]See Appendix VIII.

core melt, unless it is precluded by containment leakage in excess of that caused by a hole about 1 in. in diameter (100% per day at LOCA blowdown pressure). For low leakage, an overpressure failure would occur before explosion or burning of hydrogen. Leakage sufficient to preclude an overpressure failure of containment would likely prevent buildup of hydrogen to an explosive or combustible concentration. Therefore, CR-B and ESF-B are not appropriate for the BWR containment event.

2.2.1.6 CR-MT.

Core melt-through of the containment is an inevitable result of core melt, but it is a potential mode of containment integrity failure only for the PWR. For the BWR, either the containment failed because of overpressure before melt-through or containment leakage was large enough to prevent overpressure.

In the above discussions, the necessary headings have been identified for each containment event tree as follows:

For the PWR: CL, CR-VSE, CR-OP, CR-B, CR-MT

For the BWR: CL (specified as to location and rate, CR-VSE, CR-CSE, CR-OP, SC, SBGTS

Construction of each tree requires placement of applicable headings in logical order and elimination of illogical or physically meaningless sequences. The PWR and BWR containment event trees used for risk assessment are presented below.

2.2.2 PWR CONTAINMENT EVENT TREE

A description of PWR containment appears in Appendix II. The physical processes anticipated following core melt are analyzed in Appendix VIII.

The potential events that can affect PWR containment after core melting were identified in the preceding section. To construct the PWR containment event tree (Fig. I 2-12), the events were put into logical order and unnecessary sequences were eliminated.

CR-SEV is placed first on the tree because, if such a steam explosion occurs, it will occur before any of the other possible gross containment failure modes. CR-VSE has no branches on the path for its occurrence since it precludes the other events.

CL precedes CR-B and CR-OP because leakage at a sufficient rate precludes both hydrogen burning[1] and pressure buildup sufficient to violate containment. The CL occurrence path therefore has no branches for CR-B or CR-OP.

CR-B is included in the containment event tree because in some accident sequences, the availability of coolant to generate steam imposes a limit on the steam partial pressure that can be developed in the containment atmosphere. In such circumstances, the presence of additional energy to superheat the containment atmosphere can raise the containment pressure into the rupture range; thus this incremental pressure from hydrogen burning leads to containment failure. CR-B preceeds CR-OP because if hydrogen burning occurs, it will likely occur before sufficient partial pressure of steam can build up to cause containment failure. Whether or not CR-OP occurs, or the incremental pressure from hydrogen burning is of importance depends on the operability state of the containment heat removal system (CHRS), which is specified by the input sequence. With the CHRS system operating successfully, CR-OP cannot occur.

CR-MT is placed last because melt-through generally will occur last and will not contribute significantly to consequences.

In Fig. I 2-12 each heading has been assigned a Greek letter. The sequences on the tree are assigned the same letters to indicate their modes of containment failure. These letter designations are used later, in accident sequence descriptions, to indicate the possible failure modes considered in the asessment of probabilities and consequences.

2.2.3 BWR CONTAINMENT EVENT TREE

A detailed description of BWR containment and its isolation system appears in Appendix II. The physical processes anticipated following core melt are analyzed in Appendix VIII.

The basic containment events have been identified as CL (specified as to location and rate), CR-VSE, CR-CSE, CR-OP, SC, and SBGTS. The tree (Fig. I 2-13) was constructed by placing the events in logical order and identifying the branches of interest.

---

[1] See Appendix VIII.

CR-VSE is placed first on the tree because, if such a steam explosion occurs, it will occur before any other gross containment failure. The occurrence path has no branches since it precludes the other events.

Since explosion in the containment could occur only after vessel meltthrough and elimination of the possibility of a steam explosion in the vessel, CR-CSE is placed second. No branches for the remaining events are shown on its occurrence path since they would be precluded.

CR-OP is placed third because, if it occurs, the resulting energy release will cause failure of SC and SBGTS; no branches are shown for these on its occurrence path. CR-OP is closely related to leakage events, which are therefore placed next to it.

If sufficient leakage should not occur, then, without a steam explosion, CR-OP would almost certainly follow core melting. Therefore, on the path for non-occurrence of CR-OP, leakage rate is pre-determined as not less than that from about a 1 in. hole. The locations of interest are the wetwell and the drywell, since the magnitudes of radioactivity release from them differ, as noted above.

For either location of interest, the rate of leakage determines the potential for successful PARR outside the containment. The two branches correspond to leakage rates less than or greater than the rate that would cause failure of SC. This rate is equivalent to that from a hole about 6 in. in diameter. Accordingly, the occurrence path for the larger leakage rate has no success branches for PARR features.

Finally, SC is placed before SBGTS because SC integrity is necessary for guiding releases to the SBGTS. These headings complete the tree because, although meltthrough is an inevitable eventual result of core melting, it is highly unlikely to be an initial mode of containment failure for the BWR. As in the PWR tree in Fig. I 2-12, each heading in Fig. I 2-13 has been assigned a Greek letter. The CL heading has been assigned two locations, one in the LOCA tree and one in the containment event tree, to distinguish large (>6") equivalent opening and moderate (1" - 6") leakage. (Non-occurrence of CR-OP assumes leakage of at least 1".) These letters appear at the right of the figure to designate containment failure modes to be considered in consequences assessments.

2.3 USE OF EVENT TREES IN RISK ASSESSMENT

The event trees used in this study have provided the basic tool for relating the probabilities and consequences of radioactivity releases from the containment into the environment. Probabilities for the events shown on the trees have been estimated by a number of special analyses: fault tree analyses were made to identify system elements contributing to failures of systems and functions to quantify the probability of these failures under accident conditions; probabilities were estimated for the various modes of containment failures; and analyses were done to estimate the probabilities of occurrence of accident initiating events. Further, analyses were made of the mechanisms of radioactivity release and transport from the fuel into the containment atmosphere for each accident sequence in the LOCA tree.

Modes of containment failure were analyzed to determine the magnitude of the release from the containment to the environment for each sequence. The event trees provide a framework and an organizing principle for linking together the results of all these analyses.

Figure I 2-14 illustrates how event trees are used to combine probabilities of events in estimating the probability of a sequence. It shows the probability of a functional failure for each failure branch on the LOCA tree in Fig. I 2-6. Functional failure probabilities are derived from probabilities of failure modes for the systems performing the functions. The same functional failure has different probabilities in different sequences. Assignment of a failure probability to a system requires precise definition of its failure, i.e., a criterion, and consideration of the conditions under which the system is called upon to perform, i.e., a context. Both context and criterion may vary not only with initiating events but also for different paths on the same event tree. For example, for the ECI function the criteria for success or failure depend on whether the LOCA is initiated by a small or a large pipe break, as indicated in Table I 2-1.

Each specific system performing ESF functions may have various failure modes, some of which may be inconsistent with the success of other related

systems. For example, for the PWR, since both PAHR and PARR are automatically initiated by a single control system, failure modes for PAHR on a success branch for PARR do not include failures due to that control system. For sequence S3 in Fig. I 2-14 the probability of PAHR failure, P_{E1}, does not include failure of initiating signals. However, for sequence S6, P_{E2} may include failure modes due to the signal system, since PARR fails in this sequence. Furthermore, since sequence S6 involves the failure of two systems, i.e., D and E, then the two must be examined carefully for additional dependencies or common mode failures.

2.3.1 LINKING ACCIDENT EVENT TREES AND CONTAINMENT EVENT TREES

An accident sequence that results in core melting is not completely described without consideration of potential containment failure modes. Figure I 2-15 shows how a containment event tree is used in conjunction with an accident event tree. The containment tree here is the PWR tree in Fig. I 2-12. The containment integrity (CI) function must be considered for every sequence; three sequences are illustrated in Fig. I 2-15:

a. For sequence S1, all functions after the pipe break are successful and the core does not melt; therefore, the only function of interest on the containment tree is CL.

b. Sequence S3 results in core melt because PAHR fails. Overpressurization is a likely mode of failure also due to the PAHR failure, and this is reflected in the assigned probability for this sequence.

c. Sequence S7 results in core melt due to ECI failure, but it includes a success branch for PAHR. For the PWR, the PAHR success implies negligible probability of containment failure through overpressure with or without hydrogen burning (path δ and γ). Thus the δ and γ paths are eliminated from the containment event tree. All other containment failure modes are possible, each with its appropriate probability.

2.3.2 ASSOCIATING PROBABILITIES AND CONSEQUENCES

Each complete accident includes the containment failure mode, if any, that leads to a potential release of radioactivity[1]. Any specific combination of ESF failures may lead to releases differing in quantity and type of radioactivity as well as in time of release, depending on the containment failure mode. On the other hand, different accident sequences may lead to similar releases, which would then have equivalent consequences. For risk assessment, the goal is to determine the probabilities associated with different consequence levels (Fig. I 2-16). An intermediate step is to calculate the probabilities associated with radioactivity release; event trees provide a framework for doing this. Probabilities of all complete sequences can be combined to obtain the probability that this particular level of consequences will occur.

It is now possible to make more explicit the concept of "significant contribution to risk" alluded to earlier. The significance of the contribution of any particular accident sequence to potential risk depends on the relationship of both its probability and its consequences to those of other sequences. As stated, the goal of the risk assessment is to determine the probabilities associated with representative levels of consequence. To that end, sequences with equivalent consequences are ultimately grouped together, and their probabilities are combined to determine the probability that this consequence level is reached in an accident. Therefore, if any accident sequence has a very much smaller probability than others with the same consequences, it can be omitted without appreciably changing the associated composite probability. For illustration, Fig. I 2-16 shows the probabilities, for each consequence interval chosen, for a few complete sequences. These are representative of sequences having significant contributions at distinct levels.

2.3.3 DESCRIPTIVE MATERIAL ON ACCIDENT SEQUENCES

In the risk assessment process, estimation of probabilities and consequences requires determination of a number of specific parameters associated with each potential sequence:

a. Context and criterion of successful operation of systems providing accident mitigation functions.

---

[1] See Appendix V for Release Magnitude Categories.

b. System interrelationships that either preclude or make more likely various failure modes for individual sequences.

c. Parameters associated with potential radioactivity release which are needed to assess probable consequences in terms of public safety.

These parameters are used as input to the analytic studies reported in other appendices. Appendix II presents fault tree analyses, which require context and criterion definitions as input. System interrelationships in terms of failure modes are essential to the event tree quantification analysis in Appendix V. The consequence model in Appendix VI requires parameters of radioactivity release magnitudes and associated probabilities for estimation of potential implications for public safety.

The required information for each accident sequence is incorporated in tabular sequence descriptions that accompany the event trees to be presented in section 4 of this appendix.

To provide the kinds of information needed, the sequence descriptions incorporate (1) operability status of systems, (2) core conditions, and (3) the timing of various physical processes.

2.3.4 RADIOACTIVITY RELEASES

The core of a reactor that has operated for some time contains radioactive material (due to the fission process) in forms not present in the original fuel. The various radioactive species also differ widely in important characteristics including physical properties such as melting temperatures, volatilities, oxidation potentials and chemical affinities that affect their release magnitudes and their dispersal when released; radioactive properties such as half life and the form and energy of radioactive emissions; and biological properties that influence the health effects associated with exposure, inhalation, or ingestion of the radioactive materials after release.

Studies of the anticipated magnitude of radioactivity released from nonmolten and molten cores and from the containment as a result of various potential accident processes are presented in Appendix VII in terms of the fractional release of available inventories.

Calculation of potential consequences from releases of radioactivity requires consideration of reactor site characteristics such as weather and demography, and the release conditions such as height, energy discharged, and time. An estimate on these factors and of the inventory of biologically important fission products contained in reactor cores is given in Appendix VI. The methodology used for consequence calculations is also described in considerable detail.

2.4 CONTRIBUTION OF EVENT TREES TO THE STUDY OF COMMON MODE FAILURES

The potential effects of common mode failures (CMFs) on the safety of nuclear power plants have been increasingly discussed in recent years. Current design requirements related to safety address this matter in certain areas, principally with regard to possible external forces due to natural phenomena and airplane crashes. This is because a large external force such as an earthquake might not only initiate an accident but also result in failures of engineered safety features provided to mitigate the accident. Therefore, all the systems that contribute to assuring the safety of the plant (e.g., the reactor coolant system and all the ESFs) are designed to withstand substantial earthquakes without failure (Ref. 1). In addition to the above, LOCAs can impose large reaction forces and cause missiles which have the potential to damage components whose failure can interfere with the performance of ECCs and other ESFs. This has led to the use of pipe restraints, missile shields and other such design requirements to prevent damage by the LOCA. Beyond this, limited analysis has been done to quantify the effects of potential common mode failures on reactor accidents.

An important objective of this study has been to develop methodologies suitable for quantifying the contribution of common mode failures to reactor accident risks (see Appendix IV). Event trees play a role in CMF studies because they eliminate illogical and meaningless accident sequences. Evaluation of potential CMF contributions requires examination of the potential CMF interrelationships of the various events in each accident sequence; any sequences that can be eliminated need not be examined. The disciplined examination of the function-to-function, function-to-system, and system-to-system interrelationships in the specific context defined by the accident sequences has

made a key contribution in limiting the magnitude of the CMF effort needed in this study.

A measure of this contribution is comparison of the number of interactions possible with the number actually involved. This can be done, for instance, by examining the large LOCA and containment event trees described above for the PWR and BWR. The PWR trees have 8 and 5 headings, respectively; the BWR, 9 and 7. Use of 2^{n-1} tree with all possible permutations and combinations of choices included would give roughly 4000 accident sequences for the PWR and 32,000 for the BWR. Since each sequence would have 12 and 15 elements, respectively, the number of potential CMF interactions to be investigated would be about 48,000 for the PWR and about 480,000 for the BWR. However, the PWR and BWR large LOCA and containment event trees involve only about 150 sequences each, with an average of about 10 potential interactions per sequence. Thus the total number of potential interactions for the PWR and BWR would be about 1500 each, or a reduction from the 2^{n-1} approach of about a factor of 32 for the PWR and 320 for the BWR.

Thus, for the large LOCA, the use of event trees has eliminated illogical and meaningless combinations of events and thus reduced the areas requiring examination for CMFs by about three orders of magnitude. This approach contributes enormously to making the analysis of potential CMFs tractable.

In considering the total number of event trees involved in the overall study (see sections 4 and 5 of this Appendix), it can be seen that many thousands of potential accident sequences involving hundreds of thousands of potential interactions were screened in this study to arrive at a relatively small number of potential CMF interactions. As will be shown in later Appendices (IV and V), further screening involving the identification of those particular sequences which were the dominant contributors to risk reduced the number of potential interactions of interest by additional very large factors.

In addition to the above, it should be noted that the containment trees discussed in sections 2.1.6 and 2.2 represent an extensive common mode failure investigation of the relationship between core melting and containment integrity. While it has long been known that a molten core would almost surely result in loss of containment integrity, this study has shown that there are widely different consequences having widely different probabilities for the various modes of containment failures.[1]

2.5 SUMMARY

It has been shown that the event trees used in this study were an essential component of the overall risk assessment methodology. Most of the event trees discussed in the preceeding paragraphs were developed for illustrative purposes and only to indicate the thought processes followed in event tree development. The initial requirement is definition of the functions to be performed after an initiating event (failure) and of the interrelationships between the various functions. Next, the systems provided to perform the functions are identified, and the interrelationships between the functions to be performed and the operability states of the systems are analyzed. Finally the interrelationships between the operability states of the various systems are defined. At each step, dependencies are considered and illogical or meaningless sequence combinations are eliminated. Thus the event tree can be regarded as a filter into which is fed all pertinent system information affecting the course of events following an initial failure and out of which come only logical and relevant functional and system relationships.

The trees are deceptively simple in appearance. Many interrelationships exist that are difficult to represent in a manageable two-dimensional tree. The trees must therefore be split into manageable parts such as a LOCA tree and a containment tree, and the sequences on them supplemented with descriptions to assure that all meaningful information about each sequence is used in a quantitative assessment of the trees.

In summary, the following points can be made about event trees as used in this study:

a. Event trees have provided the overall guidance needed to quantify the risks involved in nuclear power plant accidents because they are well suited for use in combining probabilities and consequences of accident sequences and to display the logic used.

---

[1] See Appendices V, VI, VII, and VIII.

b. They have assisted in identifying a spectrum of meaningful accident sequences to be quantitatively analyzed.

c. They have assisted in the definition of interrelationships among post accident functions, among these functions and the relevant ESF systems provided to perform the functions, and among ESF systems themselves.

d. Their use in eliminating illogical and meaningless relationships has helped to simplify the amount of analysis required. This has resulted in an efficient approach to the assessment of potential common mode failures by directing the search for common mode mechanisms only to those systems whose interrelationships are important to risk.

e. They have helped to define which physical processes affecting release and transport of radioactivity from fuel into containment and which modes of containment failure required analysis for completion of the quantitative risk assessment.

f. They have helped to define how ESFs can affect and be affected by the physical processes that can occur in various accident sequences.

g. They have helped in the utilization of fault tree techniques in the quantification of risk. Fault trees are difficult to use in defining system interrelationships; event trees help to indicate which systems required fault tree analysis, the conditions of failure, and the way individual system fault trees had to be combined for estimation of the probabilities of occurrence of applicable accident sequences.

h. They have helped to provide the consequence model (Appendix VI) with the fundamental inputs regarding the probabilities and magnitudes of radioactivity release from nuclear power plant accidents.

References

1. 36 Federal Register 12247.

2. Appendix A, Title 10, Code of Federal Regulations, Part 50, Criteria No. 35-36.

3. "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled Nuclear Power Reactors" December 28, 1973.

4. AEC General Design Criteria, Appendix A, Title 10, Code of Federal Regulations, Part 50, Criterion No. 2.

TABLE I 2-1 ESF FUNCTIONS TO ESF SYSTEM INTERRELATIONSHIPS

	RT	ECI	PARR	PAHR	ECR[(a)]
PWR LARGE LOCA >6" diam.		ACC and LPIS	CSIS or CSRS + SHA{CSIS or LPIS or HPIS}	CSRS and CHRS	LPRS {CSRS and CHRS}
PWR SMALL LOCA 2"-6" diam.break	RPS	ACC and HPIS	Same	Same	LPRS and HPRS {CSRS and CHRS}
PWR SMALL LOCA 1/2"-2" diam.break	Same	HPIS and AFW	Same	CSRS and CHRS {CSIS}	Same
BWR LARGE LOCA >6" diam.	RPS	CSIS or LPCIS	V.S. + SC and SBGTS {CI}	LPCRS and HPSWS	LPCRS {HPSWS}
BWR SMALL LOCA <6"	Same	HPCIS or ADS and CSIS or LPCIS	Same	Same	Same

(a) CI is omitted here, but will be discussed in section 2.2

or = Optional; success either way.

and = Both systems required for success.

+ = Adds improvement in function.

{ = System interdependencies that affect principal system operation.

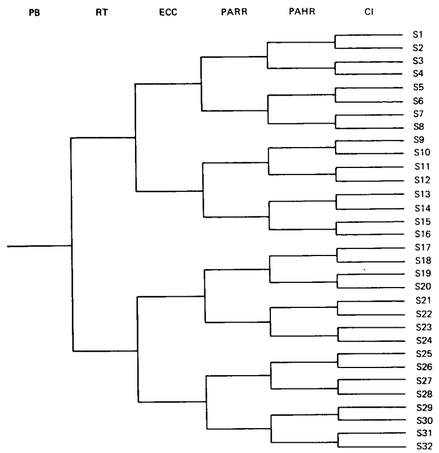


FIGURE I 2-1 Illustrative Event Tree for LOCA Functions

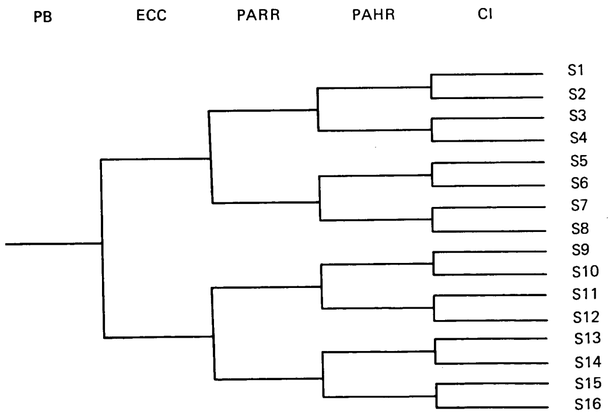


FIGURE I 2-2 Illustrative Event Tree for LOCA Functions with RT Omitted

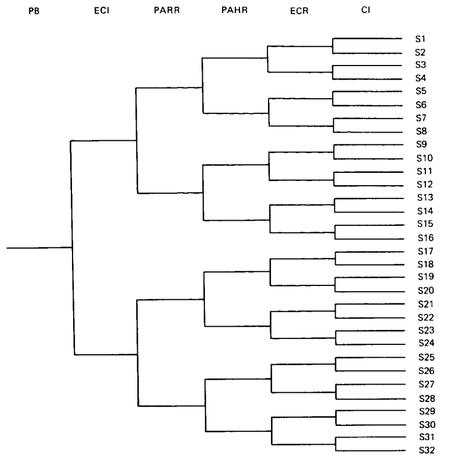


FIGURE I 2-3 Illustrative Event Tree with ECC Replaced by ECI and ECR

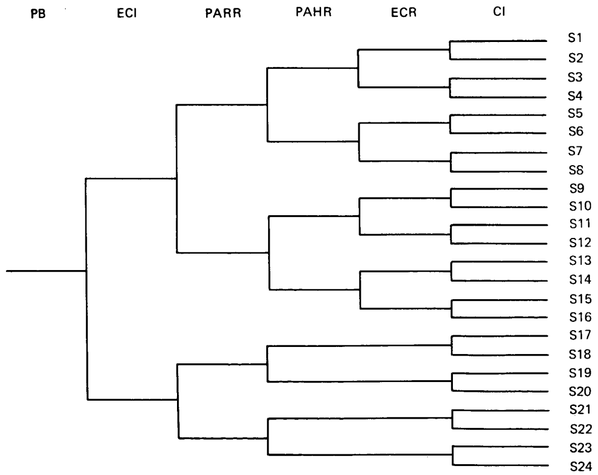


FIGURE I 2-4 Illustrative Event Tree Showing ECI-ECR Functional Interrelationship

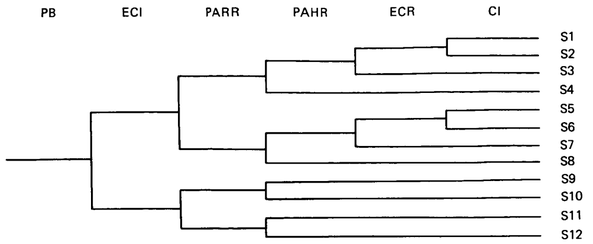


FIGURE I 2-5 LOCA Event Tree Showing Functional Interrelationships

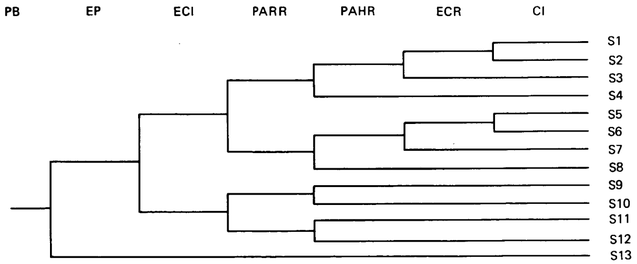


FIGURE I 2-6 Functional LOCA Event Tree Showing Interrelationships with Electric Power

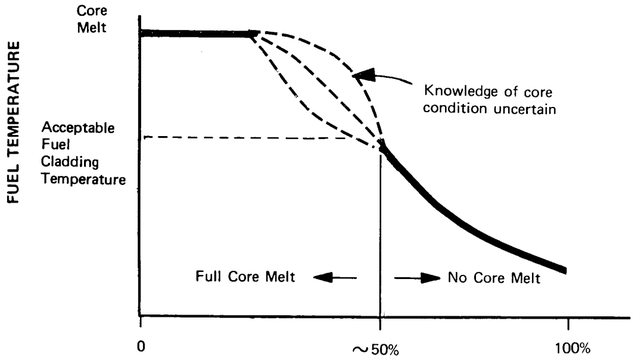


FIGURE I 2-7 Illustration of Conservative Approach used in Relationship Between ECC Functionability and ECCS Operability

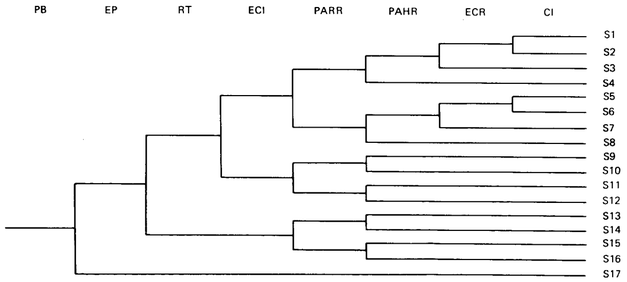


FIGURE I 2-8 Functional LOCA Event Tree Showing Interrelationships with RT

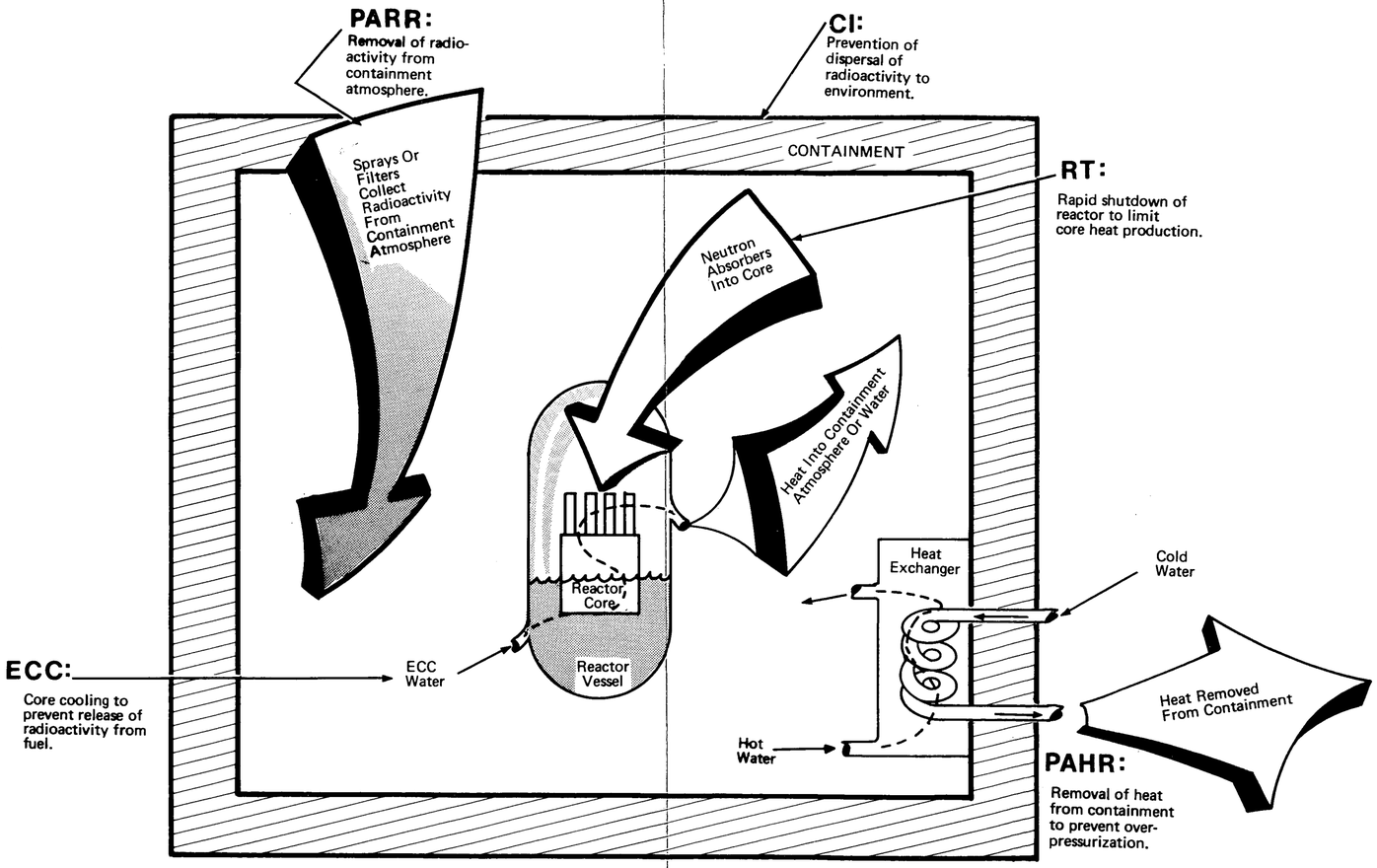


FIGURE I 2-9 Power Water Reactors Loss of Coolant Accident (LOCA) Engineered Safety system (ESF) Functions

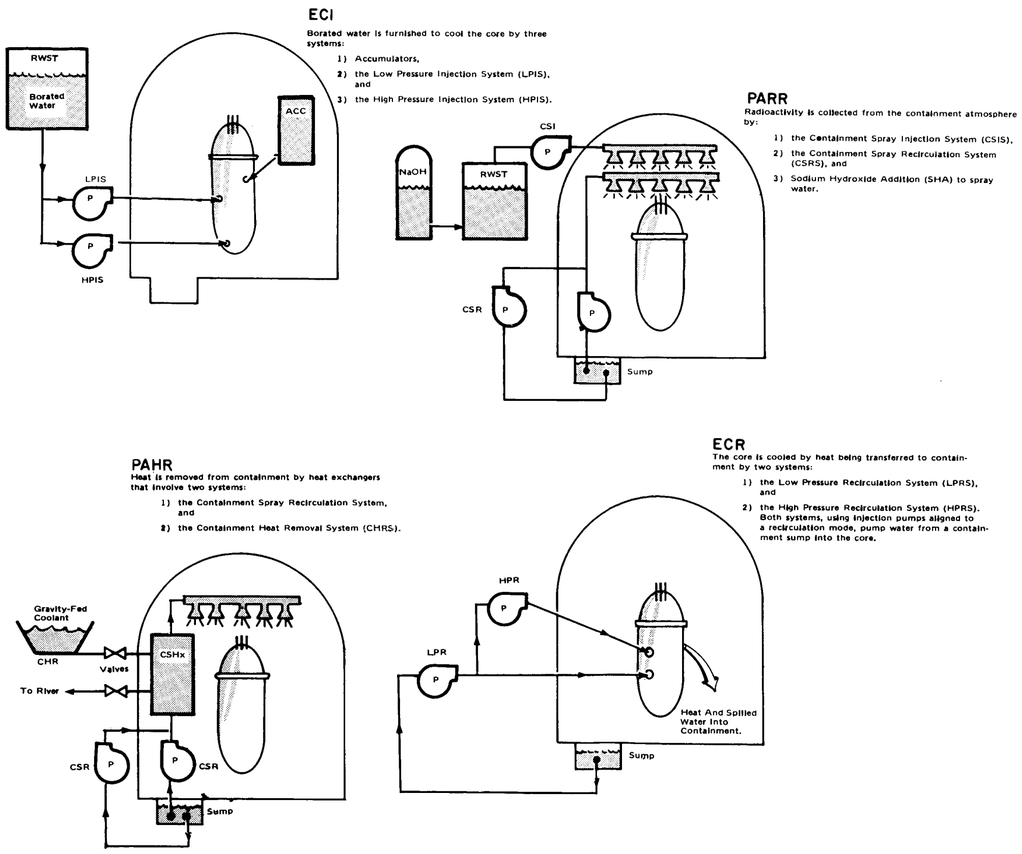


FIGURE I 2-10 Illustrations of PWR Systems Used to Perform ESF Functions

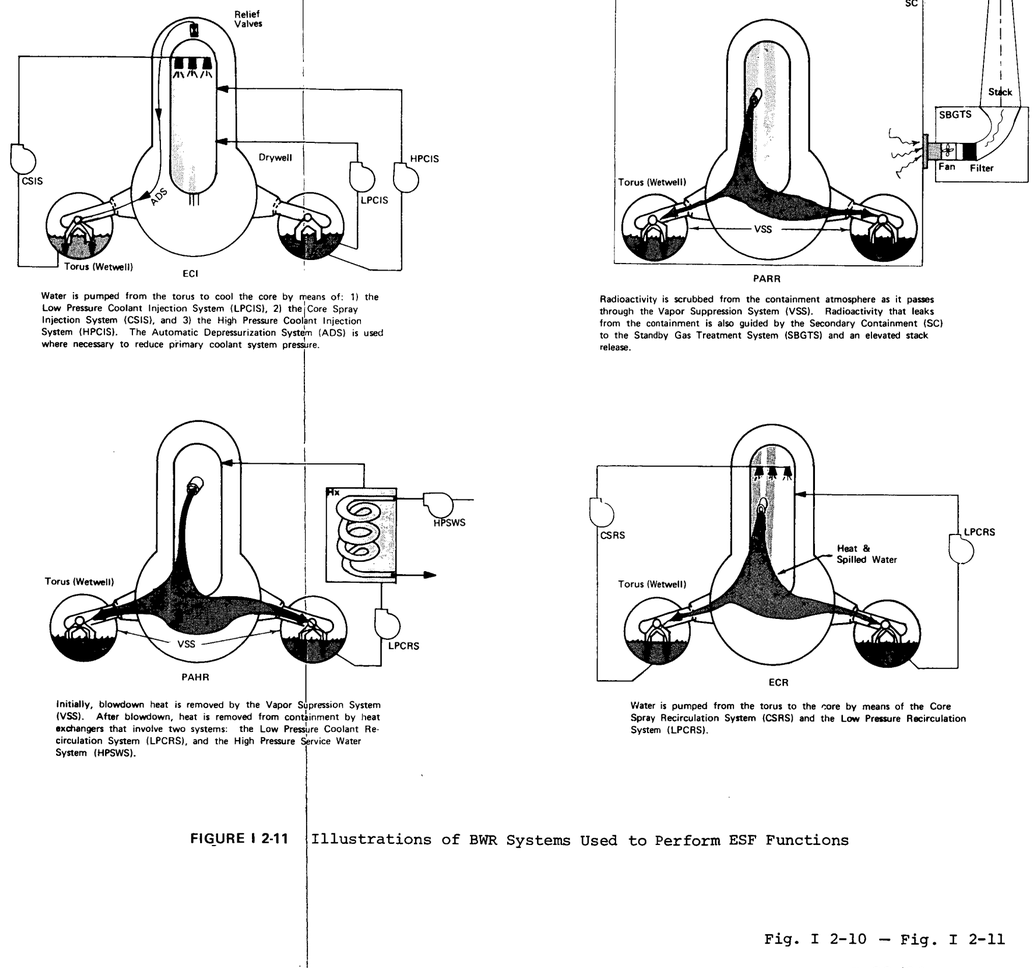


FIGURE I 2-11 Illustrations of BWR Systems Used to Perform ESF Functions

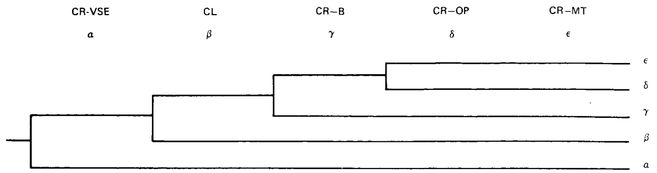
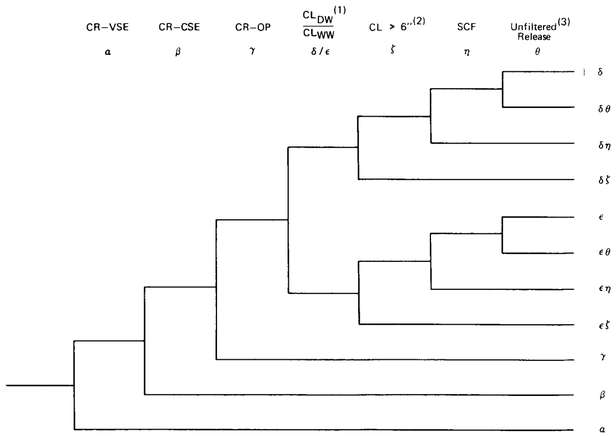


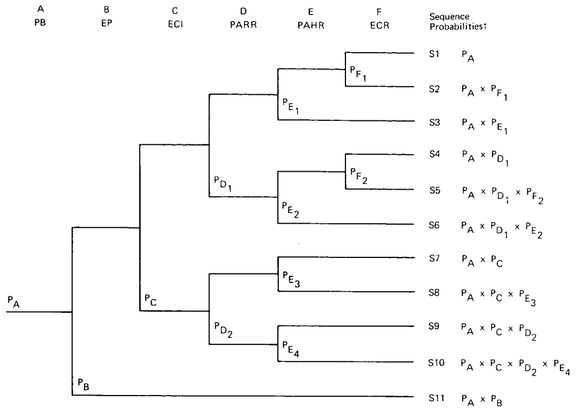
FIGURE I 2-12 PWR Containment Event Tree



NOTES:

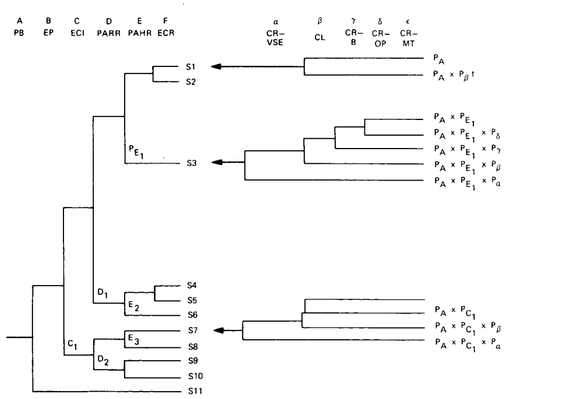
1. Upward path indicates containment leakage from the dry well (δ) downward path indicates leakage from the wet well (ϵ).
2. Leakage greater than a 6" equivalent diameter hole in the containment.
3. Elevated release which bypasses filters.

FIGURE I 2-13 BWR Containment Event Tree



†Precise computation of probabilities would include factors of the form (1-P) for all branches. Since the P values are very small numbers, these factors may be omitted.

FIGURE I 2-14 Illustration of Using the Event Tree to Show Functional Failure Probabilities



†Represents a spectrum of leakage rates that should not be interpreted in terms of the failure definition for CL on the Containment Event Tree.

FIGURE I 2-15 Linking of Accident and Containment Event Trees

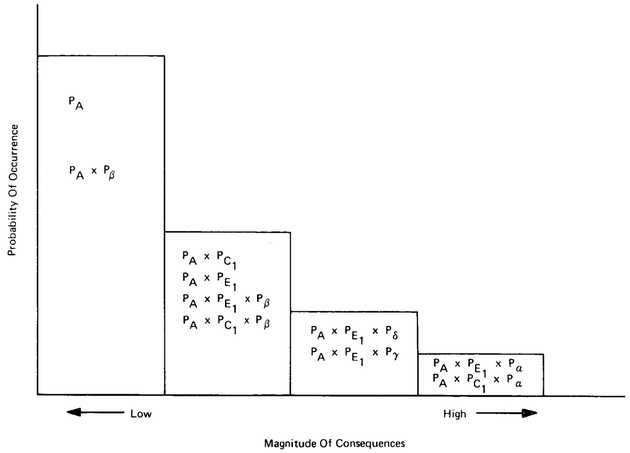


FIGURE I 2-16 Illustrative Association of Probabilities and Consequences

Section 3

Potential Accidents Covered by the Reactor Safety Study

To be sure that the risk assessment performed by this study would provide a true perspective of the magnitude of public risk from nuclear power plant accidents, it was necessary to identify those potential accidents that could cause the release of significant amounts of radioactivity to the environment. Thus, it was necessary first to identify the location and size of the sources of radioactivity in the plant and second to identify the possible ways that this radioactivity could be released. This covered initiating events or failures that could occur spontaneously within the plant and those that could potentially be caused by external forces such as earthquakes.

The rationale used to identify and sort out the accident events that were considered by the study is as follows:

a. The locations and sizes of sources of radioactivity in the plant are easily identified as indicated in Table I 3-1. The basis for the values given in the table are discussed below.

b. Table I 3-1 indicates that by far the largest inventory of radioactivity is in the core. Furthermore, the fuel in the core has a much larger heat generation rate even when shut down than the fuel in any of the other locations indicated in the table.

c. As will be seen later, the only way large consequence accidents can occur is by the release of large fractions of the core inventory.

d. For large fractions of the core inventory to be released, the fuel temperature must rise to high levels, or in essence, melt. There is only one way to melt fuel - an imbalance must exist between the heat generated in the fuel and the heat being removed from the fuel.

e. This heat imbalance, if it persists for even a relatively short time, can cause the fuel to overheat and release its radioactivity. The two ways to create this heat imbalance are as follows:[1]

   1. The occurrence of a loss of coolant event will allow the fuel to overheat due to its decay heat generation rate unless emergency cooling water is supplied to the core.

   2. Overheating of fuel can result from transient events which cause the reactor power to increase beyond the capacity of the reactor cooling system, or which cause the heat removal capacity of the reactor cooling system to drop below the core heat generation rate.

f. Thus the identification of potential accidents revolves about those failures which might cause heat imbalances in the fuel. Of course, the many such potential failures previously defined by the many years of safety analysis in the AEC and in the licensing process for commercial nuclear power plants served as a starting point for this effort in the Reactor Safety Study. However, in addition to starting with such previously defined initiating

---

[1] It should be noted here that it is also possible to overheat fuel during normal power operations due to some mechanical interference to flow of water to the core (commonly called flow blockage). While such events have occurred in test and experimental reactors and have led to localized fuel melting, they have not occurred in power water reactors. However, should such flow blockage occur during normal operations, it might be expected to cause some small amount of fuel melting in an intact reactor coolant system. Experience and investigations have indicated that such localized melting has not propagated among fuel elements and has not otherwise damaged the reactor coolant system. Thus, any release of radioactivity to the environment could be controlled to levels consistent with normal operations.

events, events not previously covered, such as reactor vessel failures, have also been considered. Further, the logical combinations of failures of systems which could mitigate the course of events following initial failures were also considered. In addition, searches were conducted for newly defined initiating events as well as events that could simultaneously violate more than one barrier to the release of radioactivity.

g. Those accidents for fuel not located in the reactor core (spent fuel storage pool, shipping cask, refueling) involve fuel which has a much lower heat generation rate than that in the core because of the longer decay times involved since termination of core operations and fewer fuel elements should be involved. This means that it is more difficult to overheat or melt this fuel. As will be shown later, the probability of releasing radioactivity from such fuel is quite low and the releases will be much smaller than core releases. Also, as will be shown later, the releases from the Waste Gas Storage Tanks and the Liquid Waste Storage Tanks have very small consequences. Correspondingly, the associated hardware or safety systems are less complex than those related to the core and thus the evaluations of accident sequences are simpler to perform. Section 5 treats these potential accidents.

The preceding discussion is intended to convey the sense of those factors that had to be considered in attempting to ensure that the study considered all accidents of significance. The identification of all significant sources of radioactivity, the requirement for fuel to melt to release significant amounts of radioactivity, knowledge of the factors that affect heat balances in the fuel and the fact that mechanisms leading to the creation of heat imbalances have been scrutinized for many years give a high degree of confidence that all accidents of significance have been identified in this study. This confidence also rests on the fact that thousands of accident sequences were considered and screened to identify those that were the dominant contributors to the risk. While a guarantee cannot be given that all accidents were in fact identified, the likelihood that a dominant contributor to the overall risk assessment was omitted is considered to be very small. Of course, should a new accident of some type be defined, it does not invalidate the work already done here; it can be analyzed and incorporated into the existing results.

A word should be said here about accidents due to external forces such as earthquakes, tornadoes and airplane crashes. The work in this appendix covers only those accidents that are caused by intrinsic failures within the plant itself. Appendix IX points out the design provisions used in nuclear power plants to make the likelihood of accidents initiated by external forces very small. Section 5 of the study's main report discusses the implications of external forces on accidents.

3.1 PRINCIPAL SOURCES AND AMOUNTS OF RADIOACTIVITY IN A NUCLEAR POWER PLANT

Table I 3-1 shows the inventory of significant radioactivity at a nuclear power plant site and the places where the radioactivity is located. It becomes immediately apparent that the radioactivity in the core dominates all other potential sources by a very large factor. The core radioactivity is largest because it contains the largest number of fuel elements that are subject to the shortest radioactive decay at the time the radioactivity can potentially be released.

During refueling, the fuel storage pool receives the one-third of the core that has the highest radioactive inventory at the time the reactor was shut down for refueling.[1] The storage pool cannot receive this fuel until about 72 hours after power operation has ceased. The larger radioactive inventory of this fuel adds relatively little radioactivity (about 20%) to the core average. However, the 72 hours of decay time prior to the commencing of refueling activities causes the fuel in the pool at the time refueling begins to have only about 16% compared to the core's total activity. Since the radioactivity in the fuel must be allowed to decay to the point that the fuel will not melt without cooling when shipped to a fuel reprocessing plant, a minimum storage period of approximately 150 days is involved. At this time, the percentage of radioactivity in the fuel

[1] For a two reactor plant, there could be another 1/3 of a core with about 150 day decay present in the pool.

assemblies within the spent fuel pool would be about 4%.

In the refueling process, only one spent fuel element is handled at a time. Although on the average these elements would have a higher inventory than the average fuel element in the core, they will have about 240 hours' decay time. This would give the average refueled bundle about 0.3% of the core inventory.

As indicated in the table, the inventory in the waste gas storage tank (WGST) is very small. This is due to the fact that the design basis of these tanks is such that if the tank were to rupture with its maximum inventory, the dose at the site boundary would be well below 10 CFR 100 guidelines. Also, as indicated, the inventory of the liquid waste storage tank (LWST) is also very small.

3.2 POTENTIAL ACCIDENTS LEADING TO THE RELEASE OF RADIOACTIVITY

The following sections will discuss the accidents which could potentially release radioactivity from the various locations at a nuclear power plant site. Section 4.0 will discuss accidents involving the core, with sections 4.1 and 4.2 discussing LOCA event trees and section 4.3 discussing the transient event trees. Section 5.0 will discuss accidents not involving the core and will make rough estimates of both the probability and amount of the release of radioactivity from each location.

TABLE I 3-1 TYPICAL RADIOACTIVITY INVENTORY OF LWRS

Location	Total Inventory (Curies)			Fraction of Core Inventory		
	Fuel	Gap	Total	Fuel	Gap	Total
Core[(a)]	8.0×10^{9}	1.4×10^{8}	8.1×10^{9}	9.8×10^{-1}	1.8×10^{-2}	1
Spent Fuel Storage Pool (Max.)[(b)]	1.3×10^{9}	1.3×10^{7}	1.3×10^{9}	1.6×10^{-1}	1.6×10^{-3}	1.6×10^{-1}
Spent Fuel Storage Pool (Av.)[(c)]	3.6×10^{8}	3.8×10^{6}	3.6×10^{8}	4.5×10^{-2}	4.8×10^{-4}	4.5×10^{-2}
Shipping Cask[(d)]	2.2×10^{7}	3.1×10^{5}	2.2×10^{7}	2.7×10^{-3}	3.8×10^{-5}	2.7×10^{-3}
Refueling[(e)]	2.2×10^{7}	2×10^{5}	2.2×10^{7}	2.7×10^{-3}	2.5×10^{-5}	2.7×10^{-3}
Waste Gas Storage Tank	--	--	9.3×10^{-4}	--	--	1.2×10^{-5}
Liquid Waste Storage Tank	--	--	9.5×10^{1}	--	--	1.2×10^{-8}

(a) Core inventory based on activity 1/2 hour after shutdown.

(b) Inventory of 2/3 core loading; 1/3 core with three day decay and 1/3 core with 150 day decay.

(c) Inventory of 1/2 core loading; 1/6 core with 150 day decay and 1/3 core with 60 day decay.

(d) Inventory based on 7 PWR or 17 BWR fuel assemblies with 150 day decay.

(e) Inventory for one fuel assembly with three day decay.

Section 4
Analysis of Potential Accidents Involving the Reactor Core

This section presents and discusses the event trees relating to loss of coolant accidents and transient events for the pressurized and boiling water reactors.

The loss of coolant accident is commonly thought of as being initiated by the break or rupture of a pipe in the reactor coolant system (RCS). Since this study is considering all possible significant LOCA initiating events, the loss of coolant accident has to be considered in a more general sense to include ruptures occurring anywhere in the RCS, including the reactor vessel. Analysis has shown that emergency core cooling systems provided in nuclear power plants have considerable capability to deal with ruptures in the reactor vessel depending upon their size and location (Ref. 1). Events such as these will, therefore, be considered equivalent to pipe breaks and incorporated into the loss of coolant accident event trees where pipe break is the initiating event. Breaks in the reactor vessel beyond the capability of the ECCS will be considered as a part of the group of reactor vessel ruptures that can be termed gross ruptures.

Section 2 of this appendix discussed some of the implications of RCS break size and location as they pertain to requirements for performance of the ECCS. In general, ECC systems are designed to cover two main categories of breaks in the RCS, large and small. The large break covers sizes that range from the equivalent of a six inch diameter hole size to the double-ended rupture of the largest pipe in the RCS. The small break size is further divided into two categories, that is, one-half to two inches and two to six inches equivalent diameter hole size. These distinctions reflect the differences in demand imposed by break size on the amount of the core cooling equipment that has to operate in order to provide core cooling. For example, as shown in Fig. I 4-1 for the PWR, smaller breaks in the small break category do not require accumulator action for adequate core cooling, whereas the larger end of the small break spectrum requires the operation of 2 out of 3 accumulators.

The transient events considered in this study are categorized into two groups, i.e., likely, or anticipated, transients, and unlikely, or unanticipated, transients. Event trees were developed for the anticipated transients since, as will be shown in later discussion, they are the events that are the major contributors to the risk assessment.

The event tree methodology discussed in section 2 of this appendix has been used herein to identify the accident sequences for both the loss of coolant accidents and the transient events. Figures I 4-2 and I 4-8 show the large LOCA event trees for PWR and BWR, respectively. These system event trees are discussed in sections 4.1.1 and 4.2.1 of this appendix. They were derived by substituting the ESF systems for each reactor, as listed in Table I 2-1, for the functional headings in the LOCA functional event tree, Fig. I 2-8. Small ruptures were treated similarly and are discussed in sections 4.1.2 and 4.1.3 for PWR and in sections 4.2.2 and 4.2.3 for BWR. Transient event trees are shown and discussed in sections 4.3, 4.3.1, and 4.3.2.

4.1 PWR LOSS OF COOLANT ACCIDENTS

Reactor coolant system (RCS) ruptures which result in loss of coolant accidents can be categorized as a function of rupture location. RCS ruptures inside the containment barrier are distinguished from ruptures that occur into systems that interface with the RCS and penetrate the containment. One rupture of the latter type has the potential for the release of large amounts of radioactivity directly to the environment. Further, two types of ruptures into the containment are recognized, according to whether the rupture occurs into the reactor cavity or outside of the reactor cavity. This distinction arises from the potential lack of availability of water supply from the containment sump to the containment recirculation spray system for the case of a small break occurring inside the reactor cavity.

Evaluation has shown that the significant loss of coolant accidents can be covered by six accident categories, and these are treated in the following subsections:

4.1.1 PWR Large LOCA Event Tree

4.1.2 PWR Small LOCA Event Tree - S1

4.1.3 PWR Small LOCA Event Tree - S2

4.1.4 PWR Reactor Vessel Rupture

4.1.5 PWR Steam Generator Ruptures

4.1.6 PWR RCS Ruptures Into Interfacing Systems

The three subsections 4.1.1, 4.1.2, and 4.1.3 treat the PWR LOCAs. Factors affecting this category include break size and break location with respect to the RCS main circulating water pumps, pressurizer, and steam generator.

As noted in section 4 and shown in Fig. I 4-1, break size considerations relate to the required delivery capabilities of the ECCS. The break size ranges shown in the figure not only require different safety systems to mitigate the incidents but also lead to different functional relationships among the systems. For example, the containment spray recirculation system (CSRS) is assumed to require successful operation of the containment spray injection system (CSIS) for break sizes in the smallest range (less than 2 inches diameter) because of the potential of starting and damaging (by dry operation) the recirculating pumps before the liquid from the break reaches the sump. For larger breaks, the RCS depressurizes faster, and liquid from the break is calculated to reach the sump before CSRS starts even if CSIS fails. These relationships are described further in the discussions of the individual trees.

Section 4.1.4 treats ruptures of the reactor vessels. As indicated earlier, this section will cover only those reactor vessel ruptures that are beyond the capability of ECC systems.

Section 4.1.5 treats large ruptures of a PWR steam generator and includes those ruptures which could be of such potential severity as to result in a LOCA.

Section 4.1.6 treats PWR RCS ruptures into interfacing systems that could potentially result in a significant amount of radioactivity bypassing the containment barrier and the containment ESFs.

4.1.1 PWR LARGE LOCA EVENT TREE

The PWR large LOCA event tree, Fig. I 4-2, shows the potential sequences that could result from a large area break of the RCS. Definitions of headings on the event tree are presented in detail following the discussion on the development of the tree.

4.1.1.1 PWR Large LOCA Event Tree Development.

The development of the PWR large LOCA event tree and some of the functional logic underlying the selection of column headings presented on the event trees are discussed below.

The initiating events, the first column heading, are either a random rupture in the reactor coolant system, ranging in size from the equivalent of about a 6-inch diameter hole up to the double ended rupture of the largest pipe in the system, or those failures in the reactor pressure vessel which do not exceed the capability of the ECC systems to cool the core.

The availability of electric power is considered after the initiating event (as is the case described for the functional tree in Fig. I 2-8) so as to determine if ESFs can be operated.

The next column to convert from Fig. I 2-8 to the PWR large LOCA event tree (Fig. I 4-2) is the emergency coolant injection (ECI). It should be noted that the containment spray injection system (CSIS) was originally placed on the large LOCA event tree before ECI due to possible dependencies between the ECI systems and the CSIS which decreases containment pressure. Although later analysis revealed no important dependencies, CSIS was not moved from this location.

From Table I 2-1 it can be seen that the PWR systems needed for the ECI function are the accumulators and the low pressure injection system (LPIS). To simplify the event tree, these systems are combined as ECI. The definitions of the other headings that follow show how the systems are combined.

Immediately following the ECI, a column labeled emergency cooling functionability (ECF) is shown. This column was included to account for the possibility that ECCS does not properly cool the core even though the systems operate as designed. Additional discussion of the emergency cooling functionability (ECF) column and its relative importance to

the overall core melt probability is presented in section 4 of Appendix V.

The next heading of Fig. I 2-8 is post accident radioactivity removal (PARR) and, as shown in Table I 4-1, the appropriate PWR systems are CSIS, the containment spray recirculation system (CSRS) and the sodium hydroxide addition (SHA). The CSIS system is shown earlier on the event tree as discussed above. The CSRS is shown next on the tree but SHA is held until last because its influence in enhancing iodine removal is significant only when either CSIS or CSRS operates during the period of radioactivity release from the RCS.

The next heading on Fig. I 2-8 is the post accident heat removal (PAHR) which involves both the CSRS and the containment heat removal system (CHRS). The CHRS success or failure choice is valid only for sequences in which CSRS is successful. This is so because the heat exchangers in the CHRS are coupled with the CSRS and depend on its operation. For sequences where CSRS is not successful, no CHRS choice is shown.

The final heading on Fig. I 2-8 is emergency coolant recirculation (ECR). As discussed earlier in section 2.1, no ECR success choice is shown when ECI has failed since core melt is underway before ECR is established. The ECR function is achieved by the low pressure recirculation system (LPRS) which also depends on the CSRS and CHRS for its continued successful operation. Therefore, a success choice for LPRS is shown on the event tree only for those cases where both CSRS and CHRS are successful. Finally, as described above, SHA is included on the event tree for sequences where its iodine removal influence could be significant.

4.1.1.2 Event Tree System Interrelationships.

Several illogical paths on the functional event trees of section 2 were eliminated based on functional interrelationships and functional-operability relationships. Likewise, the PWR large LOCA event tree in Fig. I 4-2 illustrates that a number of illogical paths have been eliminated based on various system to system interrelationships as well as the system relationships to preceeded functions. See Table I 4-1 for the delineation of the logic for the accident sequences. Table I 4-1 also illustrates the relationships of the large LOCA event tree to the containment event tree developed in section 2 of this appendix.

Sequences 5a, 6a, 7a, 8a, 25a, 26a, and 27a show no option for the operability of LPRS. These choices were eliminated because earlier failure in either containment spray recirculation system (CSRS) or in the containment heat removal system (CHRS) precludes continued success of the low pressure recirculation system (LPRS). This relationship exists because loss of either CSRS or CHRS would likely pressurize the containment until failure occurs. The resultant depressurization of the containment from very high pressure and temperature conditions will reduce the net positive suction heat available to the LPRS pumps and cause them to cavitate and fail. Thus, no choice is shown for LPRS for these sequences.

The b sequences in 5, 6, 7, 8, 25, 26, and 27 differ from the a sequences in the order in which failures occur. For example, in sequence 6b, the sequence AHGI indicates that the system in column G initially operates, then the system in column H fails. This failure is accompanied by or followed by failure of the system in column G. No operability choice for LPRS exists for these sequences either.

For sequences 9-20 and 28-37 the core is assumed to have melted because of a failure to cool the core during the injection phase and therefore no choice on the operability of the LPRS is shown because it cannot significantly change the consequences.

Because the PWR heat exchange function requires operability of both the CSRS and CHRS for success, operation of the CHRS cannot succeed in sequences 7, 8, 13, 14, 19, 20, 27, 32, and 37, where CSRS is shown failed. Thus, no choice is shown for CHRS for these sequences. Similarly, the ECF choice is not shown when ECI has failed as in sequences 15-20 and 33-37.

Sequences 27, 32, and 37 show cases where neither CSIS or CSRS is operable; for these cases no choice is shown for SHA since the sodium hydroxide must be sprayed through the containment atmosphere to affect the reduction of radioactivity.

When electric power is failed (sequence 38), no choice is shown for the other ESFs since electric power is required to permit their operation.

The status of particular systems is further addressed in Table I 4-1.

4.1.1.3 Definitions of Events for the Large LOCA Event Tree.

4.1.1.3.1 Event A - Large Break in the Reactor Coolant System: Large LOCA. The initiating event is a random rupture in the RCS that creates a break area equivalent to that resulting from about a 6-in. diameter rupture and ranging up to the area of a double-ended rupture of the largest primary pipe and causes the depressurization of the RCS. Ruptures of the reactor vessel that place no more stringent demands on the safeguards than a double-ended cold-leg break are included as well as pipe ruptures (etc.) that discharge coolant to the containment.

4.1.1.3.2 Event B - Electric Power: EP. Because operability of the ESFs depend on the availability of electric power, the event tree is structured to show the unavailability of electric power (EP) as the first event of interest after the initiating event. EP addresses the availability of AC power to the buses that furnish power to the ESFs. The off-site AC network and on-site AC diesel generators together with DC control systems comprise the principal components of the electric power system.

EP failure is defined as failure to provide sufficient AC and DC power for the operation of the engineered safety features required to mitigate the initiating event. The probability of failure of the AC or DC power systems, either total or partial failures, including the respective bus pairs required for operation of particular ESFs are accounted for in the PWR fault trees presented in Appendix II.

The structure of the event tree for subsequent events reflects the dependence of other ESFs on electric power. Thus, when electric power fails, further choices are omitted so as to imply failure. As noted above, other types of electric failures, such as those affecting individual components, are treated in individual system fault tree analysis. The electrical system and the other systems discussed below are more fully described in Appendix II.

4.1.1.3.3 Event C - Containment Spray Injection System: CSIS. The containment spray injection system (CSIS) delivers spray to the containment to remove radioactivity from the containment atmosphere during the first half hour after the RCS break.[1] Also, the spray helps to reduce the containment building pressure, and thereby helps to reduce leakage of radioactivity from the containment to the outside environment. Finally, the containment spray injection fluid provides one of the means for delivering sodium hydroxide to the containment building (see Event I). The CSIS consists of redundant spray headers and pumps that deliver water from the refueling water storage tank (RWST). Failure of the CSIS system is considered to be failure to deliver borated water from the refueling water storage tank to the containment atmosphere at a rate at least equivalent to the full delivery from one of two containment spray pumps.

4.1.1.3.4 Event D - Emergency Coolant Injection: ECI. ECI is a group of three subsystems that operate in different combinations to provide emergency coolant to prevent core damage for various break sizes. For a large break area rupture of the RCS, two of the three systems are required to operate: namely, the accumulators (ACC) and the low pressure injection system (LPIS). The accumulators discharge stored borated water into the RCS cold legs when the RCS depressurization causes a reversal of the pressure drop across check valves in the accumulator pipes. The LPIS injects borated water from the RWST into the RCS cold legs by using redundant, electrically driven pumps.

ECI failure is 1) delivery of less borated water than would result from the discharge of two accumulators into the RCS cold legs immediately following a large pipe break, or 2) delivery of borated water at a flow rate less than the design output of one low head safety injection pump to the RCS cold legs (starting at about thirty seconds following a large pipe break and lasting 1/2 hour). This period of emergency coolant water delivery is termed the injection phase of delivery.

4.1.1.3.5 Event E - Emergency Cooling Functionability: ECF. Emergency cooling functionability (ECF) relates to the probability of failing to cool the core even though the ECI operates successful-

---

[1] Duration of the CSIS operation varies depending on the number of CSIS pumps and LPIS pumps that operate since they all draw water from the same storage tank.

ly. Although the Reactor Safety Study has accepted the recent AEC rules for predicting the response to such accidents as being suitably conservative to ensure adequate cooling, it is also recognized that the criteria were not meant to encompass all postulated elements that might influence ECI (Ref. 2).

Several possibilities exist for failure of the emergency core cooling system to reflood and cool the core even though emergency coolant is delivered to the primary system cold legs. Included are steam binding due to excessive leakage from secondary system to primary system, failure of core supporting structures resulting in an undefined coolant flow path within the vessel, and an uncoolable core geometry as a result of blowdown loads and subsequent thermal distortion of the core.

4.1.1.3.6 Event F - Containment Spray Recirculation System: CSRS. CSRS provides for recirculation of sump water through heat exchangers to spray headers inside the containment for the purposes of pressure control and removal of radioactivity and heat from the containment. The system is comprised of four trains, each of which contains a separate pump, spray header, and heat exchanger.

CSRS failure is considered to be a flow rate less than the equivalent of the normal output of two recirculation spray pumps for the first twenty-four hours or the normal output of one recirculation spray pump thereafter.

4.1.1.3.7 Event G - Containment Heat Removal System: CHRS. The containment heat removal system (CHRS) provides heat removal from the containment by passing service water through heat exchangers in the CSRS system. There are four heat exchangers in the plant, one for each of the CSRS trains; to successfully remove heat, service water must flow through a heat exchanger located in an operating train of the CSRS. CHRS failure is operation of less than two of the four containment spray heat exchangers during the first 24 hours and operation of less than one of the four heat exchangers thereafter.

4.1.1.3.8 Event H - Low Pressure Recirculation System: LPRS. When ECI has succeeded, the continuity of emergency core cooling is provided by the recirculation mode of the low pressure injection system (LPIS), which is realigned to take coolant from the containment sump rather than from the refueling water storage tank (RWST). In this mode of operation, the LPIS is redesignated to be the LPRS. Alignment into this recirculation mode occurs approximately one-half hour after the LOCA when the RWST approaches depletion and requires human actions from the control room to switch the valve arrangements for the low pressure system.

The initial alignment for recirculation is for the low pressure pump to deliver into the RCS cold legs only. Unlike the injection phase, however, the inadvertent delivery into the RCS hot legs is not considered as failure. Further, within about one day after the large LOCA initiated by a break in the RCS cold leg piping, the LPRS should be aligned to deliver into the RCS hot leg piping to help avoid potential accumulations of residue or debris in the reactor vessel which may result from continuous boiling.

Failure of the LPRS is defined as failure to inject into the RCS from at least one low-pressure pump. Failure to realign to hot leg delivery (or failure to achieve coolant delivery, in part, through the hot legs with the continuance of delivery into cold legs) is also considered LPRS failure.

4.1.1.3.9 Event I - Sodium Hydroxide Addition: SHA. Sodium hydroxide is added, from a separate storage tank, into the RWST, from which the containment spray injection and emergency core cooling injection systems take their water after the LOCA. Addition of the sodium hydroxide is accomplished by gravity flow into the RWST upon automatic opening of valves that separate the two tanks. Actuation of these valves occurs following the LOCA when sensors in the consequence limiting control system (CLCS) signal the existence of high pressure in the containment. Sodium hydroxide addition (SHA) provides a basic solution that assists in the reduction of radioactivity from the containment atmosphere when added to the water sprayed by the containment spray systems; CSIS and CSRS.

Sodium hydroxide that is delivered to the RWST should go directly to the containment atmosphere. If it does not, because of CSIS unavailability, it would eventually reach the containment sump if water is being delivered to the RCS by any of the emergency core cooling injection subsystems. From there it could be sprayed into the containment atmosphere by operation of CSRS. Failure of SHA is

defined as the failure to introduce sodium hydroxide into the RWST.

4.1.1.4 Discussion of Event Tree System Status and Containment Failure Modes.

As noted in section 2 of this appendix, the event tree shown in Fig. I 4-2 illustrates the functionability and operability interrelationships which exist between the various systems provided to either 1) prevent or limit core damage, or 2) reduce off site exposure. To aid in understanding the interrelationships involved, a chart providing a sequence-by-sequence description of the event tree is presented in Table I 4-1. This chart summarizes the results of individual sequences from the PWR large LOCA event tree as to whether or not the sequences result in core melt. Also the chart links the sequences with the Containment Event Tree developed in section 2 of this appendix and identifies the possible modes of containment vessel failure considered for each sequence.

To provide additional assistance in understanding the accident sequences, Table I 4-2 presents a listing of the time phasing of certain important physical events occurring in each sequence with estimates of the containment pressure at these times.

4.1.2 PWR SMALL LOCA EVENT TREE - S1

As indicated in section 4, one category of small breaks pertains to a break area of about 2 to 6 inches equivalent diameter. The event tree shown in Fig. I 4-3 illustrates the systems used to mitigate this accident and the possible sequences following this initiating event. This tree results from the substitution of the appropriate ESFs shown in Table I 2-1 into the functional event tree shown in Fig. I 4-3. This size rupture requires a different combination of ESFs to mitigate the incident. Column headings for this event tree are discussed below. Table I 4-3 presents the system status and containment failure modes for this event tree.

DEFINITIONS

S1 - Initiating Event

The initiating event is a random rupture of the RCS boundary during normal full power operation. This creates a break size ranging from ~2 inch to ~6 inches equivalent diameter through which loss of coolant occurs. The rupture is assumed to occur spontaneously in either the liquid or steam space regions of the reactor coolant (RCS) above the core. This event requires emergency makeup water to be delivered by the accumulators and by the high pressure coolant injection system (HPIS) to arrest the fuel-clad temperature rise and to mitigate accident consequences. Within about 30 minutes or more, the event requires recirculation of the emergency cooling water by means of the emergency core cooling high and low pressure pumping systems. Recirculation is required for an extended period of time (on the order of four months).

B - Electric Power: EP

Electric power failure is defined as insufficient AC and DC power to the emergency buses to operate the minimum engineered safety feature subsystems as defined herein. Specifically, this failure is taken to mean loss of power to certain pairs of emergency buses as described in the definitions for the large LOCA tree.

K - Reactor Protection Systems: RPS

Failure of the reactor protection system (RPS) is conservatively defined to be the failure of more than two full-length control rod assemblies to insert into the core within approximately 30 seconds after the initiating event (small LOCA). The failure of the required control rod assemblies to insert may be caused by electrical faults in the signals or equipment required to release the rods into the core, or by mechanical faults that cause a hangup of more than two full-length control rod assemblies.

C - Containment Spray Injection System; CSIS

Same as large LOCA.

D - Emergency Coolant Injection: ECI[1]

As illustrated by Fig. I 4-1, the ECI definition has a break-size dependency. Failure of ECI for a break size between ~2 and 6 inches in diameter is defined as less than two of three accumulators delivering borated water to the reactor

[1]The ECF column heading has been eliminated from the small LOCA event trees for the reasons discussed in section 4 of Appendix V.

vessel or less than one of three HPIS pumps delivering borated water from the RWST. This definition is applicable only to the three loop PWR design under consideration.

When a small LOCA is caused by a break between ~2" and 6" in diameter in the RCS vapor space (pressurizer), the requisite pressurizer low level signals for automatic initiation of the high pressure injection system (HPIS) may not be obtained.[1]

Actuation of ECI either manually or ultimately by high containment pressure may have to be relied upon in this situation. Vendor analyses of these pressurizer vapor space breaks have, however, indicated that a delay of about 50 minutes could be tolerated in the HPIS provided that 2 of 3 accumulators deliver coolant into the RCS.[2]

When the small LOCA is caused by breaks between ~2" and 6" in diameter in the RCS liquid region above the reactor core, the delivery from less than 1 of 3 accumulators is considered failure of ECI.

F - Containment Spray Recirculation System: CSRS

As in the large pipe break LOCA, failure of CSRS constitutes delivery of recirculation spray water through spray nozzles at less than the equivalent of the output of 2 of 4 recirculation spray pumps for about the first twenty-four hours after the incident or less than the equivalent of the output of one recirculation spray pump thereafter. Note that for a break of ~2 to 6 inches diameter outside the reactor vessel cavity, CSRS does not depend on the previous operation of the containment spray injection system (CSIS) to build up sufficient inventory in the sump.

G - Containment Heat Removal System: CHRS

Failure of CHRS constitutes delivery of service water to less than two of the four heat exchangers during the first 24 hours; thereafter only one is required.

H - Emergency Coolant Recirculation: ECR

Failure of ECR is defined as failure to deliver water from the containment sump to the reactor cold legs by at least one high head pump taking suction from the discharge from one low head pump. ECR failure is also considered to be failure to switch to hot leg injection at about 1 day after the initiating event occurs.

I - Sodium Hydroxide Addition: SHA

Same as for large LOCA.

4.1.3 PWR SMALL LOCA EVENT TREE - S2

As indicated in section 4, the second category of small breaks pertains to a break area of about 1/2 to 2 inches in diameter. The event tree shown in Fig. I 4-4 illustrates the systems used to mitigate this incident and the possible sequences following this initiating event. This tree results from substitution of the appropriate ESF's shown in Table I 2-1 into the functional event tree shown in Fig. I 2-8. The event tree is applicable to any break location in the RCS that discharges the primary coolant to the containment atmosphere. For breaks in this range, the use of auxiliary feedwater (AFWS) is assumed to be required for approximately one-half day to augment heat removal from the RCS and thereby control the RCS pressure. Column headings for the event tree are discussed below. Table I 4-4 presents the system status and containment failure modes for this event tree.

DEFINITIONS

S2 - Initiating Event

The initiating event is a random rupture in the RCS boundary during normal full-power operation. This creates a break area ranging from 1/2 to 2 inches in diameter through which loss of coolant occurs. The rupture could occur in either the liquid or vapor-space regions of the RCS, above or below the core. This event requires ECC injection via the high pressure coolant injection system (HPIS).

B - Electric Power - EP

Electric power considerations are the same as on the large LOCA event tree in section 4.1.1, except that evaluation of the fault trees requires consideration of electric power distribution to both

---

[1] For example, when pressurizer safety valves inadvertently open and discharge to the pressurizer quench tank.

[2] These modes of actuation are accounted for in the fault tree evaluation model for the small LOCA ECCS. Refer to Appendix II.

the high pressure coolant injection system and the auxiliary feedwater system (AFWS) as well as the other ESFs previously considered. These considerations are necessary for completeness but were not found to significantly affect the probability of electric power availability to the appropriate ESFs following a specific LOCA.

K - Reactor Protection System - RPS

Same as for S1 described previously.

L - Secondary Steam Relief and Auxiliary Feedwater - SSR & AFWS

To augment heat removal from the RCS, heat from the primary system is transferred to water in the steam generators which is provided by the auxiliary feedwater system, and the resultant steam is discharged to the outside atmosphere via two of three power-operated relief valves or two of fifteen mechanical safety valves.[1] Auxiliary feedwater delivery failure is considered to be less than full delivery from one of two half-size electric-driven feedwater pumps or the equivalent flow from the full-size steam-driven auxiliary feedwater pump. The period of demand and operation for the SSR and AFWS are about 1/2 day for the small LOCA event.

C - Containment Spray Injection System - CSIS

This is the same as the large LOCA except that automatic initiation via the consequence limiting control system (CLCS) cannot be expected for about 30 minutes following the incident because of the slow rise in containment pressure. This allows for a somewhat higher probability of operator-initiated CSIS, which is considered desirable as CSRS requires success of CSIS as discussed below.

D - Emergency Coolant Injection - ECI

ECI failure is less than the equivalent in delivery of one of three high head injection pumps. Accumulators are not required.

F - Containment Spray Recirculation System - CSRS

This is the same as the large LOCA with the period of operation dependent on how CLCS is initiated, as discussed for CSIS above. CSRS can depend on water delivered by CSIS to the containment sump for its supply and is assumed to fail if CSIS fails.

G - Containment Heat Removal System - CHRS

This is the same as the large LOCA.

H - Emergency Coolant Recirculation - ECR

This is the same as the small LOCA S1 except that the switchover to hot leg injection is not required because the core is not uncovered during the incident if ECI is successful.

I - Sodium Hydroxide Addition - SHA

This is the same as the large LOCA.

4.1.4 PWR REACTOR VESSEL RUPTURE

For the purposes of this study, it was convenient to class vessel rupture into two categories which can have different consequences:

a. Potential ruptures in the vessel were considered that could be of such size and location that they are essentially equivalent to pipe breaks and thus ECI and ECR would be expected to cool the core.[1] If the rupture is of such size as to be within pipe break size limits equivalent to about the double-ended break of the largest RCS pipe (~10 ft.^{2}) and if it were to be generally located above the core region, then ECCS should be able to cool the core as well as if the break were in the pipe. Breaks such as these are covered by the previously presented LOCA trees. Since it is expected that the likelihood of vessel rup-

[1] A unique feature for steam relief exists for this PWR to permit atmospheric steam relief after about 1/2 hour. This feature includes a decay heat release control valve, operated from the main control room, and a line that discharges to the atmosphere from the residual heat release header. Operator usage of this feature at periods greater than about 30 minutes could augment or back up the secondary steam relief capability defined above. This feature has not been included in the above definition because its inclusion would not be expected to change the overall availability of SSR and AFWS because of the dominance of the AFWS contribution.

[1] See previous LOCA sections 4.1.1, 4.1.2, and 4.1.3 for ECI and ECR definitions.

tures of this size would be far smaller than that of pipe ruptures, this would not represent a significant contribution to the study's risk assessment.

b. Potentially large ruptures in the vessel were considered that could prevent effective cooling of the core by ECCS. Since certain of these ruptures appeared to be capable of causing missiles (such as the reactor vessel head) with sufficient momentum to rupture the containment, this area was examined with some care. The presence of a polar crane weighing 200 tons was determined to be a sufficient obstruction to prevent even a very large missile from penetrating the top of the containment. Thus it is, in general, expected that this type of vessel rupture would cause a core melt inside an intact containment.

However, because of the physical plant layout, there is some small probability that a large vessel missile could in fact impact directly on the containment and penetrate through the wall. This type of rupture could involve a core meltdown in a non-intact containment.

In these cases, the reactor vessel rupture leads directly to core melting and the only ESFs of interest are those which remove radioactivity and decay heat from the containment atmosphere. This can be seen in the event tree shown in Fig. I 4-5.

4.1.5 PWR STEAM GENERATOR RUPTURES

Consideration was also given to the consequences that would follow from ruptures in either the primary or secondary side of one steam generator. Some 30 possible accident sequences were identified using event trees, but the end result is either a rapid cooldown transient or a LOCA.

Transients are more comprehensively discussed in section 4.3.1, but it should be noted here that steam generator induced transients do not lead to core melt but could cause release of gaseous radioactivity into the RCS from the fuel-clad gap. In magnitude this result is roughly comparable to a transient induced by the inadvertent full-opening of the turbine bypass valves to the condenser but is less likely.[1] Hence the steam generator rupture is not an important factor in the risks due to transient events.

With respect to a LOCA induced by a steam generator rupture, those sequences which could potentially involve a significant release of radioactivity must damage the RCS. The distinguishing feature of a LOCA induced by steam generator failure is the addition of the energy in the affected generator to that of the RCS in blowing down to the containment. This incremental energy would have a small effect on the containment pressure, but otherwise the situation would be much like other LOCAs. It should also be noted that even a severe rupture of the steam generator would result in a LOCA no larger than the equivalent of a double-ended break. Further, the probability of a severe rupture is low, of the order of failure of the reactor pressure vessel, which is much less than the failure probability of piping. Thus, the rupture of a PWR steam generator does not contribute importantly as a LOCA path.

4.1.6 PWR RCS RUPTURE INTO INTERFACING SYSTEMS

Part of this study of the LOCAs included the investigation of a number of piping systems that connect to the reactor coolant system and also go through the containment. Such connections have the potential to cause a LOCA in which the interior of the reactor vessel may communicate to the environment. All, except the LPIS check valve situation discussed below, were dismissed for any or a combination of the following reasons:

a. The multiplicity of barriers that would be required to fail would render the LOCA much less probable than the check valves.

b. Failure of the barriers would not involve loss of vital safeguards and the loss of RCS coolant could be accommodated within the design of the interfacing systems through safety and relief provisions, and the coolant loss could be controlled or contained without a core melt occurring.

---

[1] Table I 4-10, section 4.3.1, PWR Transients, in this Appendix.

c. Failure of the barriers would involve a LOCA into the containment and would, therefore, be covered by previous LOCA event trees.

During the course of this study, a potential deficiency was identified in the design of a portion of the emergency core cooling system (ECCS) which uses double (in-series) check valves as barriers between the low pressure injection system (LPIS) which is outside the containment and the high pressure RCS which is inside the containment. Figure I 4-6 shows the configuration of interest. Common failure of these double barriers could result in a LOCA that suddenly discharges into the LPIS system and bypasses the containment. The LPIS system, with its low design pressure, could fail due to overpressure or dynamic loadings beyond its design, thus resulting in core melting. In this situation, containment ESFs would be of no interest since the release of radioactivity would largely bypass the containment system.

The check valves, when functioning as a double barrier between the interfacing systems, make the probability of LOCA due to rupture of both barriers small. In this specific design, however, no test provisions or procedures were found to exist which would assure availability of double barriers for plant operation. LPIS pumps and lines are required to be flow tested at least yearly to ensure that passage of coolant to the RCS occurs. These tests do not, however, ensure that the check valves reseat or that both check valves would be effective as barriers. It is possible therefore that one check valve could be stuck open and only one barrier would indeed be effective during plant operation. This possibility was considered[1] and the probability of failure of the LPIS check valves leading to an uncontrolled RCS LOCA was estimated to be about 4×10^{-6}. It was found that monthly testing, for example, could also reduce this probability by more than an order of magnitude.

4.1.7 Event Tree for LPIS Check Valve.

The event tree for the LPIS check valve shows the possible sequence of events resulting from rupture of the LPIS check valve barriers. All sequences are considered to result in core melt and the dominant radioactivity release path would occur through the ruptured LPI system into a safeguards building that houses the LPI system. The discharge of RCS coolant and steam into the safeguards building would cause loss of leakage integrity of the safeguards building. Radioactivity deposition and plateout in the safeguards building has been estimated to be small since the steaming rate would tend to rapidly sweep the fission products from the small volume building to the atmosphere.

Column heading EP reflects the availability of electric power to operate the high pressure injection system (HPIS) pump which is reflected under column heading ECI. There would be no ECI success in terms of preventing a core melt. However, if the accumulators and the HPIS operated, core melt could be delayed until after the coolant delivered from the RWST has been depleted. For example, if only one of the three HPIS pumps were to operate, the rate of RWST depletion would be less and core melt could be advantageously delayed for about 10 to 11 hours. If more than 1 HPIS pump were to operate, or if the containment ESFs were to be actuated by the plant operator, or if the LPIS pumps would operate to increase RWST depletion, then core melt could occur in about 1 to 2 hours. This was the expected time of melt considered for purposes of determining the potential radioactivity release.

The column heading RPS represents success or failure of the reactor protection system to initiate trip of the reactor control rods and is illustrated merely to indicate that core melt could be hastened slightly in time if failure of RPS occurred. Column headings EP and RPS on the event tree could be readily excluded from the tree since the probability of failure for each is small and their failure would simple hasten the time of melt.

4.2 BWR LOSS-OF-COOLANT ACCIDENTS

Reactor coolant system (RCS) ruptures which result in loss of coolant accidents can be categorized as a function of rupture location. RCS ruptures inside the containment barrier are distinguished from ruptures outside the primary containment.

Evaluation has shown that the significant loss-of-coolant accidents can be covered by four major accident categories, and these are treated in the following subsections:

[1] Refer to section 4 of Appendix V.

4.2.1 BWR Large LOCA Event Tree
4.2.2 BWR Small LOCA Event Tree - S1
4.2.3 BWR Small LOCA Event Tree - S2
4.2.4 BWR Reactor Vessel Rupture

In addition to the cases treated in the above subsections, numerous possible break locations in the RCS piping were examined to determine whether cases of greater magnitude or of greater probability had been overlooked.

4.2.1 BWR LARGE LOCA EVENT TREE

The BWR large LOCA event tree, Fig. I 4-8, shows the potential sequences that could result from a large break of the RCS. Definitions of the headings on the event tree are presented in detail following the discussion on the development of the tree. The core status, the coupling of the sequences with the containment event tree, and the event timing considerations are presented in Tables I 4-5 and I 4-6.

4.2.1.1 BWR Large LOCA Event Tree Development.

The initiating event, which is the first column heading, is a random rupture in the reactor coolant system ranging in size from that equivalent to a 6-inch diameter pipe break up to double-ended rupture of the largest pipe in the system. This is the same initiating event shown on the functional LOCA event tree. The next event considered is electric power. Again, this column is identical to the functional event tree column.

Reactor trip is the next column for consideration. The reactor protection system (RPS) provides the function of reactor trip in case of an accident, and "RPS" is shown as the heading on the event tree.

The next column to convert from the functional event tree is emergency coolant injection (ECI). From Table I 2-1 in section 2 of this Appendix, it can be seen that the systems to accomplish this function are the core spray injection system (CSIS), the low pressure coolant injection system (LPCIS), or combinations of the core spray injection system and the low pressure coolant injection system. To show all these choices on the large LOCA event tree would make the tree unduly complicated. Therefore, the column heading ECI is retained on the BWR large LOCA event tree. The probability of the core spray injection system and low pressure coolant injection system succeeding or failing to accomplish this function is accounted for on the detailed fault tree of ECI (see Appendix II).

Immediately following the emergency coolant injection column, a new column has been added called emergency cooling function (ECF). This column had been added to account for the possibility that the water delivered to the reactor vessel by the emergency core cooling injection systems does not properly cool the core even though the emergency cooling injection systems operate as planned. A summary discussion of the emergency cooling functionability column is presented in section 4 of Appendix V.

The next column on the functional LOCA event tree to be considered for the BWR large LOCA event tree is the column of postaccident radioactivity removal (PARR). In a BWR this function is initially accomplished by the vapor suppression system. As gases and steam are released from the break in the drywell, they are swept into the wetwell and scrubbed by the water in the wetwell, thus capturing much of the radioactivity released and reducing the overall containment pressure. If the vapor suppression system failed to operate, the primary containment would catastrophically fail due to overpressure; therefore, the vapor suppression could in turn affect the emergency cooling injection systems (ECIS) which are partly contained in the primary containment. Due to this interrelationship, the vapor suppression column (VS) is shown just ahead of the ECI column on the BWR large LOCA event tree.

The remaining column headings on the functional LOCA event tree to be considered are post accident heat removal (PAHR) and emergency coolant recirculation (ECR). In the BWR, the ECR function must be condidered first because it is necessary to transfer the heat from the core to the containment prior to considering removal of the heat from the containment. The emergency cooling recirculation for a BWR may be handled by either the core spray recirculation system (CSRS) or the low pressure coolant recirculation system (LPCRS). It should be noted that the pumps for emergency cooling recirculation in the core spray recirculation system or the low pressure coolant recirculation system are the same pumps that were used in the emergency cooling injection system. However, since the ECI function reflooded the core, fewer pumps are needed to maintain the core in a flooded condition and to keep the water circulating through the core. For the BWR large LOCA event tree, the LOCA

functional event tree column heading of ECR is replaced by the systems headings CSRS and LPCRS. The next function to consider is the post accident heat removal. This is accomplished in the BWR by the low pressure coolant injection pump passing water through a heat exchanger on the tube side. On the shell side of the heat exchanger, the high pressure service water system circulates water and thus removes heat from the primary system. Therefore, for the function of post accident heat removal (PAHR), the BWR large LOCA event tree shows the high pressure service water system (HPSW).

The core spray recirculation system pumps and the low pressure coolant recirculation system pumps must have a minimum net position suction head (NPSH) to operate properly. As long as the high pressure service water system (HPSW) is removing the heat from the containment, the minimum net positive suction head required for these pumps will be available for proper operation. However, if there is a failure of the high pressure service water system, amount of time that a net positive suction head is available for proper pump operation is a function of the status of the primary containment integrity. It has been determined that if the leakage from the primary containment is greater than 100% volume per day (approximately the size of a one-inch hole in the primary containment), the pumps will cavitate due to the lack of a net positive suction head, and therefore, fail the function of emergency cooling recirculation. Due to this dependency, a new column has been added to the BWR large LOCA event tree. This column heading is containment leakage less than 100% per day and the column is placed just prior to the systems that provide the emergency coolant recirculation (ECR) function.

By making the above system substitutions into the BWR large LOCA event tree to account for the functions on the functional LOCA event tree, and adding the columns of vapor suppression (VS) and containment leakage (CL) at their appropriate places, the conversion is made from the functional LOCA event tree to the BWR large LOCA event tree as presented in Fig. I 4-8.

4.2.1.2 BWR Large LOCA Event Tree System Interrelationships.

Several illogical paths on the functional event trees of section 2 were eliminated due to both functional interrelationships and functional-operability interrelationships as well as the system relationships to preceding functions. See Table I 4-5 for the delineation of logic for the accident sequences. Table I 4-1 also illustrates the relationships of the large LOCA event tree to the containment event tree developed in section 2 of this appendix.

In sequences 3, 6, 9, and 12, no choice has been made on high pressure service water (HPSW). This choice has been eliminated because the low pressure coolant recirculation pump is not carrying the water containing the heat from the containment to the heat exchanger. The failure of this system prevents the HPSW from performing its function of removing the heat on the secondary side of the heat exchanger. Therefore, no choice is made. In sequences 6 and 12, both systems which provide emergency cooling recirculation (ECR) have failed. Therefore, the heat is not being removed from the core and transferred to the torus water of the containment. Again, since there is no path for the containment heat to the heat exchanger, the HPSW cannot perform its function and therefore no choice is made.

In sequences 13 and 14, no choice is shown for the CSRS, the LPCRS, or the HPSW. Since the core will melt due to the functionability failure of the emergency cooling injection, the functions of emergency cooling recirculation and containment heat removal are of no importance and have no significant impact on the results of these sequences. Therefore, these choices have been eliminated.

Sequences 15 and 16 eliminate the choice of ECF when the emergency cooling injection system (ECIS) fails. Since the injection system does not deliver an adequate amount of water to cool the core, it could not possibly function to cool the core, and, therefore, this choice is eliminated. Since the core will melt due to ECI failure, the choices of CSRS, LPCRS and HPSW have been eliminated for the same reasons given above for the ECF failure. This logic is also applicable to sequences 23 and 24.

In sequences 15, 16, 24, and 25, ECI failure has two possibilities; (a) an inadequate amount of water delivered to cool the core or, (b) no water delivered to the core. Since these different failures can have different consequences, each sequence is subdivided into two parts, a and b.

If there is a vapor suppression failure, there is no choice on the containment leakage. Vapor suppression failure will overpressurize the primary containment and eliminate the containment leakage choice since it will always be greater than 100% per day. This is reflected in sequences 17 through 24. In the sequences considering an RPS failure, no choice has been made on ECI, ECF, CSRS, LPCRS or HPSW. As discussed in section 1, these sequences which consider failure of RPS have always been estimated, conservatively, to result in a core melt. Therefore, all following system operation considerations have been eliminated.

In the sequences considering electric power failures, sequences 28, 29 and 30, none of the emergency safeguard systems can operate due to the failure of electric power, therefore, these choices are again eliminated. The RPS choice is not shown because the system will trip automatically on loss of electric power.

Examination of sequences 1 through 6 vs. 7 through 12 shows that these are identical paths except for the consideration of containment leakage. Since the status of the containment leakage (CL) can affect the release of radioactivity at various periods of time, a question on the magnitude of leakage is always logical except when there is a failure of vapor suppression (VS). As discussed before, vapor suppression failure automatically eliminates any containment leakage choices.

4.2.1.3 Definitions of Events for the Large LOCA Event Tree.

Event A - Large Break in the Reactor Coolant System: Large LOCA

The initiating event is a random rupture of a primary system pressure boundary pipe creating an opening from 0.4 square feet to the design basis accident (double-ended break of one main recirculation line). This size break will depressurize the system without relief valve, HPCI, or ADS assistance, and requires only the low pressure emergency cooling system operation to mitigate the accident consequences.

For this study, any primary system pressure boundary pipe break is conservatively assumed to be the double-ended recirculation line break because this break places the most severe demands on the ECCS and the consequences of any other break are bounded on the upper limit by the consequences of the double-ended recirculation line break.

Event B - Electric Power: EP

The various emergency and standby systems require AC power, DC power, or both, to operate successfully. AC power is received from two separate off-site sources. In the event of total loss of power from off-site sources, AC power is supplied to the emergency and standby equipment by diesel generators located on the site. These power sources are independent of the normal AC supply systems. Each power source, up to the point of its connection to the auxiliary power bus, is capable of complete and rapid electrical isolation from any other sources. Loads important to plant safety are split and diversified between auxiliary bus sections, and means are provided for rapid isolation of system faults. Station batteries are provided as a reliable source of DC control power for the emergency and standby systems.

Failure of electrical power is defined as the failure to provide AC and DC power for the operation of the engineered safety features required to mitigate the initiating event. The probability of partial failures of AC or DC power required for appropriate operation of individual components of engineered safety systems are accounted for in the fault tree for each system.

Electric power was placed early in the event tree because all of the emergency and standby systems require either AC power, DC power, or both, to operate successfully; therefore, failure of electric power, as defined, eliminates the choices on the emergency and standby systems and these were placed later in the event tree.

The electrical systems and the other systems discussed below are more fully described in Appendix II.

Event C - Reactor Protection System: RPS

RPS is the operating function which consists of the simultaneous insertion of all reactor control rods to shut down the reactor and keep it subcritical. RPS is automatically initiated if a monitored critical variable exceeds its set point, e.g., high drywell pressure. The reactor protection system (RPS) opens valves in the control rod drive modules which releases pressurized water into the rod drives, providing the force to rapidly insert the control rods.

Failures of RPS is defined as the failures of more than two adjacent control rods to insert to make the reactor

subcritical prior to reflooding the core with ECCS. It has been ascertained that at 100°C more than two adjacent control rods not inserted in the interior of the reactor will give a $K_{eff} \geq 1$.

This event was placed immediately following electric power (EP) because its failure alone will result in the reactor remaining at a significant power level while there is moderator in the core during both the blowdown and reflooding phases of the accident. Therefore, it was assumed that failure of RPS ultimately leads to core melt.

Event D - Vapor Suppression: VS

A vapor suppression primary containment houses the reactor vessel, the reactor coolant recirculating loops, and other branch connections of the reactor primary system. The vapor suppression system consists of a drywell, a pressure suppression chamber storing a large volume of water, a connecting vent system between the drywell and the water pool, isolation valves, containment cooling systems, and other service equipment. In the event of a process system piping failure within the drywell, reactor water and steam would be released into the drywell air space. The resulting increased drywell pressure would then force a mixture of air, steam, and water through the vents into the pool of water stored in the suppression chamber. The steam would condense rapidly in the suppression pool and result in a rapid pressure reduction in the drywell.

Failure of vapor suppression is defined as the failure of the vapor suppression system to condense an adequate quantity of steam to lower the pressure to a value which does not cause the primary containment to fail structurally. The most probable cause of vapor suppression failure is a bypass from the drywell to the air space of the wetwell. For the large LOCA, the bypass area would have to be greater than one vacuum relief valve open to result in failure.

The event was placed prior to the containment leakage and emergency core cooling events because its failure destroys the containment and increases the probability of failure of the core cooling system.

Event E - Emergency Coolant Injection: ECI

A number of emergency core cooling systems are provided to prevent excessive fuel clad temperatures in the event of a rupture of the primary coolant pressure boundary resulting in the loss of reactor coolant. The two systems provided for a large LOCA are the core spray injection system (CSIS) and the low pressure coolant injection system (LPCIS).

The core spray injection system consists of two independent pump loops that deliver cooling water to spray spargers over the core. The system is actuated by conditions indicating that a breach exists in the nuclear system process barrier, but water is delivered to the core only after reactor vessel pressure is reduced. This system provides the capability to cool the fuel by spraying water onto the core and uses two pumps in each loop.

Low pressure coolant injection (LPCI) is an operating mode of the residual heat removal system (RHRS) and is an engineered safeguard. LPCI uses the pump loops of the RHRS to inject cooling water at low pressure into an undamaged reactor recirculation loop. LPCI is actuated by conditions indicating a breach in the nuclear system process barrier, but water is delivered to the core only after reactor vessel pressure is reduced. LPCI operation, together with the core shroud and jet pump arrangement, provides the capability of core reflooding following a loss-of-coolant accident in time to prevent excessive fuel clad temperatures. There are four LPCI pumps.

Successful cooling of the core, as measured by ability to meet the AEC criterion for "single failure" in addition to loss of off-site power, can be achieved with various combinations of LPCI and CS pumps but does not require that they all be operable. Analysis of the following combinations of pumps determined that these were successful:

a. All four CS pumps operate - any number of LPCIS pumps can be failed.

b. Any three LPCI pumps operate, and at least two CS pumps operate. (Two CS pumps must be in the same loop.)

Realistically, other combinations can be expected to be successful, but, for purposes of this study, all other combinations will be considered failure. Failure means inability to deliver water to the vessel, which can result from failure of the pumps or from failure of the associated controls, piping, etc. The ECCS must operate until the core is reflooded, at which time one ECCS pump

is sufficient to maintain the water level in the core.

This is a conservative definition of failure, but there is little impact in the overall risk evaluation.

All systems that operate at their minimum design basis are assumed to achieve their design function with the exception of the systems that provide emergency core cooling capability, i.e., low pressure coolant injection (LPCI) and core spray. These emergency core cooling systems are shown with both operability and functionability delineated on the event tree.

Event F - Emergency Cooling Functionability: ECF

Theoretical possibilities exist for failure of the emergency core cooling system to reflood and cool the core even though emergency coolant is delivered to the reactor vessel. Included are failure of core supporting structures resulting in an undefined coolant flow path within the vessel and an uncoolable core geometry as a result of blowdown loads and subsequent thermal distortion of the core.

Failure is defined as the failure to provide the required quantity of water to the reactor core to prevent core melt, due to structural failures, such as core shroud failure, jet pump failure, or other failures which may result from initial blowdown.

Functionability is considered on the event tree only when operability is successful. Failure of either ECI or ECF is assumed to result in core melt. The column headings for ECI and ECF are located prior to ECR and HPSW since successful ECR and HPSW system operation is not possible unless the core is reflooded and maintained in a reflooded condition within a short period of time following the LOCA.

Event G - Containment Leakage: CL

The primary containment and reactor vessel isolation control system automatically initiates closure of isolation valves to close off all process lines which are potential leakage paths for radioactive material to the environs. The action is taken upon indication of a potential breach in the nuclear system process barrier.

The rate of leakage from the containment following a LOCA can affect the operation of other emergency and standby systems.

If leakage is less than 100% per day and the system that removes heat from the suppression pool water fails, the ECCS pumps will operate until the primary containment fails due to overpressure.

On the other hand, if the leakage is greater than 100% per day and the long term cooling fails, the ECCS pumps will cavitate due to inadequate net positive suction head (NPSH) for the pumps. However, the leakage rate from the primary containment will be sufficiently high to keep it from reaching rupture pressure.

Based on these considerations, the definition of containment success is: Less than 100 percent of the containment volume per day. This success path is defined as having no or minor failures of primary containment isolation which result in a leakage rate to the secondary containment of less than 100 volume per cent per day. This leakage rate is equivalent to approximately a one inch diameter hole in the primary containment. Therefore, the failure path is defined as any leakage greater than 100 volume per cent per day.

The containment failure column heading is placed on the event tree prior to the CSRS and LPCRS column headings because the failure or partial success of the containment affects the timing of possible ECR failures due to the NPSH requirements of the ECR pumps.

Event H - Core Spray Recirculation System: CSRS
and
Event I - Low Pressure Coolant Recirculation System: LPCRS

The core spray recirculation system (CSRS) or the low pressure coolant recirculation system (LPCRS) provide for the long term recirculation of water through the core after the ECI function has been successfully accomplished. Once the core has been reflooded by the ECI systems, the flow requirements for the long term recirculation are greatly reduced.

Failure of CSRS is defined as the failure of 4 of 4 core spray pumps to provide long term recirculation of water through the core.

The definition of the LPCRS failure is dependent on the success or failure of the CSRS. Therefore, LPCRS failures are given in two categories:

a. Failure of LPCRS given success of CSRS is:

   Failure of 4 of 4 LPCRS pumps to provide flow of the heated torus water through the shell side of a residual heat removal heat exchanger and return to the torus.

b. Failure of LPCRS given failure of CSRS is:

   Failure of 4 of 4 LPCRS pumps to provide long term recirculation of water through the core and provide flow of the heated torus water through the shell side of a residual heat removal heat exchanger.

Event J - High Pressure Service Water: HPSW

The high pressure service water (HPSW) is a plant system which provides for river water flow through the tube side of a residual heat removal heat exchanger. This system provides for heat removal by transferring the heat from the hot water on the shell side of the heat exchanger to the cooler river water on the tube side of the heat exchanger.

Failure of the HPSW is defined as: Failure of 4 of 4 HPSW pumps to deliver river water to the tube side of a residual heat removal heat exchanger and return the water to the river.

The HPSW system must be initiated within 25 hours when primary containment integrity is maintained and within two hours when primary containment is violated. Residual heat removal has to be maintained for approximately six months. Within the six month period, provisions can be made for transferring the fuel to the spent fuel storage pool, or alternate methods of core cooling can be provided if required.

4.2.2 BWR SMALL LOCA EVENT TREE - S1

As indicated in section 4, the S1 rupture pertains to a break area of about 2 to 6 inches diameter in the RCS. Figure I 4-9 illustrates the possible sequences for this initiating event. This event tree was developed in the same manner as the large LOCA event tree, i.e., substituting appropriate ESFs for the functions shown on the functional LOCA event tree, Fig. I 2-8, section 2.

The break size range for this LOCA represents ruptures in the RCS that require specific combination of ESFs to mitigate the incident. The differences between the required systems for this break range and the required systems for the large LOCA case (section 4.2.1) are discussed in the event definitions which follow. Table I 4-7 presents the system status and containment failure modes for this event tree.

DEFINITIONS

S1 - Initiating Event

The initiating event is a failure of the reactor coolant pressure boundary (RCPB) creating an opening of about 2.5 to 8.5 inches diameter for a liquid break and about 4.7 to 6.0 inches diameter for a steam break. Openings larger than the maximum sizes stated above are considered to be large LOCAs since they will depressurize the system without relief valve, HPCI, or ADS assistance, and require only the low pressure ECCS operation to reflood the core.

All small LOCAs are conservatively assumed to occur instantaneously with the reactor operating at normal full power; that is, it is assumed that there is no prior warning of an impending pipe break from the leak detection system.

E - Emergency Coolant Injection: ECI[1]

A number of systems are provided to prevent excessive fuel clad temperatures in the event of a failure of the reactor coolant pressure boundary. One of these systems is the high pressure coolant injection (HPCI) system. This system consists of a steam-turbine driven pump, connecting piping, and associated instrumentation. The pump can take suction from either the condensate storage tank or the suppression pool and pump the water to the reactor vessel.

The low pressure ECCS (core spray and low pressure coolant injection (LPCI) systems) are also available to provide and/or maintain an adequate inventory of reactor coolant in the vessel in the event of a small LOCA. However, the operation of the automatic depressurization system (ADS) or manual operation of the safety relief valves to reduce the pressure within the reactor coolant system is necessary to allow the low pressure ECCS to operate following a small LOCA.

[1]The ECF Column has been eliminated from the small LOCA event trees for the reasons discussed in section 4.2 of Appendix V.

The HPCI system can operate only while the steam pressure within the reactor coolant system is at or above 150 psia. Once the pressure decreases below this level, it is necessary to operate at least one of the low pressure ECCS pumps to maintain the core in a reflooded condition.

Therefore, failure of the ECCS to operate results from:

a. Failure of all of the core spray pumps and all of the LPCI pumps to deliver flow to the reactor vessel after the reactor steam pressure has decreased to a value insufficient to operate the HPCI pump turbine; or

b. Failure of HPCI system to operate and either (1) failure of the automatic depressurization system or operator action to reduce system pressure to below 300 psig, or (2) failure of a sufficient number of core spray and/or low pressure coolant injection pumps to operate once the reactor pressure is reduced below 300 psig.

Actually, the feedwater system will normally continue to operate and maintain the reactor coolant inventory following a small LOCA. In this regard it is essentially redundant to the HPCI system. The possible success path afforded by the feedwater system was conservatively ignored in the definition of ECI failure.

4.2.3 BWR SMALL LOCA EVENT TREE - S2

As indicated in section 4, the S2 rupture pertains to a break area of about 1/2 to 2 inches diameter in the RCS. Figure I 4-10 illustrates the possible sequences following this initiating event.

The S2 event tree is identical to the S1 event tree except for the break size range and the emergency coolant injection (ECI) requirements. These differences are discussed in the event definitions that follow.

Table I 4-8 presents the core status resulting from the various accident sequences and couples these with the containment event tree.

DEFINITIONS

S2 - Initiating Event

The initiating event is a failure of the reactor coolant pressure boundary (RCPB) creating an opening of about 0.6 to 2.6 inches diameter for a liquid break and 1.0 to 4.7 inches diameter for a steam break. For openings smaller than these minimum sizes, adequate coolant inventory within the reactor vessel is maintained by the control rod drive hydraulic supply systems. Openings larger than the maximum sizes stated above are considered to be large LOCAs since they will depressurize the system without relief valve, HPCI, or ADS assistance, and require only the low pressure ECCS operation to reflood the core.

All small LOCAs are conservatively assumed to occur instantaneously with the reactor operating at normal full power, that is, it is assumed that there is no prior warning of an impending pipe break from the leak detection system.

E - Emergency Coolant Injection: ECI

A number of systems are provided to prevent excessive fuel clad temperatures in the event of a failure of the reactor coolant pressure boundary. One of these systems is the high pressure coolant injection (HPCI) system. This system consists of a steam turbine driven pump, connecting piping, and associated instrumentation. The pump can take suction from either the condensate storage tank or the suppression pool and pump the water to the reactor vessel. The reactor core isolation cooling (RCIC) system is similar to the HPCI system but provides only about 21% as much flow. The RCIC flow is sufficient for relatively small openings, up to and including one safety/relief valve failed in the open position. The low pressure ECCS [core spray (CS) and low pressure coolant injection (LPCI) systems] are also available to provide and/or maintain an adequate inventory of reactor coolant in the vessel in the event of a small LOCA. However, the operation of the automatic depressurization system (ADS) or manual operation of the safety relief valves to reduce the pressure within the reactor coolant system is necessary to allow the low pressure ECCS to operate following a small LOCA.

The HPCI and RCIC systems can operate only while the steam pressure within the reactor coolant system is at or above 150 psia. Once the pressure decreases below this level, it is necessary to operate at least one of the low pressure ECCS pumps to maintain the core in reflooded condition.

Therefore, failure of the ECCS to operate results from:

a. Failure of all of the core spray pumps and all of the LPCI pumps to deliver flow to the reactor vessel after the reactor steam pressure has decreased to a value insufficient to operate the HPCI and RCIC pump turbines; or

b. Failure of the HPCI or RCIC systems to operate and either (1) failure of the automatic depressurization system and operator action to reduce system pressure to below 300 psig, or (2) failure of a sufficient number of core spray and/or low pressure coolant injection pumps to operate once the reactor pressure is reduced below 300 psig.

Actually, the feedwater system will normally continue to operate and maintain the reactor coolant inventory following a small LOCA. In this regard, it is essentially redundant to the HPCI system. The possible success path afforded by the feedwater system was conservatively ignored in the definition of ECI failure.

4.2.4 BWR REACTOR VESSEL RUPTURE

This portion of the study was aimed at assessing the risk contributions that could result from potential ruptures of the BWR reactor vessel. Since only a limited number of possible outcomes can occur in the event of a BWR reactor vessel rupture, the use of an event tree to illustrate these few possibilities was found unnecessary.

Basically, three categories of vessel ruptures were considered and these are summarized as follows.

a. A vessel rupture of a size and location such that it is essentially equivalent to a large or small pipe break could occur. If the rupture is within size limits equivalent to a double-ended break of an outside recirculation line and if it were to be generally located above the core region (for the larger break sizes), then the effects of the rupture can be mitigated by the ECCS. Vessel breaks such as these are covered by the previously presented BWR large and small LOCA trees.

b. Large vessel breaks of about the same size as for a double-ended break of a recirculation line, but in the region below the core shroud, could result in a failure of core reflood capability and could potentially lead to excessive blowdown forces on the reactor vessel internals causing distortions of emergency cooling flow paths through the core. Inability to flood the core and core distortion would result in a failure of the emergency cooling function. The vapor suppression containment would be likely to initially contain the blowdown, but this class of vessel breaks would result in a core melt which would then be followed by an eventual rupture of the primary containment. When the primary containment ruptures, the secondary containment could also be ruptured, as described for those core melt sequences previously covered under the BWR large and small LOCA trees.

c. Very large vessel ruptures could result in high energy missiles, such as the reactor vessel head, or could cause motion of the reactor vessel to occur. An immediate breach of the primary containment structure and loss of leakage integrity could result in either case since the pressure suppression system could not accommodate the rate of energy released. In addition, the containment is small in size and and its proximity to the reactor vessel would indicate that severe vessel ruptures might either tear or cause missiles to penetrate the containment shell.

Because of the considerations in paragraph c above, it appeared that there could be some potential for a vessel rupture to cause breaks in the containment in more than one location and thus cause air circulation paths through the containment. Such paths could cause an increase in the radioactivity released because of the presence of an oxidizing environment.[1] Thus, the type of vessel rupture considered in paragraph c, as distinct from contribution to the LOCA event trees discussed in items a and b above, involves core melt in both a nonoxidizing and in an oxidizing environment in a failed containment.

4.2.5 BWR RCS RUPTURE INTO INTERFACING SYSTEMS

An investigation similar to that described in section 4.1.6 for the PWR was

[1] See Appendix VII for a discussion of the effects of oxidizing and nonoxidizing environments on radioactive release magnitudes.

made for the BWR. No significant contributions to the overall risk were found from the investigation of various break locations and ruptures into interfacing systems.

An example of the various break locations examined is the steam line break external to the containment. For this event to result in a core melt, both of the steam line isolation valves would have to fail to close and an additional failure of the reactor trip (RPS) or the emergency core cooling system (ECCS) would have to occur. The probability of such accident sequences occurring was found to be much less (by several orders of magnitude) than that of comparable core melt accident sequences (e.g., AEG-δζ) already covered in the large LOCA event tree. Thus the probability contribution from a steam line break was negligibly small when compared to LOCA sequences yielding similar releases of radioactivity.

4.3 TRANSIENT EVENT TREES

PWRs and BWRs are designed to accommodate variations from normal values of process parameters that may occur in operation. Many of these variations are corrected by the reactor operator or by the process control systems provided. Others require rapid shutdown of the reactor to prevent fuel heat imbalances. In the case of transients without shutdown of the reactor, the fuel heat imbalance has the potential to cause fuel melting in an intact reactor coolant system (RCS) or overpressure and rupture of the RCS.[1] Also, under some conditions (such as stuck open safety/relief valves), it is possible that a transient could potentially result in a loss of primary system coolant and still leave the core coolable by ECCS. This can be treated in the transient event trees or handled by transferring the applicable accident sequences into the LOCA event trees.

Transients generally fall into two categories - those that are fairly likely, or anticipated transients, and those that are unlikely, or unanticipated transients. In assessing the potential risks due to these types of transients, the wide variability in frequency of occurrence of the two categories suggests that only the more likely ones will be contributors to the overall risk. This is due to the fact that, except for those that cause LOCAs, all the transients, where protective systems fail, have essentially the same end point - a molten core and a ruptured reactor coolant system in an intact containment.[1] Thus, it should be necessary only to identify the several most likely ways for core melt to occur and the unlikely ways that result in the same consequence should not be important contributors to the risk.

Figures I 4-11 and I 4-12, applicable to the PWR and the BWR, respectively, show several simplified transient trees, with estimated failure probabilities assigned to the various events to illustrate why the unlikely transients may be ignored. The failure probabilities assigned are generally derived from experience data and the fault trees in Appendix II. In two cases (failure of the power conversion system and the occurrence of unlikely transients), estimates were made for the probability of occurrence. The values in these cases were chosen in such a way as to ensure that the differences in probability of occurrence of the various accidents in the different trees would not be overstated.

Parts a and b in Fig. I 4-11 cover the high probability end and low probability end of the spectrum of anticipated transients for the PWR. Parts c and d show the high probability end and low probability end of the spectrum of unanticipated transients. It can be seen from these figures that the core melt likelihood is clearly dominated by parts a and b as opposed to c and d.

Figure I 4-12 shows three simple transient event trees for the BWR. As in the PWR, the anticipated transients clearly dominate the probability of core melt.

The prominent role played in the overall probabilities of accident sequences by the initial probabilities (first column) requires a further word as to the source of the initial probability numbers. The

---

[1] Of course, large scale fuel melting in an intact RCS will almost certainly ultimately rupture the RCS.

[1] A control rod drop accident in a BWR, if it were to occur at specific conditions, and if there were a failure to scram, could perhaps result in a failure of the reactor vessel and thus the primary containment. The plant design makes the probability of the specific conditions for such an accident negligibly small.

value of 10 per year for likely events is derived from operating experience from U.S. PWR and BWR plants, which reveals that unplanned shutdowns have occurred from various equipment malfunctions or failures, operator errors, and related operational transients (Ref. 3).

On the other hand, there are about 150 reactor years of experience in which no unanticipated transients have occurred. From these data the unanticipated transient occurrence rate is probably less than 10^{-2} to 10^{-3} per reactor year. Since the amount of experience is small, these data can be supplemented by estimates of systems and reliability considerations. An examination of the various factors involved in the occurrence of unanticipated transients and a comparison with experience, other analyses, and numbers obtained in the study suggest that the rate is actually much less than 10^{-2} or 10^{-3}; therefore ~10^{-5} has been selected for use in the illustrative comparisons made in Figs. I 4-11 and I 4-12. It should be noted that even if a high rate is used, say 10^{-3}, the unanticipated transient tree would still not contribute significantly to the overall risk.

The principal aim of this portion of the Reactor Safety Study was to assess these more frequent anticipated transient events and to establish their incremental contribution to the public risk. To assist in this effort, detailed PWR and BWR transient event trees were developed and are discussed in sections 4.3.1 and 4.3.2 respectively.

4.3.1 PWR TRANSIENTS

As indicated in section 4.3 of this Appendix, only likely transient events need to be covered by a transient event tree. Table I 4-9 contains a list of all transients identified as being applicable to the PWR plant.

4.3.1.1 PWR Transient Event Tree Development.

The PWR transient event tree presented in Fig. I 4-14 was developed using functional logic similar to that addressed in some detail in section 2 of this Appendix for development of the LOCA event trees. The functional logic underlying the PWR transient event tree is summarized below to emphasize the various system relationships that exist for the PWR.

This section discusses:

a. The functions required following PWR transient events in order to perform a safe shutdown and cooldown of the plant.

b. The PWR transient event tree in terms of systems necessary to perform the functions of safe shutdown and cooldown.

c. The definitions of system success/failure that are needed to assist in the development of fault trees and in quantification of the PWR transient event tree.

4.3.1.2 PWR Functions and Functional Event Tree.

The functions that must be performed following the transient event in order to preclude core damage are:

1. The fission process must be terminated.

2. The reactor coolant pressure must be limited to a value that will not cause failure of the reactor coolant system (RCS).

3. An adequate coolant inventory must be maintained within the RCS.

4. The core shutdown heat energy must be transferred to the environment.

These functions are illustrated on the functional event tree presented in Fig. I 4-13. This figure indicates that the core is not damaged if all four functions cited above are performed successfully. If any of functions (1), (3), or (4) is not successful, core damage and melt could occur. If function (2) is not successful, LOCA could result and the possible accident sequences that might subsequently occur are evaluated using the PWR LOCA and the containment event trees previously described.

A PWR event tree in terms of systems was developed from the functional tree using the same logic that was described in section 2 of this Appendix. This logic first requires that the systems that are able to perform each of the basic functions be identified. This identification is summarized in Table I 4-10. The logic used to develop the PWR anticipated transient tree, Fig. I 4-14, is briefly discussed in the following paragraphs.

The systems that can operate to make the reactor subcritical are shown in

Table I 4-10. Included is the reactor protection system, RPS, which can trip reactor control rods and the chemical volume control system (CVCS) which could provide alternate shutdown capability by delivery of a concentrated boron solution into the RCS. Certain transients such as those that cause an interruption or loss of the normal heat removal systems (e.g., main feedwater delivery to the steam generators) required rapid power shutdown in order to prevent overpressure of the RCS. The delivery of concentrated boron solution by the CVCS pumps would not be rapid enough in such cases to prevent RCS overpressure, although eventually sufficient boron could be delivered to make the reactor subcritical. Rapid shutdown can be accomplished only by the control rods. Therefore, only the RPS was included under the column heading Reactor Subcritical. The CVCS is shown under a separate heading (VCVC). The VCVC function is needed to enable coolant makeup to be provided for control of coolant contraction during cooldown, and to ensure shutdown margin during cooldown of the plant if the transient event leads to a decision to bring the plant to the cold shutdown condition.

The column HTE_H (Heat Transfer Environment - hot shutdown) indicates that during hot shutdown, core heat can be satisfactorily transferred to the environment after the transient event has occurred providing that portions of the power conversion system (PCS) are operable, or that the auxiliary feedwater system (AFWS) is operable. Successful operation of the PCS requires availability of A.C. power from non-emergency sources. Since the availability of the PCS can depend on the specific transient event and the AFWS may not, these systems were treated as separate columns on the PWR transient event tree, Fig. I 4-14.

The column RCS-OP indicates that the RCS pressure limiting function is performed by the pressurizer safety valve and the power operated relief valves. These are two possible failure modes. First, the valves may fail to open and second, once opened, the valves may fail to reclose. These two possibilities result in different situations: (1) if the safety valves fail to open,, the RCS pressure boundary would be subjected to very high pressure levels and in all likelihood rupture of the RCS would occur and provide the necessary relief. If the pressure level were to become very high, not only would the rupture of the RCS result in a LOCA but also the blowdown loads on the core and reactor vessel internals could potentially cause disruption of the core geometry and result in melting of the core. Where very high RCS overpressure levels resulted, it was assumed that the RCS would rupture and that core melt would occur. (2) If the required valves open but fail to reclose, then the result is, in effect, a small LOCA with coolant discharge occurring from the pressurizer vapor space. Since these situations are different and must be evaluated through use of different LOCA event trees, two separate columns were used in the PWR transient event tree.

The column HTE_C indicates that the heat transfer to the environment can be accomplished by the plant residual heat removal system (RHRS). This system is a low pressure system that would be used to transfer core decay heat once the plant operator decides to bring the plant to cold shutdown after any particular transient event that has not resulted in a rupture of the RCS. To bring the plant to cold shutdown (to where use of the RHRS is permissible) requires used of the CVCS and either the PCS or the AFWS. The RHRS is depicted by a single column heading on the tree and has been included principally for completeness. Should the RHRS be inoperable, the plant could remain at hot shutdown conditions with either the PCS or the AFWS providing for the required decay heat removal from the core.

4.3.1.3 PWR Transient Event Tree (Systems).

The PWR transient event tree is presented in terms of systems in Fig. I 4-14. The rationale used to develop this tree was summarized above. The individual column headings of the systems tree are discussed and defined in section 4.3.2.5. The PWR transient event tree is generalized and is intended to apply to all anticipated transients which require that the reactor be safely shut down and cooled and which are not the result of a LOCA.

The tree and accompanying chart, Fig. I 4-11, together show in a logical manner those combinations of system operations that will adequately cool the core and those sequences of system failures that will either cause a LOCA or result in core melting. A complete set of trees is formed by the anticipated transient tree, the LOCA event trees, and the containment event trees. These represent coverage of all important situations forseeable by this study whereby core melt could potentially occur as a result of malfunction or failure of the

plant's mechanical or electrical equipment.

4.3.1.4 PWR Transient Event Tree Definitions.

This section defines the systems represented by the event columns of the PWR transient event tree. Minimum operability states are presented below for those systems needed to carry out the core shutdown and cooling functions following a transient event. Less than the defined minimum operability state for a given system constitutes failure for that system.

Transient Event: TE

The initiating events are malfunctions, failures, or faults in the plant equipment or in the station's electrical network that result in a transient being imposed on the PWR reactor coolant system and core that (1) leads to a demand for the operation of the reactor protection system (RPS) to cause trip of the reactor control rods to shutdown the reactor core and (2) requires operation of the plant normal or alternate heat removal systems to ensure cooling of the reactor core. Other sequences which potentially result in RCS overpressures that could cause a rupture of the RCS boundary are included within the applicable PWR LOCA event trees presented previously in section 4.1 of this Appendix.

Reactor Protection System: RPS

The process of making the reactor subcritical at hot shutdown (or standby) is accomplished, normally, by a rapid insertion of the control rods, which after an interruption of holding power to the breakers, would be released to drop by gravity into the PWR core. Within several seconds the drop (or insertion) of the control rods makes the reactor subcritical at the hot shutdown condition (about ~547°F and 2250 psi). The rapid insertion of the control rods serves to arrest core power increases for all transient events. However, for those transient events which may initially result in a rapid cooldown of the RCS, the core can return to critical, and, as previously noted, the delivery of concentrated boron solution to the RCS would assist in returning the core to a subcritical condition. Although such cooldown transients cause reactivity to increase, the fuel damage from these events would be limited to the release of radioactivity into the RCS, even if delivery of the concentrated boron failed to occur. Alternately, if the control rods fail to insert and the anticipated transient event is relatively slow, the delivery of concentrated boron to the RCS via the CVCS pumps could serve to limit the core power increases and bring the reactor subcritical at the hot standby condition within about 5 to 10 minutes.[1]

If the anticipated transient event requires the plant to be further cooled down and depressurized from the hot standby condition, the addition of boron by the CVCS pumps is used to ensure that a safe shutdown margin (~1% $\Delta k/k$) is maintained through the RCS cooldown to the cold shutdown condition ($\lesssim$150°F and $\lesssim$400 psia).

As noted previously, the PWR transient event tree is considered applicable to both slowly occurring and rapidly occurring anticipated transients, and, since only the reactor protection system (RPS) would be effective in limiting core power for both, the RPS and boration functions are presented separately on the tree.

Failure of RPS is conservatively defined as the failure of the control rods to insert into the reactor core with no more than two adjacent rods failing to insert on demand.

Secondary Steam Relief and Power Conversion System - SSR and PCS(M)

This column heading includes portions of the PWR power conversion system which are normally in use (1) to maintain an adequate coolant inventory within the PWR steam generators, and (2) to transfer heat to the environment following a transient event. To be successful, this portion of the power conversion system must include the partial operation of the main feedwater and condensate system, which is used to deliver condensate from the turbine condenser to the steam generators following a transient event. These modes of partial PCS operation are discussed below.

Given a turbine trip, the steam from the steam generators is normally "dumped", or bypassed, into the condenser via the turbine steam bypass system. To enable

[1] Only in the case of those unlikely initiating events (e.g., events 2 through 5, Table I 4-9) would substantial core damage and potential melt be expected to occur with failure of the RPS to operate.

heat to be removed via this system, a vacuum in the condenser must be maintained. This requires that the transient event must not involve a loss of condenser vacuum. The operation of air ejectors and the circulating water system enables the condenser vacuum to be maintained, provided that a breach of the condenser has not occurred. If the main feedwater pumps are driven by turbine steam, as is the case for many PWR designs, then loss of condenser vacuum can also result in a loss of the main feedwater pumps. If the main feedwater pumps are electrically driven, as in the case of the PWR studied, then loss of condenser vacuum would only result in loss of the turbine steam bypass system and not the main feedwater pumps. In the situation where condenser vacuum has been lost, the electrically driven main feedwater and condensate pumps could be used to provide water makeup to the steam generators, and heat could still be rejected to the environment via the steam generator safety valves. This would lead to acceptable heat rejection to the atmosphere, but, eventually, the condensate supply from the condenser would become exhausted.

Regardless of whether the main feed pumps are steam driven or electrically driven, the condensate pumps (which are driven electrically in all PWR cases of which this study is aware) would be needed to enable water makeup to be provided from the condenser hotwell to the steam generators. Assuming failure of the condenser vacuum occurs and affects operability of the main feedwater pumps, the condensate pumps could potentially be used to deliver water to the steam generators. In this case, action by the plant operator would be needed, however, to depressurize the steam generators. This is so because the design of the condensate pumps would not permit water delivery against the high steam pressure conditions ($\leq$1100 psi) that would prevail in the steam generators, if steam discharges to the atmosphere at set point pressures of the steam generator safety valves. The plant operator could manually operate the power-operated relief valves provided for the steam generators and, in this way, depressurize the steam generators to permit water makeup to be provided by the condensate pumps. Since the condensate pumps are electrically driven and are required for each transient event in order for the PCS to be functional, the principal common fault leading to a loss of PCS would be the loss of AC power to the station auxiliaries (main feedwater pumps, condensate pumps, circulating water pumps, etc.). The PCS function could not, therefore, be restored for this transient event until a restoration of AC power was accomplished. Assuming that the reactor protection system operates to reduce core power level, a total lack of feedwater delivery to the steam generators to remove heat generated by the core would result in the steam generators boiling dry on the order of about 1/2 hour. An alternate feedwater supply is, however, provided by the auxiliary feedwater system (AFWS). Operation of this alternate feedwater system in conjunction with steam relief to the atmosphere through safety valves would result in successful cooling of the core following all transient events involving the interruption and loss of normal PCS heat removal capability. Should the auxiliary feedwater system fail on demand, the time available for the plant operator to restore operation of either the PCS or the AFWS, without risking an excessive loss of RCS coolant from the RCS pressurizer safety and relief valves and thus a core melt, would be approximately 1 to 1 1/2 hours. A loss of AC power to the station auxiliaries in excess of this time, in conjunction with a loss of the AFWS, could result in core melting.

For the PCS to successfully perform the function of transferring core heat to the environment requires certain components to be operable and certain conditions to be in existence as described below. Failure of PCS is defined to have occurred when these operable states and conditions are not met for the system.

a. Successful water makeup requires at least one complete train of the condensate and main feedwater piping system to be intact and operable to deliver water from the condenser hot well to the steam generators. A limiting condition for operability of the condensate and main feedwater pumps is the requirement that sufficient AC electrical power be available to drive the pumps. If the main feedwater pumps are not operable, successful PCS performance requires operability of the condensate pumps, with operator action taken to reduce the pressure level in the steam generators in order to accommodate coolant delivery at a lower pressure by the condensate pumps. Operability of the power operated relief valves in the main steam system is also required to permit the successful performance of the condensate pumps.

b. Successful heat removal from the core requires steam relief from the generators. This function can be accomplished by (1) operation of the turbine bypass valves to the condenser when availability of condenser vacuum permits; or (2) operation of the main steam system safety valves when both the condensate and main feedwater pumps are operable; or, (3) operation of the main steam system power operated relief valves under operator control when only condensate pumps are operable.

If the heat is removed from the core by steam relief to the atmosphere via either the main steam system safety valves or the main steam system power operated relief valves, the availability of makeup water from the PCS is considered to be limited to the inventory of condensate initially residing in the condenser hotwell. If heat is removed by steam relief to the condenser via operation of the turbine steam bypass valve system, the availability of makeup water to the steam generators is not limited by a loss of condensate to the atmosphere. Conditions permitting heat to be removed via the turbine steam bypass valve system also require that the main steam line isolation valves be open and that the condenser vacuum be maintained within acceptable limits by, (1) operability of the condenser air ejector system; and (2) operability of the circulating water system for condenser cooling.

Secondary Steam Relief and Auxiliary Feedwater System: SSR and AFWS

In the absence of M, above, the feedwater delivery equivalent to the flow from at least one of the three auxiliary feedwater pumps was used as the basis[1] for the definition given below of failure for the auxiliary feedwater system. Failure of this alternate heat removal function, provided by the secondary steam relief and auxiliary feedwater system, is considered to occur when at least the principal components listed below are not operating following the transient event:

a. Steam Relief Function (SSR):

Either: (1) no less than one of the five main steam system safety valves located on each main steam line;

(2) no less than two of three of manually operable and power operated main steam relief valves.

b. Auxiliary Feedwater and Condensate Delivery Function (AFWS):

Either: (1) operability of the one steam turbine driven auxiliary feedwater pump delivering water from the 100,000 gallon condensate storage tank until the tank is exhausted (~8 hours) and then from the plant fire protection system thereafter until such time as the plant is successfully cooled down and depressurized to permit core heat removal to be continued without dependence on the AFWS;

(2) operability of one of the two electrically driven auxiliary feedwater pumps delivering water as described above.

The time period of interest for hot standby or cooldown operations for either the PCS or AFWS would normally be expected to be ~6 hours following a transient.

RCS Safety/Relief Valves Open: S/R VO

This column heading represents the opening of the RCS pressurizer safety or safety and relief valves to limit the rise in the reactor coolant pressure immediately following the initiating transient event. Not all anticipated transient events (e.g., turbine trip) require operability of the safety valves, since the surge capacity of the pressurizer would suffice to accept the transient event with but a small surge in the pressure being seen. For more severe transients, such as those involving failure of the RPS to terminate core power, the operability of the pressurizer safety valves would be required to prevent a rupture of the RCS.

[1] The minimum operability requirement for the AFWS was based on analysis of ATWS transients as provided in WCAP-8096.

Three RCS pressurizer safety valves and two relief valves (power operated) are provided for the PWR. For those anticipated transients where RPS operates to terminate core power, the operation of only two of three of the pressurizer safety valves would suffice to limit the RCS overpressure transient to less than, or about, 110 percent of RCS design pressure. Sequences one through nine include these possibilities.

For those anticipated transients where RPS fails to terminate core power (i.e., the ATWS transients), the operation of three of three pressurizer safety valves would be needed to limit the RCS pressure level to less than about 150 percent of the RCS design pressure. Operation of the two pressurizer relief valves with the operation of the three safety valves would be expected to further reduce the RCS pressure level to less than, or about, 125 percent of the RCS design pressure. In general, the specific RCS pressure level that results from the ATWS transients will depend considerably on the specific combinations of systems operating during the transient event. As noted previously, the interruption or loss of the PWR main feedwater system potentially given rise to the most severe RCS overpressure levels. The possible variations in the predicted RCS overpressure levels were considered by the study, and, for sequences in which the safety valves failed to operate, it was assumed that the result was an RCS rupture with core melt. No commonly accepted, specific "design basis" combination of systems to be used for analysis of ATWS has yet emerged (Ref. 4). However, for purposes of this study, a reasonably conservative definition has been selected which encompasses all anticipated transient events and the ATWS events. Failure of the RCS safety/relief valves to open is defined as being the operation of less than three of the three RCS pressurizer safety valves.

Safety/Relief Valves Reclose: SR/VR

The RCS pressurizer safety/relief valves that open as a result of a transient event must reclose to prevent a discharge of an excessive quantity of coolant from the RCS. Otherwise, a valve sticking open following the transient event of interest would result in a loss of coolant event covered under the previously described small LOCA event trees.

Chemical Volume Control System: CVCS

This system is normally in use during all power operations to control the volume of RCS coolant, condition the chemistry of coolant, and assist in cooling of the main RCS circulating pumps. As will be discussed in detail subsequently,[1] the chemical volume and control system provides for multiple functions to be carried out during plant operations, during transients, or during LOCA events. For example, if a cooldown transient or a LOCA event occurs, an automatic alignment of the CVCS pumps takes place so the pump delivers emergency coolant and concentrated boron solution to the reactor core. This realignment of the CVCS system places the system into the high pressure injection system (HPIS) mode of operation. Also, the CVCS pumps can be used with suction to the pumps realigned to deliver concentrated boron solution from boric acid tanks (BAT's) in the plant. This second mode of realignment can be initiated by the plant operator should he elect to use this realignment for emergency boration to provide for a backup shutdown capability.

For purposes of failure definition for the CVCS during transient events, the previous definition developed for the High Pressure Injection System (see small LOCA - sections 4.1.2 and 4.1.3), reflecting failure to be less than the delivery from one of three HPIS pumps, is considered to be conservatively applicable to the transient event tree.

Residual Heat Removal System: RHRS

In the PWR plant studied, the RHRS would normally provide for continuity of cooling after the PCS or AFWS has been used in conjunction with the CVCS to cool and depressurize the plant from the hot shutdown (or standby) conditions. The RHRS has been included in the tree, principally for completeness.[2] Normally, the RHRS would not be used following

---

[1] See Appendix II - Fault Tree Analysis, High Pressure Injection System.

[2] The RHRS was not evaluated by use of the fault tree techniques as described in Appendix II for a number of the PWR ESFs. This increment of study effort could be accomplished at a later time if additional completeness is felt to be warranted. For the reasons outlined above, the risk contribution pertaining to PWR transient events did not require this incremental effort.

a transient event unless an extended shutdown period (for maintenance purposes, refueling activities, etc.) was planned. Unless the PCS or AFWS operates in conjunction with the CVCS following a transient event to allow for reduction in the RCS pressure, the operation of the RHRS would not be permissible. This is so because the RHRS is a low design pressure system that can operate only after the RCS pressure is reduced to less than 600 psi. Alternately, if RHRS operation were satisfactorily instituted in approximately 6 hours following a planned shutdown, and if subsequently, faults or malfunctions developed in the RHRS, the option would exist to reinstitute the heat removal capability of the AFWS. This option would exist for a finite time during the shutdown period until such time as, for example, the reactor vessel head was unbolted in preparation for refueling activities to take place. Since the intent of this portion of the study was to focus on those transient events that experience shows to occur frequently during reactor operations, the operability state of the RHRS system was considered to be of limited interest.

4.3.2 BWR TRANSIENTS

As in the case of PWR transients treated in section 4.3.1, only likely transient events are covered in the BWR transient tree (see also section 4.3). Table I 4-12 contains a complete list of all transients indentified as being applicable to the BWR plant.

4.3.2.1 BWR Transient Event Tree Development.

The BWR transient event tree presented herein was developed using functional logic similar to that addressed in some detail by section 2 of this appendix. The functional logic underlying the BWR transient is summarized below to emphasize the various system relationships that exist for the BWR.

This section discusses:

a. The functions required following a shutdown from power operation and the systems available to perform these functions.

b. The BWR transient event tree in terms of systems.

c. The detailed definitions of system success/failure that are needed in the development of the fault trees and in the quantification of the BWR transient event tree.

4.3.2.2 BWR Functions and Functional Event Tree.

The functions that must be performed following the transient event in order to preclude core damage are:

a. The reactor must be made subcritical;

b. The reactor coolant pressure must be limited to a value that will not cause the failure of the reactor coolant pressure boundary (RCPB);

c. An adequate coolant inventory must be maintained within the reactor vessel;

d. The shutdown core heat energy must be transferred to the environment.

These functions are illustrated on the functional event tree presented in Fig. I 4-15. This figure indicates that the core is not damaged if all of the four functions cited above are performed successfully. On the other hand, if any of the four functions above is not successful, the core could melt.

A BWR event tree in terms of systems was developed from the functional tree using the same logic that was described in the section on event tree development, section 2 of this appendix. This logic first requires that the systems that are able to perform each of the basic functions be identified. This identification is summarized in Table I 4-13. This information was used in conjunction with the functional event tree of Fig. I 4-15 to develop the BWR transient event tree (Fig. I 4-16). The logic utilized to develop the anticipated transient tree is briefly discussed in the following paragraphs.

The systems that operate to make the reactor subcritical appear in Table I 4-13 only in the function column entitled "Reactor Subcritical", RS. Therefore, this column heading is also used in the systems event tree.[1]

The pressure limiting function is performed by the safety valves and the safety/relief valves, as shown in the

---

[1] Detailed definitions of the systems operation that are required for success (or failure) are presented in section 4.3.2.4.

"Overpressure Protection" column, OP. There are two possible failure modes. First, the valves may fail to open and, second, once opened, the valves may fail to reclose.

These two possibilities result in different situations. If an insufficient number of the safety and relief valves fail to open, the reactor coolant pressure boundary (RCPB) is likely to be subjected to higher than design stresses and a core melt is assumed to result. If the required number of safety or safety/relief valves open, but do not all reclose, the result can be regarded as a small LOCA with the failure of the RCPS occurring in the steam space. Since these situations are different, two separate columns, M and P, are used on the BWR transient event tree, Fig. I 4-16.

Table I 4-13 shows that several systems can perform the function of maintaining an adequate vessel water inventory in the reactor vessel. One of these, the feedwater system, requires the availability of AC power from non-emergency sources to operate successsfully. Therefore, this system was treated using column Q on the transient tree.

The other systems shown in Table I 4-13 that can perform the function of maintaining an adequate vessel water inventory fall into two categories. The HPCI and RCIC systems require only DC power and steam to operate (AC power is not needed for operation of these systems). Therefore, they were grouped together in column U. On the other hand, the low pressure emergency core cooling systems (LP ECCS) require AC power to operate. Further, relief valves must be operated to reduce the reactor pressure prior to operation of the LP ECCS. Therefore, these systems were treated separately from those in columns Q and U and become column heading V of the transient tree.[1]

Table I 4-13 lists the systems available to transfer heat to the environment. The power conversion system can perform this function and reduce the reactor coolant temperature to about 200°F. The two other systems listed under the HTE function in Table I 4-13 (RHR and HPSW) must both operate in order to reject heat to the environment. The two methods of transferring heat to the environment (PCS alone, or RHR and HPSW) were treated with a single column heading, W, on the transient tree.

4.3.2.3 BWR Transient Event Tree (Systems).

The BWR transient event tree is presented in terms of systems in Fig. I 4-15. The rationale used to develop this tree from the function tree was discussed above. The individual column headings of the systems tree are defined below.

The tree and the accompanying chart, Fig. I 4-16 and Table I 4-14, relate those sequences that result in core melt to the possible sequences that exist on the containment event tree that was presented in section 2 of this appendix. The containment event tree options shown on Table I 4-14 assume that containment integrity is maintained during the period immediately following the initiating event. This assumption greatly reduces the number of cases that had to be considered to quantify the BWR transient event tree. The assumption is very slightly non-conservative regarding the probability of core melt. The magnitude of this non-conservatism is, however, less than one per cent, as discussed below.

4.3.2.3.1 Applicability of the BWR Transient Event Tree. The BWR transient event tree is intended to apply to all anticipated transients requiring reactor shutdowns from power operation that are not a result of a large or small LOCA. The tree shows in a logical manner those combinations of system operation that will adequately cool the core and those combinations of system failures that will result in core melting.

Some of these transients can lead to RCS overpressure if the safety and safety/relief valves do not operate as designed. For such sequences it was assumed that core melt would result. This possibility is explicitly considered in the tree. If the relief valve(s) open at the proper pressure but fail to reclose, this is effectively a small LOCA. This possibility is explicitly considered in the analysis of the BWR transient event tree by all sequences denoted TP (Fig. I 4-16).

The BWR transient tree, along with the large LOCA, the small LOCA, and the

---

[1] Some limited makeup to the vessel water inventory can also be provided by the control rod drive pumps; however it is not clear that these pumps alone can provide sufficient makeup to handle water losses due to boiloff. Thus this capability was conservatively omitted as a possible success path.

containment event trees form a complete set. The large and small LOCA event trees cover all situations, other than a catastrophic pressure vessel failure, in which there is a failure of the reactor coolant pressure boundary while the reactor is in operating condition. The anticipated transient tree covers all other situations resulting from anticipated transients where the plant is shutdown from power operation. Since any equipment malfunction or operating transient that might endanger the fuel clad integrity results in the initiation of a scram signal, all of these possibilities are treated by the BWR transient event tree. The containment tree treats all combinations of initiating events (from power operation) and system failures that result in a core melt, whether these are the result of a normal shutdown, a small LOCA, or a large LOCA. Therefore, all situations arising from power operation, except for catastrophic pressure vessel failure, are treated by the complete set of trees.

4.3.2.3.2 Effect of Containment Integrity Assumption. As stated above, the anticipated transient tree assumes the containment integrity is maintained during the period immediately following the shutdown from full power. This assumption is very slightly non-conservative regarding the probability of core melt. The magnitude of this non-conservatism was determined and is discussed in the following paragraphs.

If containment integrity is not maintained following a shutdown from full power, then the period of delay that can be permitted prior to initiating decay heat removal is reduced in some cases. Analysis of the fault trees has shown that the effect of this shorter time period increases the probability of failure by less than a factor of two. However, analysis of the containment fault tree shows that the probability of containment failure is about 6×10^{-3}. That is, if one assumes one-thousand shutdowns, containment integrity would be maintained successfully in 994 cases and would fail in 6 cases.

Assuming that the probability of core melt is doubled for those shutdowns in which containment integrity is not maintained, the effect of assuming successful containment integrity for all cases results in less than a one percent nonconservative error in the number of core melt cases that would be predicted.

4.3.2.4 BWR Transient Event Tree Definitions.

T - Anticipated Transient: AT

The initiating events are malfunctions, failures or faults in the plant equipment or in the station's electrical network other than a failure in the reactor coolant pressure boundary that result in a transient being imposed on the BWR which results in a demand for trip of the control rods and requires operation of the plant heat removal systems to ensure a safe shutdown and cooling of the core.

C - Reactor Subcritical: RS

This column represents the process of making the reactor subcritical by any of several methods. Each of the methods listed below is able to successfully make the reactor subcritical:

a. Rapid insertion of control rods (scram) with no more than two adjacent control rods failing to be inserted.

b. Slowly driving in any control rods not successfully inserted as a result of the reactor scram signal. For success, all but two adjacent control rods must be inserted within about 30 minutes after the scram signal.

c. Tripping of the reactor coolant recirculation pumps and successfully operating the standby liquid control system to deliver sodium pentaborate solution to the reactor coolant system. For success, system operation must be initiated within 10 minutes of receipt of the scram signal and the reactor must be rendered subcritical within 38 minutes of the receipt of the scram signal.

M - Safety/Relief Valves Open: S/R VO

This column represents the opening of the safety or safety/relief valves to limit reactor coolant pressure to 110 percent of the RCPB design pressure immediately following the initiating transient. For the severe transient, i.e., a turbine trip from high power without the turbine bypass, 8 of the 13 valves must open to be successful.

P - Safety/Relief Valves Reclose: S/R VR

The safety/relief valves that open as a

result of a transient must reclose to prevent discharge of an excessive quantity of reactor coolant to the suppression pool. For success, all of the safety/relief valves must reclose.

Q - Feedwater System: FW

To be successful, the feedwater system must maintain an adequate coolant inventory in the reactor vessel. Replenishment of the reactor vessel coolant inventory must be initiated within about 30 minutes after the initiation of the reactor trip signal. This function requires that one complete condensate-feedwater piping system is operable and able to deliver water from the condensate storage tank to the reactor vessel. This requires that the condensate and feedwater pumps in the piping system be operable, or that the condensate pump be operable and that the operator reduces reactor pressure to below 540 psia by using the relief valves. The water inventory in the condensate tank in the unit experiencing the transient will delay the need for the heat rejection function for about 22 hours. This time can be extended to about 27 hours if the water inventory in the condensate tank for the other unit is also used, or if the fire water or the makeup systems are used to replenish the condensate storage tank water inventory.

U - High Pressure Coolant Injection or Reactor Core Isolation Cooling: HPCI or RCIC

Successful operation of either the high pressure coolant injection (HPCI) system or the reactor core isolation cooling (RCIC) system will maintain an adequate coolant inventory in the reactor vessel. For success, operation of either of these systems must be initiated within about 30 minutes of the initiating event.

V - Low Pressure Emergency Core Cooling Systems: LP ECCS

Successful operation of the LP ECCS to maintain an adequate water inventory in the reactor vessel requires both of the following:

a. That the operator activates four or more relief valves to reduce reactor system pressure to below 300 psi within 30 minutes after the initiating event.

b. That four of four core spray pumps or two of four core spray pumps and three of four LPCIS pumps[1] operate immediately after the reactor coolant pressure is reduced to below 300 psia.

W - Residual Heat Removal and High Pressure Service Water or Power Conversion System: RHR and RPSW or PCS

For success either (a) the RHR and HPSW must both operate or (b) the Power Conversion System must operate to reject fission product decay heat to the environment. Heat rejection to the environment must be initiated using either method (a) or (b) within about 27 hours after the initiating transient in order to be successful.

a. For success, the RHR system must provide a complete flow path from and to the reactor coolant system through at least one RHR heat exchanger. In addition, the high pressure service water system must provide cooling water to the corresponding RHR heat exchanger.

b. Successful performance of the PCS to perform the function of transferring fission product decay heat to the environment requires that all of the following components be operable:

   1. One complete condensate-feedwater piping system is operable and able to deliver water from the condenser hotwell to the reactor vessel. This requires that the condensate and feedwater pumps in the piping system be operable, or that the condensate pump be operable and that the operator reduces reactor pressure to below 540 psia by using the relief valves.

   2. The main steam line isolation valves in one of the four main steam lines must remain open (or be reopened if they closed as a result of the initiating transient). Further, the turbine bypass line must open. If condenser vacuum falls below seven inches of Hg, the low vacuum interlocks on the bypass valves must be over-ridden.

---

[1] These pump combinations are identical to that required for a large LOCA and were selected in an attempt to be conservative.

3. At least one of the main condenser circulating pumps must be operable and delivering cooling water to the main condenser.

References

1. "Pressurized Water Reactor Loss of Coolant Accident by Hypothetical Vessel Rupture", by P. L. Doan, ScD. Thesis, Department of Nuclear Engineering, MIT, dated August 1972.

2. "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Cooled Nuclear Power Reactors," U. S. Atomic Energy Commission, Washington, D. C. 20545, Docket No. RM-50-1, December 28, 1973.

3. Evaluation of Nuclear Power Plant Availability OOE-ES-001, USAEC Office of Operations Evaluation, January 1974.

4. WASH 1270.

5. Michelotti, L. A., "Analysis of Anticipated Transients Without Scram", General Electric, APED, NEDO-10349 (March, 1971).

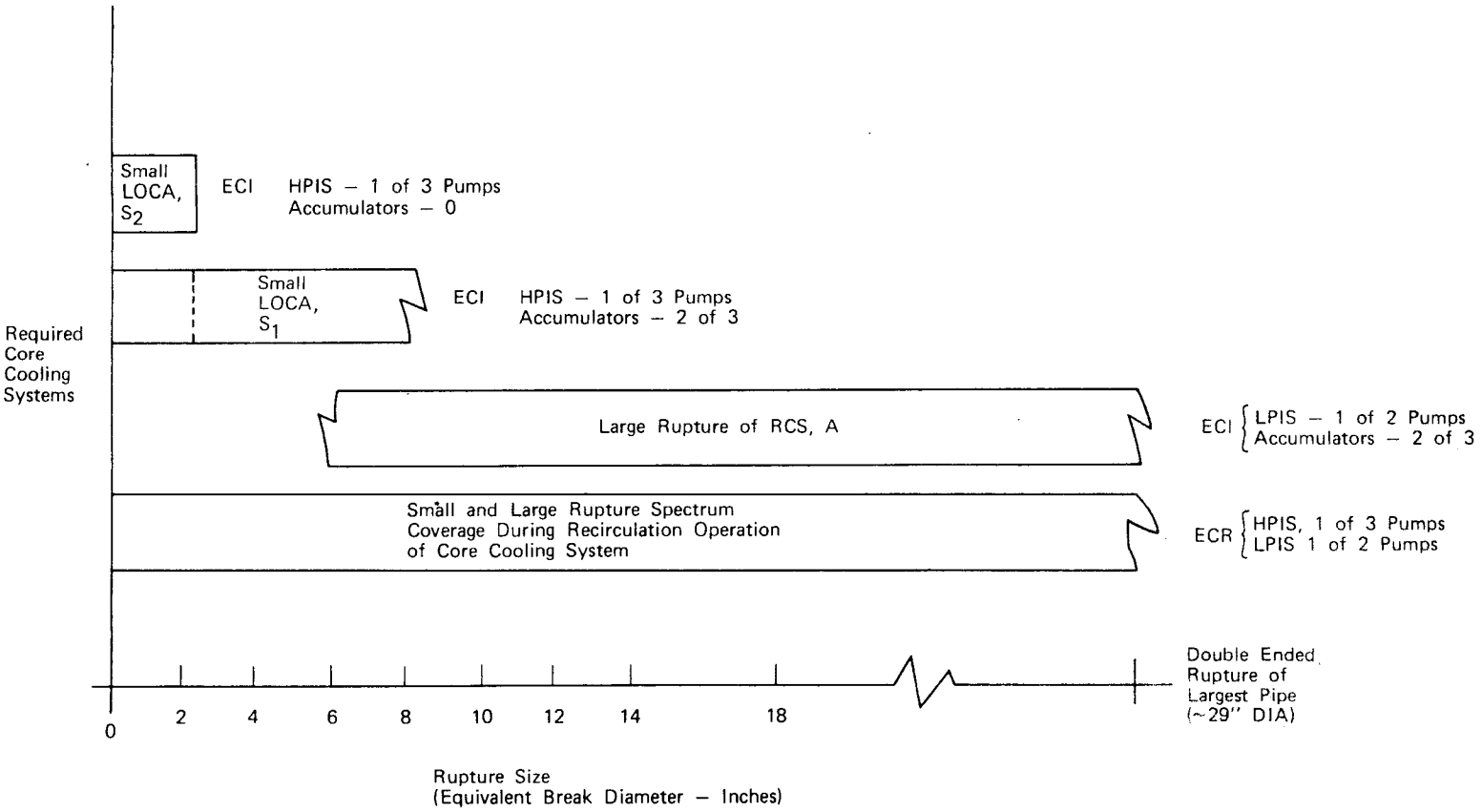


FIGURE I 4-1 Core Cooling Systems Combinations Required to Operate for Core Protection Following Various Size Ruptures of Reactor Coolant Systems

TABLE I 4-1 FOOTNOTES

(a) Failure to remove heat through the recirculation spray heat exchangers causes the containment to pressurize and ultimately to fail due to the almost adiabatic addition of decay heat to the containment atmosphere. As discussed in Appendix VIII, containment failure is predicted to occur at a pressure of about 100 psi. Since the water in the containment sump will be at the saturation temperature associated with the partial pressure of steam within containment, the rapid depressurization which occurs upon containment failure will cause the water in the sump to flash and cause cavitation of the CSRS and LPRS pumps. It is assumed that this cavitation will damage the pumps, preventing operation of either the CSR or LPR systems following containment failure.

(b) Note CSRS and SHA are available only prior to the occurrence of core melt.

(c) For this sequence, containment failure causes eventual core melt. A steam explosion, which occurs as the molten fuel drops into the residual water in the lower pressure vessel head, will increase the "puff" release of activity from the already failed containment.

(d) Independent LPRS failure. Loss of heat removal through a failure of the recirculation spray heat exchangers leads to containment overpressurization. Containment failure may occur because of such overpressurization or because of the interactions with the molten core and melt-through.

(e) Since the emergency core cooling injection system does not function to cool the core, core meltdown will result. Success of LPRS will have no effect on core damage since melting would be in progress when LPRS is available.

(f) If the emergency core cooling injection system fails to operate, the question of functionability is moot. Since core meltdown results if ECI fails, LPRS operation would not succeed in preventing the core melt.

(g) Failure of CSIS and CSRS eliminate all means of reducing containment pressure or washing fission products from the containment atmosphere.

(h) Partial ECI operation is required in order to inject NaOH into the water used in the CSRS system.

(i) EP failure prevents operation of other systems.

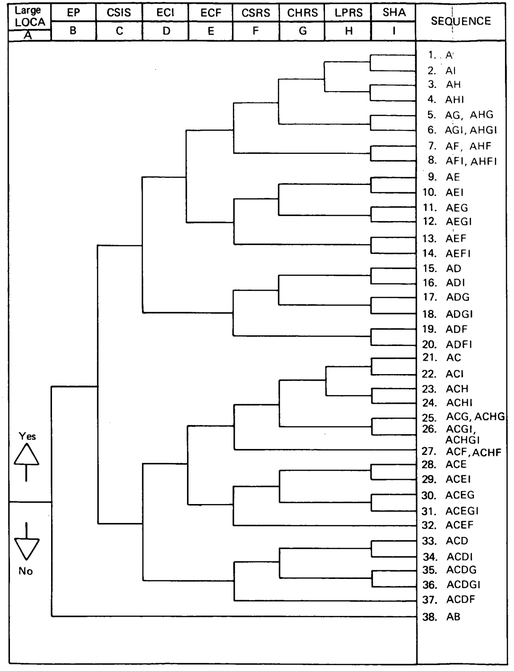


FIGURE I 4-2 PWR Large LOCA Event Tree

TABLE I 4-1 PWR LARGE LOCA SYSTEMS STATUS AND CONTAINMENT FAILURE MODES

SEQUENCE	SNO	A LPB	B EP	C CSIS	D ECI	E ECF	F CSRS	G CHRS	H LPRS	I SHA	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	FOOT NOTES
A	1	f									N		X				DBA
AI	2	f								f	N		X				
AH	3	f							f		Y	X	X			X	
AHI	4	f							f	f	Y	X	X			X	
AG	5a	f					f_G	f	f_G	O_F	Y	X			X		a,b,c
AHG	5b	f					f_G	f	f_G	f_F	Y	X	X		X	X	d
AGI	6a	f					f_G	f	f_G	f	Y	X			X		a,b,c
AHGI	6b	f					f_G	f	f	f	Y	X	X		X	X	d
AF	7a	f						O_F	f_F	f_F	Y	X			X		a,b,c
AHF	7b	f						O_F	f	f_F	Y	X	X	X	X	X	d
AFI	8a	f						O_F	f	f_F	Y	X			X		a,c
AHFI	8b	f						O_F	f	f	Y	X	X	X	X	X	d
AE	9	f				f			O_E		Y	X	X			X	e
AEI	10	f				f			O_E	f	Y	X	X			X	e
AEG	11	f				f	f_G	f	O_E	f_F	Y	X	X		X	X	a,e
AEGI	12	f				f	f_G	f	O_E	f_F	Y	X	X		X	X	a,e
AEF	13	f				f	f_G	O_F	O_E	f_F	Y	X	X		X	X	d,e
AEFI	14	f				f	f	O_F	O_E	f	Y	X	X		X	X	a,e
AD	15	f			f	O_D			O_D		Y	X	X			X	f
ADI	16	f			f	O_D			O_D	f	Y	X	X			X	f
ADG	17	f			f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	a,f
ADGI	18	f			f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	a,f
ADF	19	f			f	O_D	f	O_F	O_D	f_F	Y	X	X		X	X	a,f
ADFI	20	f			f	O_D	f	O_F	O_D	f	Y	X	X			X	a,f
AC	21	f		f							N		X				
ACI	22	f		f						f	N		X				
ACH	23	f		f					f		Y	X	X			X	
ACHI	24	f		f					f	f	Y	X	X			X	
ACG	25a	f		f			f_G	f	f_G	O_F	Y	X			X		a,b,c
ACHG	25b	f		f			f_G	f	f_G	f_F	Y	X	X		X	X	d
ACGI	26a	f		f			f_G	f	f	f	Y	X			X		a,b,c
ACHGI	26b	f		f			f_G	f	f	f	Y	X	X		X	X	d
ACF	27a	f		f			f_G	O_F	f_F	O_{CF}	Y	X			X		a,c,g
ACHF	27b	f		f			f	O_F	f	O_{CF}	Y	X	X	X	X	X	d
ACE	28	f		f		f			O_E	f	Y	X	X			X	e
ACEI	29	f		f		f			O_E	f	Y	X	X			X	e
ACEG	30	f		f		f	f_G	f	O_E	f_F	Y	X	X		X	X	a,e
ACEGI	31	f		f		f	f_G	f	O_E	f_F	Y	X	X		X	X	a,e
ACEF	32	f		f		f	f	O_F	O_E	O_{CF}	Y	X	X	X	X	X	e,g
ACD	33	f		f	f	O_D			O_D		Y	X	X			X	f,h
ACDI	34	f		f	f	O_D			O_D	f	Y	X	X			X	f
ACDG	35	f		f	f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	a,f,h
ACDGI	36	f		f	f	O_D	f_G	f	O_D	f	Y	X	X		X	X	a,f
ACDF	37	f		f	f	O_D	f_G	O_F	O_D	O_{CF}	Y	X	X	X	X	X	f,h
AB	38	f	f	Z_B	Z_B	O_D	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	i

Key: f – FAILURE
f_N – DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N – DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" FAILURE
Z_N – FAILURE PREDICATED BY FAILURE OF "N"
Y – YES
N – NO
X – POTENTIAL CONTAINMENT VESSEL FAILURE MODE

FOOTNOTES ON APRON

TABLE I 4-2 PWR LARGE LOCA EVENT TIMING(d)

Sequence	Start Boiloff min	Core Melting Time, min Start	Core Melting Time, min End(a)	Core Melting Pressure, psia w/o H_2 Comb.(b)	Core Melting Pressure, psia w/ H_2 Comb.(b)	Reactor Vessel Melt-through Time, min	Reactor Vessel Melt-through Pressure, psis	Containment Overpressure Failure min	Containment Melt-through Start min(c)	Containment Melt-through Pressure psis	Containment Melt-through End, min	Containment Melt-through Pressure, psis
A	--	--	--	--	--	--	--	--	--	--	--	--
AI	--	--	--	--	--	--	--	--	--	--	--	--
AH	60	100	150	16		13	210	16	--	230	18	1290	29
AHI	60	100	150	16		13	210	16	--	230	18	1290	29
AG	1290	1370	1490	15		15	1610	15	1290	1630	15	3800	15
AGI	1290	1370	1490	15		15	1610	15	1290	1630	15	3800	15
AHG	60	100	150	16		17	210	16	1280	230	18	1290	100
AHGI	60	100	150	16		17	210	16	1280	230	18	1290	100
AF	530	590	670	15		15	760	15	530	790	15	2400	15
AFI	530	590	670	15		15	760	15	530	790	15	2400	15
AHF	60	100	150	46		65	210	40	230	230	80	1290	45
AHFI	60	100	150	46		65	210	40	230	230	80	1290	45
AE	1	16	60	14		11	120	16	--	140	18	1200	29
AEI	1	16	60	14		11	120	16	--	140	18	1200	29
AEG	1	16	60	15		22	120	16	1280	140	18	1200	94
AEGI	1	16	60	15		22	120	16	1280	140	18	1200	94
AEF	1	16	60	16		24	120	16	--	140	18	1200	50
AEFI	1	16	60	16		24	120	16	--	140	18	1200	50
AD	1	16	60	14		11	120	16	--	140	18	1200	29
ADI	1	16	60	14		11	120	16	--	140	18	1200	29
ADG	1	16	60	15		22	120	16	1230	140	18	1200	94
ADGI	1	16	60	15		22	120	16	1230	140	18	1200	94
ADF	1	16	60	16		24	120	16	--	140	18	1200	50
ADFI	1	16	60	16		24	120	16	--	140	18	1200	50
AC	--	--	--	--		--	--	--	--	--	--	--	--
ACI	--	--	--	--		--	--	--	--	--	--	--	--
ACH	120	170	220	16		13	280	16	--	300	18	1360	25
ACHI	120	170	220	16		13	280	16	--	300	18	1360	25
ACG	1290	1370	1490	15		15	1610	15	1290	1630	15	3800	15
ACGI	1290	1370	1490	15		15	1610	15	1290	1630	15	3800	15
ACHG	120	170	220	16		17	280	22	1280	300	24	1360	107
ACHGI	120	170	220	16		17	280	22	1280	300	24	1360	107
ACF	240	290	360	15		15	440	15	240	460	15	1900	15
ACHF	120	170	220	105		130	280	95	200	300	110	1360	75
ACE	1	16	60	43		55	120	16	--	140	18	1200	29
ACEI	1	16	60	43		55	120	16	--	140	18	1200	29
ACEG	1	16	60	43		55	120	16	1280	140	22	1200	94
ACEGI	1	16	60	43		55	120	16	1280	140	22	1200	94
ACEF	1	16	60	75		100	120	65	60	140	75	1200	60
ACD	1	16	60	43		55	120	16	--	140	18	1200	29
ACDI	1	16	60	43		55	120	16	--	140	18	1200	29
ACDG	1	16	60	43		55	120	16	1200	140	24	1200	100
ACDGI	1	16	60	43		55	120	16	1200	140	24	1200	100
ACDF	1	16	60	75		100	120	65	60	140	75	1200	60
AB	1	16	60	75		100	120	65	60	140	75	1200	60

(a) End of core melting is taken as ~80 percent of the core molten.
(b) Assuming the hydrogen from the reaction of 75 percent of the cladding with steam burns as it is generated.
(c) After the initial rapid interaction of the molten core with concrete.
(d) Additional detail on the engineering assumptions and calculations for the event timing and containment failure mode probabilities can be found in Appendices V and VIII.

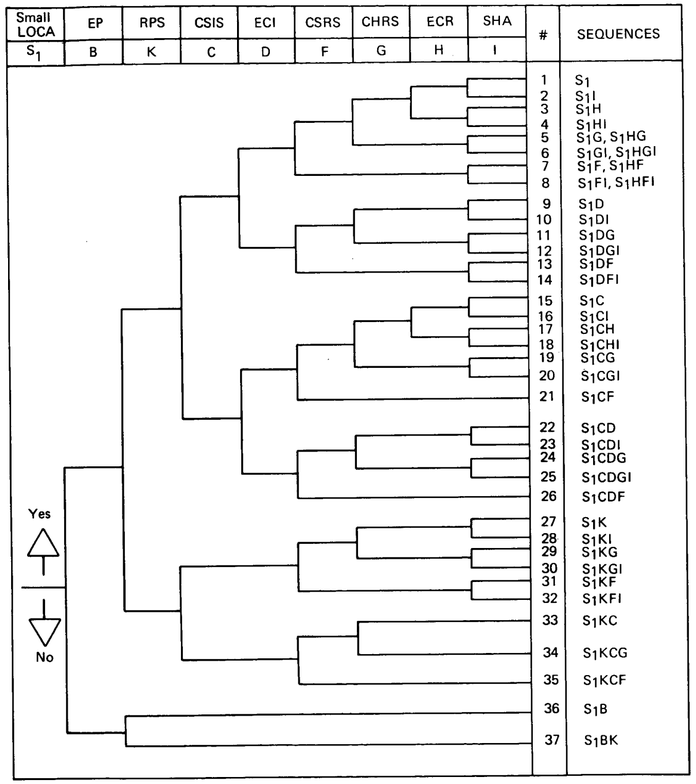


FIGURE I 4-3 PWR Small LOCA (Sl, 2-6 inch diameter) in RCS

TABLE I 4-3 PWR SMALL LOCA (S_1) SYSTEM STATUS AND CONTAINMENT FAILURE MODES

SEQUENCE	SNO	Sl	B EP	K RPS	C CSIS	D ECI	F CSRS	G CHRS	H ECR	I SHA	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	FOOT NOTES
S_1	1	f									N		X				
S_1I	2	f								f	N		X				
S_1H	3	f							f		Y	X	X			X	
S_1HI	4	f							f	f	Y	X	X			X	
S_1G	5a	f					f_G	f	f_G	O_G	Y	X			X		a, b, c, g
S_1HG	5b	f					f_G	f	f_G	O_G	Y	X	X		X	X	d
S_1GI	6a	f					f_G	f	f_G	f	Y	X			X		a, b, c
S_1HGI	6b	f					f_G	f	f_G	f	Y	X	X		X	X	d
S_1F	7a	f					f	O_F	f	O_F	Y	X			X		e, f, g
S_1HF	7b	f					f	O_F	f	f_G	Y	X	X		X	X	d, e, g
S_1FI	8a	f					f	O_F	f_F	f	Y	X			X		a
S_1HFI	8b	f					f	O_F	f	f	Y	X	X		X	X	a, e
S_1D	9	f				f			O_D		Y	X	X			X	h
S_1DI	10	f				f			O_D	f	Y	X	X			X	h
S_1DG	11	f				f		f	O_D		Y	X	X		X	X	h
S_1DGI	12	f				f		f	O_D	f	Y	X	X		X	X	h
S_1DF	13	f				f	f	O_F	O_D		Y	X	X		X	X	a, e, h
S_1DFI	14	f				f	f			f	Y	X	X		X	X	
S_1C	15	f			f						N		X				
S_1CI	16	f			f					f	N		X				
S_1CH	17	f			f				f		Y	X	X			X	
S_1CHI	18	f			f				f	f	Y	X	X			X	
S_1CG	19a	f			f		f_G	f	f_G	O_F	Y	X			X		a, b, c, g
S_1CHG	19b	f			f		f_G	f	f	f_G	Y	X	X		X	X	d
S_1CGI	20a	f			f		f_G	f	f_G	f	Y			X	X		a, b, c, g
S_1CHGI	20b	f			f		f_G	f	f_G	f	Y	X	X		X	X	d
S_1CF	21a	f			f		f	O_F	f_F	O_F	Y			X	X		a, b, c, g
S_1CHF	21b	f			f		f	O_F	f_F	O_F	Y	X	X	X	X	X	d
S_1CD	22	f			f	f			O_D		Y	X	X			X	h
S_1CDI	23	f			f	f			O_D	f	Y	X	X			X	h
S_1CDG	24	f			f	f		f	O_D		Y	X	X		X	X	h
S_1CDGI	25	f			f	f		f	O_D	f	Y	X	X		X	X	h
S_1CDF	26	f			f	f	f	O_F	O_D	O_{CF}	Y	X	X	X	X	X	e, h, i
S_1K	27	f		f		O_K			O_K		Y	X	X			X	j
S_1KI	28	f		f		O_K			O_K	f	Y	X	X			X	j
S_1KG	29	f		f		O_K		f	O_K		Y	X	X		X	X	j
S_1KGI	30	f		f		O_K		f	O_K	f	Y	X	X		X	X	j
S_1KF	31	f		f		O_K	f	O_F	O_K		Y	X	X		X	X	e, j
S_1KFI	32	f		f		O_K	f	O_F	O_K	f	Y	X	X		X	X	e, j
S_1KC	33	f		f	f	O_K			O_K	O_{CD}	Y	X	X			X	i, k
S_1KCG	34	f		f	f	O_K		f		O_{CD}	Y	X	X		X	X	i, k
S_1KCF	35	f		f	f		f	O_F	O_K	O_{CF}	Y	X	X	X	X	X	i, j
S_1B	36	f	f		Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	l
S_1BK	37	f	f	f	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	l, m

KEY: f - FAILURE
f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF FAILURE OF "N"
Z_N - FAILURE PREDICATED BY FAILURE OF "N"
Y - YES
N - NO
X - POTENTIAL CONTAINMENT VESSEL FAILURE MODE

TABLE I 4-3 FOOTNOTES

(a) Failure of CHRS leads to containment failure at high pressures. The subsequent flashing of high temperature water in the sump results in CSRS and ECR pump cavitation, rendering CSRS and ECR inoperable.

(b) CSRS and SHA are available only prior to the occurrence of core melt.

(c) Containment failure causes eventual core melt. A steam explosion which occurs as the molten fuel drops into the residual water in the lower head of the pressure vessel will increase the "puff" release of activity from the already failed containment.

(d) Independent ECR failure. ECR fails prior to containment failure due to depressurization.

(e) Failure of CSRS prevents delivery of sump water to the CHRS heat exchangers; therefore, operation of CHRS has no effects.

(f) Failure of CSRS leads to containment failure at high pressure. The resultant flashing of high temperature sump water cavitates the ECR pumps.

(g) Failure of CSRS prevents the spray of NaOH through the containment atmosphere following core melt. Therefore, SHA operation does not matter.

(h) Failure of ECI to operate obviates the need for ECR.

(i) Failure of CSIS and CSRS prevents spray operation, eliminating the need for SHA.

(j) Failure of RPS leads to core melt regardless of ECI or ECR operation.

(k) Failure of CSIS and ECI prevents NaOH addition to containment.

(l) EP failure prevents operation of other systems.

(m) Failure of RPS, given EP failure, results from mechanical failures only.

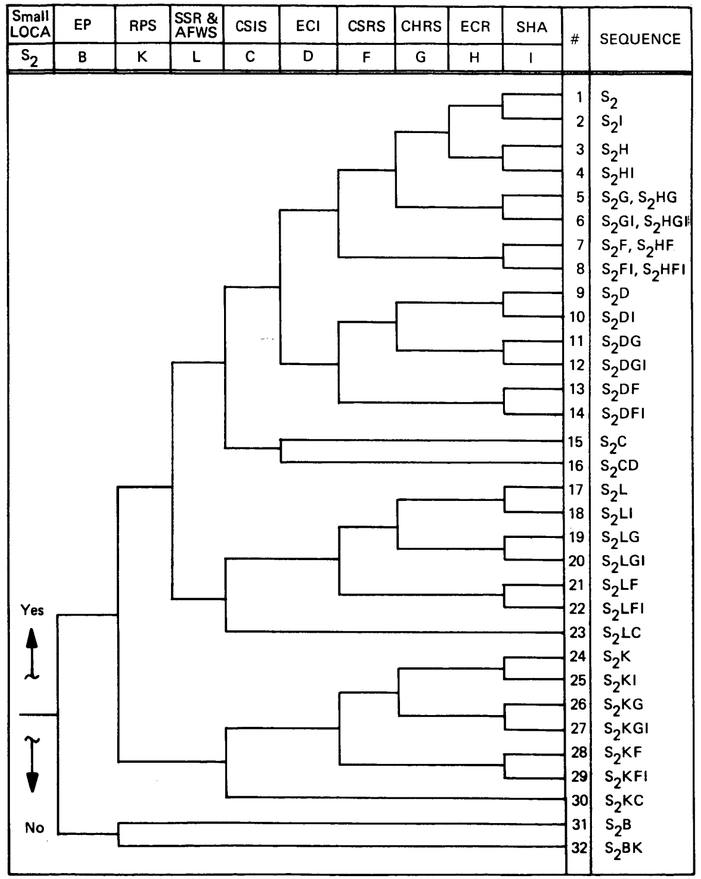


FIGURE I 4-4 PWR Small LOCA (S2, 1/2-2 inch diameter) in RCS

TABLE I 4-4 PWR SMALL LOCA (S2) SYSTEM STATUS AND CONTAINMENT FAILURE MODES

SEQUENCE	SNO	S2	B EP	K RT	L SSR& AFW	C CSIS	D ECI	F CSRS	G CHRS	H ECRS	I SHA	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	FOOT NOTES
S_2	1	f										N		X				
S_2I	2	f									f	N		X				
S_2H	3	f								f		Y	X	X			X	
S_2HI	4	f								f	f	Y	X	X			X	
S_2G	5a	f						f_G	f	f_G	O_G	Y	X			X		a, b, c
S_2HG	5b	f						f_G	f	f^*	f_G	Y	X	X		X	X	d
S_2GI	6a	f						f_G	f	f_G	f^*	Y	X			X		a, b, c
S_2HGI	6b	f						f_G	f	f^*	f	Y	X	X		X	X	d
S_2F	7a	f						f^*	O_F	f_F	O_F	Y	X			X		e, f, g
S_2HF	7b	f						f	O_F	f^*	f_F	Y	X	X		X	X	d, e, g
S_2FI	8a	f						f	O_F	f_F	f^*	Y	X			X		e, f
S_2HFI	8b	f						f	O_F	f^*	f	Y	X	X		X	X	e
S_2D	9	f					f			O_D		Y	X	X			X	h
S_2DI	10	f					f			O_D	f	Y	X	X			X	h
S_2DC	11	f					f		f	O_D		Y	X	X		X	X	h
S_2DGI	12	f					f		f	O_D	f	Y	X	X		X	X	h
S_2DF	13	f					f	f	O_F	O_D		Y	X	X		X	X	e, h
S_2DFI	14	f					f	f	O_F	O_D	f	Y	X	X		X	X	e, h
S_2C	15	f				f		Z_C	O_F	Z_C	O_{CF}	Y	X	X	X	X	X	e, i, n
S_2CD	16	f				f	f	Z_C	O_F	O_D	O_{CF}	Y	X	X	X	X	X	e, i, k, n
S_2L	17	f			f		O_L			O_L		Y	X	X			X	o
S_2LI	18	f			f		O_L			O_L	f	Y	X	X			X	o
S_2LG	19	f			f		O_L		f	O_L		Y	X	X		X	X	o
S_2LGI	20	f			f		O_L		f	O_L	f	Y	X	X		X	X	o
S_2LF	21	f			f		O_L	f	O_F	O_L		Y	X	X		X	X	e, o
S_2LFI	22	f			f		O_L	f	O_F	O_L	f	Y	X	X		X	X	e, o
S_2LC	23	f			f	f	O_L	Z_C	O_C	O_L	O_C	Y	X	X	X	X	X	e, g, n, o
S_2K	24	f		f	O_K		O_K			O_K		Y	X	X			X	j
S_2KI	25	f		f	O_K		O_K			O_K	f	Y	X	X			X	j
S_2KG	26	f		f	O_K		O_K		f	O_K		Y	X	X		X	X	j
S_2KGI	27	f		f	O_K		O_K		f	O_K	f	Y	X	X		X	X	j
S_2KF	28	f		f	O_K		O_K	f	O_F	O_K		Y	X	X		X	X	e, j
S_2KFI	29	f		f	O_K		O_K	f	O_F	O_K	f	Y	X	X		X	X	e, j
S_2KC	30	f		f	O_K	f	O_K	Z_C	O_C	O_K	O_C	Y	X	X	X	X	X	n, o
S_2B	31	f	f		Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	l
S_2BK	32	f	f	f	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	l, m

KEY: f - FAILURE
f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF FAILURE OF "N"
Z_N - FAILURE PREDICATED BY FAILURE OF "N"
Y - YES
N - NO
X - POTENTIAL CONTAINMENT VESSEL FAILURE MODE

TABLE I 4-4 FOOTNOTES

(a) Failure of CHRS leads to containment failure at high pressures. The subsequent flashing of high temperature water in the sump results in CSRS and ECR pump cavitation, rendering CSRS and ECR inoperable.

(b) CSRS and SHA are available only prior to the occurrence of core melt.

(c) Containment failure causes eventual core melt. A steam explosion which occurs as the molten fuel drops into the residual water in the lower head of the pressure vessel will increase the "puff" release of activity from the already failed containment.

(d) Independent ECR failure. ECR fails prior to containment failure due to depressurization.

(e) Failure of CSRS prevents delivery of sump water to the CHRS heat exchangers; therefore, operation of CHRS has no effects.

(f) Failure of CSRS leads to containment failure at high pressure. The resultant flashing of high temperature sump water cavitates the ECR pumps.

(g) Failure of CSRS prevents the spray of NaOH through the containment atmosphere following core melt. Therefore, SHA operation does not matter.

(h) Failure of ECI to operate obviates the need for ECR.

(i) Failure of CSIS and CSRS prevents spray operation, eliminating the need for SHA.

(j) Failure of RT leads to core melt regardless of ECI or ECR operation.

(k) Failure of CSIS and ECI prevents NaOH addition to containment.

(l) EP failure prevents operation of other systems.

(m) Failure of RT given EP failure results from mechanical failures for the rods only.

(n) Failure of CSIS prevents the addition of large quantities of borated water to the containment. Since only a small portion of the reactor coolant system inventory leaks to the sump, sufficient elevation head is not available and LPRS and CSRS pump cavitation will occur.

(o) Failure to dissipate decay heat through the secondary system results in the reactor coolant pressure increasing to the safety valve setting. Upon opening of the RCS safety valves, the reactor coolant system water inventory cannot be maintained and a core melt eventually follows. The ECCS cannot operate against the system pressures anticipated.

RVR	EP	CSIS	CSRS	CHRS	SEQUENCE	Comparable Large LOCA Sequence (1)
R	B	C	F	G		
					R	AD
					RG	ADG
					RF	ADF
					RC	ACDF
					RB	AB

(1) Refer to Section 4.1.1 for the sequences coupling with Containment Event Tree.

FIGURE I 4-5 Event Tree for PWR Reactor Vessel Rupture

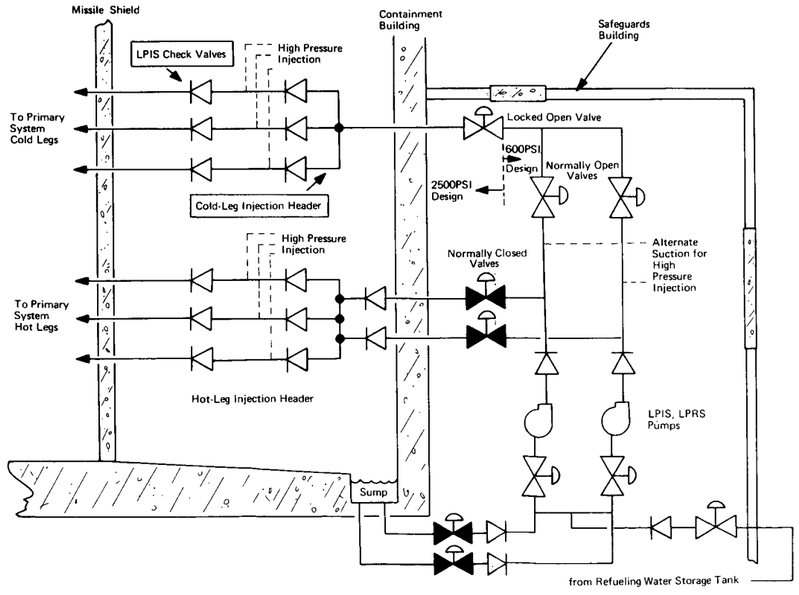


FIGURE I 4-6 Low Pressure Recirculation System Schematic Diagram

LPIS Check Valve Rupture	EP	RPS	ECI	#	SEQ	CORE
V	B	K	D			
				1	V	M
				2	VD	M
				3	VK	M
				4	VB	M

FIGURE I 4-7 LPIS Check Valve Rupture Event Tree

TABLE I 4-5 FOOTNOTES

(a) Failure to remove heat through the residual heat removal heat exchangers causes the containment to pressurize and ultimately to fail due to the almost adiabatic addition of decay heat to the containment atmosphere. As discussed in Appendix VIII, containment failure is predicted to occur at a pressure of about 177 psia. Since the water in the suppression pool will be at the saturation temperature associated with the partial pressure of the steam within the containment, the rapid depressurization which occurs upon containment failure will cause the water in the suppression pool to flash and cause cavitation of the LPCI and CS pumps. These pumps will then have insufficient NPSH to continue operating. Hence, the core will not be maintained in a reflooded condition, the water remaining the core region will be vaporized, and the core will melt.

(b) With both CSRS and LPCRS failed independently, the core is not maintained in a reflooded condition. The water in core region will be vaporized and the core will melt.

(c) Without heat removal through the residual heat removal heat exchangers, the temperature of the water in the suppression pool will increase. Since the containment has a leakage of greater than 100% per day, the LPCI and CS pumps will have inadequate NPSH to continue operating after 4 to 26 hours, depending on the magnitude of the containment leakage. Hence, the core will subsequently melt.

(d) Since the emergency core cooling injection system does not function to cool the core, core meltdown will result. Success of LPCRS and CSRS will have not effect on core damage since melting would be in progress when these systems were operating.

(e) Since the mergency core cooling injection system fails to operate successfully, it is assumed that core meltdown will result. Success of LPCRS and CSRS will have no effect on core damage since melting would be in progress when these systems were operating.

(f) The emergency core cooling injection system fails to provide any water to the core. Therefore, the LPCI and CS pumps are, by definition, inoperable in the recirculation mode. The core melts in a dry atmosphere. There is no water in the lower pressure vessel plenum; therefore, a steam explosion in the reactor vessel cannot occur.

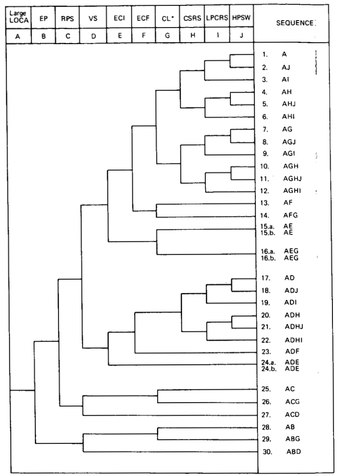
(g) If the emergency core cooling injection system fails to operate, the question of functionability is moot.

(h) Without heat removal through the residual heat removal heat exchangers, the temperature of the water in the suppression pool will increase. The failure or vapor suppression causes a massive failure of the containment structure and a high leakage rate. The LPCI and CS pumps will have inadequate NPSH after about 7 hours and the core will melt.

(i) With a large LOCA and no scram, the low pressure ECCS will attempt to reflood the core. The resulting rapid increase in reactor power, once the core reaches criticality, might result in a vessel failure or might cause the reactor to "chug" (go from subcritical to some significant power level and back to subcritical) for some period of time. This is assumed to eventually result in massive fuel cladding failures and/or a core melt.

(j) A steam explosion which may occur as the molten fuel drops into the retained water in the lower pressure vessel plenum. This will fail the containment, if it has not already failed, and will significantly increase the release of radioactive material to the environment.

(k) A steam explosion may occur as the molten core melts through the reactor vessel and drops into the water that would be remaining at the bottom of the drywell immediately below the reactor vessel. This is a possible mechanism that will result in containment failure. If a steam explosion in the containment occurs, the containment will fail sooner than it would have due to overpressurization from non-condensible gases. If containment isolation has not been successful, a containment steam explosion will increase the containment leak rate and will result in a greater release of fission products.



*leakage less than 100%/day

FIGURE I 4-8 BWR Large LOCA Event Tree

TABLE I 4-5 BWR LARGE LOCA SYSTEMS STATUS AND CONTAINMENT FAILURE MODES

SEQUENCE	SNO	A LKRCS	B EP	C RPS	D VS	E ECI	F ECF	G CL	H CSRS	I LPCRS	J HPSW	CORE MELT	q	s	y	δ	ε	cc	cn	c0	δc	δn	δ0	FOOTNOTES
A	1	f									N													
AJ	2	f								f_J	f	Y	X		X									a, j
AI	3	f								f^I	O_J	Y	X		X									a, j
AH	4	f							f			N												
AHJ	5	f							f	f_J	f	Y	X		X									a, j
AHI	6	f							f	f^I	O_I	Y	X	X										b, j, k
AG	7	f						f				N												
AGJ	8	f						f		f_J	f	Y	X		X	X		X	X	X	X	X	X	c, j, k
AGI	9	f						f		f^J	O_J	Y	X		X	X		X	X	X	X	X	X	c, j, k
AGH	10	f						f	f			N												
AGHJ	11	f						f	f	f_J	f	Y	X		X	X		X	X	X	X	X	X	c, j, k
AGHI	12	f						f	f	f^J	O_I	Y	X		X	X		X	X	X	X	X	X	b, j, k
AF	13	f				f			O_E	O_E		Y	X	X										c, j, k
AFG	14	f				f	f		O_E	O_E		Y	X	X		X	X	X	X	X	X	X	X	d, j, k
AE	15a	f			f	O_E			z_E	z_E		Y	X	X										e, g, j, k
AE	15b	f			f	O_E			z_E	z_E		Y	X	X										f, g, k
AEG	16a	f			f	O_E	f		O_E	O_E		Y	X	X		X	X	X	X	X	X	X	X	e, g, j, k
AEG	16b	f			f	O_E	f		z_E	z_E		Y	X	X		X	X	X	X	X	X	X	X	e, g, k
AD	17	f		f			z_D					N												
ADJ	18	f		f			z_D			f_J	f	Y	X		X									h, j
ADI	19	f		f			z_D			f_J	O_I	Y	X		X									h, j
ADH	20	f		f			z_D	f				N												
ADHJ	21	f		f			z_D	f		f_J	f	Y	X		X									h, j
ADHI	22	f		f			z_D	f		f^J	O_I	Y	X		X									b, j
ADF	23	f		f		f	z_D	O_E		O_E		Y	X		X									d, j
ADE	24a	f		f	f	O_E	z_D	O_E		O_E		Y	X		X									e, g, j
ADE	24b	f		f	f	O_E	z_D	O_E		O_E		Y			X									f, g
AC	25	f	f					f				Y	X	X										i, j, k
ACG	26	f	f					f				Y	X	X		X	X	X	X	X	X	X	X	i, j, k
ACD	27	f	f	f				f				Y	X		X									f, j
AB	28	f	f			z_B	O_E	z_D	z_B	z_B	z_B	Y	X	X										f, g, k
ABG	29	f	f			z_B	O_E	f	z_B	z_B	z_B	Y	X		X	X									f, g, k
ABD	30	f	f		f	z_B	O_E	z_D	z_B	z_B	z_B	Y	X		X									f, g

KEY: f – FAILURE
f_N – DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N – DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" FAILURE
z_N – FAILURE PREDICATED BY FAILURE OF "N"
Y – YES
N – NO
X – POTENTIAL CONTAINMENT FAILURE MODE

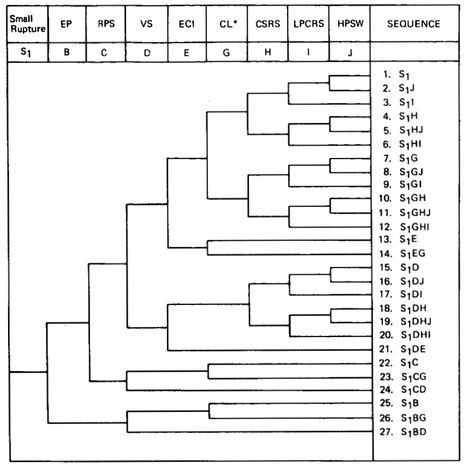
FOOTNOTES ON APRON

TABLE I 4-6 BWR LARGE LOCA EVENT TREE (c)

Sequence	Core Melting Start, min	Core Melting End, (a) min	Reactor Vessel Melt-through Pressure, psia	Reactor Vessel Melt-through Time, min	Containment Overpressure Pressure, psia	Containment Overpressure Failure, min	Containment Melt-through Start, (b) min	Containment Melt-through Pressure, psia	Containment Melt-through End, min
1. A	--	--	--	--	--	--	--	--	--
2. AJ	1520	1640	15	1730	15	1500	1750	15	5000
3. AI	1520	1640	15	1730	15	1500	1750	15	5000
4. AH	--	--	--	--	--	--	--	--	--
5. AHJ	1520	1640	15	1730	15	1500	1750	15	5000
6. AHI	20	80	52	140	128	220	160	165	2000
7. AG	--	--	--	--	--	--	--	--	--
8. AGJ	270	330	15	390	15	--	410	15	2500
9. AGI	270	330	15	390	15	--	410	15	2500
10. AGH	--	--	--	--	--	--	--	--	--
11. AGHJ	270	30	15	390	15	--	410	15	2500
12. AGHI	20	80	24	140	19	--	160	34	2000
13. AF	5	150	58	210	58	290	230	165	2000
14. AFG	5	150	18	210	16	--	230	34	2000
15.a. AE	20	150	17	210	82	640	230	107	2000
15.b. AE	20	150	17	180	17	640	200	107	2000
16.a. AEG	20	150	15	210	42	--	230	66	2000
16.b. AEG	20	150	15	180	15	--	200	66	2000
17. AD	--	--	--	--	--	--	--	--	--
18. ADJ	420	510	15	600	15	0.5	620	15	3000
19. ADI	420	510	15	600	15	0.5	620	15	3000
20. ADH	--	--	--	--	--	--	--	--	--
21. ADHJ	420	510	15	600	15	0.5	620	15	3000
22. ADHI	20	80	15	140	15	0.5	160	15	2000
23. ADF	5	150	15	210	15	0.5	230	15	2000
24.a. ADE	20	150	15	210	15	0.5	230	15	2000
24.b. ADE	20	150	15	180	15	0.5	200	15	2000
25. AC	5	150	58	210	58	290	230	165	2000
26. ACG	5	150	18	210	16	--	230	34	2000
27. ACD	5	150	15	210	15	0.5	230	15	2000
28. AB	20	150	17	180	17	640	200	107	2000
29. ABC	20	150	15	180	15	--	200	66	2000
30. ABD	20	150	15	180	15	0.5	200	15	2000

(a) End of core melting is taken as ~80 percent molten.
(b) After the initial rapid interaction between the molten core and concrete.
(c) Added detail on the engineering assumptions and calculations for the event timing and containment failure mode probabilities can be found in Appendicies V and VIII.

Fig. I 4-8
Table I 4-5 – Table I 4-6



*Containment Leakage less than 100%/day.

FIGURE I 4-9 BWR Small LOCA (S1, approximately 2.5-8 inch diameter) in RCS

TABLE I 4-7 BWR SMALL LOCA S_1 SYSTEMS STATUS AND CONTAINMENT FAILURE MODES

SEQUENCE	SNO	S_1 LOCA	B EP	C RPS	D VS	E ECI	G CL	H CSRS	I LPCRS	J HPSW	CORE MELT	α	β	γ	δ	ε	εξ	εη	εθ	δξ	δη	δθ	FOOTNOTES
S_1	1	f									N												
S_1J	2	f						f_J	f_J	f	Y	X		X									a, g
S_1I	3	f								O_I	Y			X									a, g
S_1H	4	f						f			N												
S_1HJ	5	f						f	f_J	f	Y	X		X									a, g
S_1HI	6	f						f	f_J	O_I	Y	X	X	X									b, g, h
S_1G	7	f					f				N												
S_1GJ	8	f					f	f_J	f_J	f	Y	X	X		X	X	X	X	X	X	X	X	c, g, h
S_1GI	9	f					f		f_J	O_I	Y	X	X		X	X	X	X	X	X	X	X	c, g, h
S_1GH	10	f					f	f			N												
S_1GHJ	11	f					f	f	f_J	f	Y	X	X		X	X	X	X	X	X	X	X	c, g, h
S_1GHI	12	f					f	f	f_J	O_I	Y	X	X		X	X	X	X	X	X	X	X	d, g, h
S_1E	13	f				f		O_E	O_E		Y	X	X	X									d, g, h
S_1EG	14	f				f	f	O_E	O_E		Y	X	X		X	X	X	X	X	X	X	X	d, g, h
S_1D	15	f			f		Z_D				N												
S_1DJ	16	f			f		Z_D	f_J	f_J	f	Y	X		X									e, g,
S_1DI	17	f			f		Z_D		f_J	O_I	Y	X		X									e, g
S_1DH	18	f			f		Z_D	f			N												
S_1DHJ	19	f			f		Z_D	f	f_J	f	Y	X		X									e, g
S_1DHI	20	f			f		Z_D	f	f_J	O_I	Y	X		X									b, g
S_1DE	21	f			f	f	Z_D	O_E	O_E		Y	X		X									d, g
S_1C	22	f		f							Y	X	X	X									f, g, h
S_1CG	23	f		f			f				Y	X	X		X	X	X	X	X	X	X	X	f, g, h
S_1CD	24	f		f	f		Z_D				Y	X		X									f, g
S_1B	25	f	f			Z_B		Z_B	Z_B	Z_B	Y	X	X	X									d, g, h
S_1BG	26	f	f			Z_B	f	Z_B	Z_B	Z_B	Y	X	X		X	X	X	X	X	X	X	X	d, g, h
S_1BD	27	f	f		f	Z_B	Z_D	Z_B	Z_B	Z_B	Y	X		X									d, g

KEY:
- f - FAILURE
- f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
- O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" FAILURE
- Z_N - FAILURE PREDICATED BY FAILURE OF "N"
- Y - YES
- N - NO
- X - POTENTIAL CONTAINMENT FAILURE MODE

TABLE I 4-7 FOOTNOTES

(a) Failure to remove heat through the residual heat removal heat exchangers causes the containment to pressurize and ultimately to fail due to the almost adiabatic addition of decay heat to the containment atmosphere. As discussed in Appendix VIII, containment failure is predicted to occur at a pressure of 177 psia. Since the water in the suppression pool will be at the saturation temperature associated with the partial pressure of steam within the containment, the rapid depressurization which occurs upon containment failure will cause the water in the suppression pool to flash and cause cavitation of the LPCI and CS pumps. These pumps will then have insufficient NPSH to continue operating. Hence, the core will not be maintained in a reflooded condition, the water remaining in the core region will be vaporized, and the core will melt.

(b) With both CSRS and LPCRS failed independently, the core is not maintained in a reflooded condition. The water in core region will be vaporized and the core will melt.

(c) Without heat removal through the residual heat removal heat exchangers, the temperature of the water in the suppression pool will increase. Since the containment has a leakage of greater than 100% per day, the LPCI and CS pumps will have inadequate NPSH to continue operating after 4 to 26 hours, depending on the magnitude of the containment leakage. Hence, the core will subsequently melt.

(d) Since the emergency core cooling injection system fails to operate successfully, it is assumed that core meltdown will result. Success of LPCRS and CSRS will have no effect on core damage since melting would be in progress when these systems were operating.

(e) Without heat removal through the residual heat removal heat exchangers, the temperature of the water in the suppression pool will increase. The failure of vapor suppression causes a massive failure of the containment structure and a high leakage rate. The LPCI and CS pumps will have inadequate NPSH after about 7 hours and the core will melt.

(f) With a small LOCA and no scram, the reactor will tend to remain at relatively high power immediately following the accident. Once steam flow to the turbine has been terminated due to the closure of the turbine stop valve or the main steam line isolation valves, the reactor pressure will increase. The increase in pressure will reduce the steam volume fraction in the core, the power level will increase, and reactor system pressure will increase further. Ultimately, the small LOCA will become a large LOCA, or the reactor vessel will fail.
With a large LOCA and no scram, the low pressure ECCS will attempt to reflood the core. The resulting rapid increase in reactor power, once the core reaches criticality, might result in a vessel failure, or might cause the reactor to "chug" (go from subcritical to some significant power level and back to subcritical) for some period of time. This is assumed to eventually result in massive fuel cladding failures and a core melt.
With a vessel failure, the ECCS system will probably not be able to prevent a core melt, either because a floodable volume is not maintained or because the ECCS lines will fail.

(g) A steam explosion may occur as the molten fuel drops into the residual water in the lower pressure vessel plenum. This will fail the containment, if it has not already failed, and will significantly increase the release of activity to the environment.

(h) A steam explosion may occur as the molten core melts through the reactor vessel and drops into the water that would be remaining at the bottom of the drywell immediately below the reactor vessel. This is a possible mechanism that will result in containment failure. If a steam explosion in the containment occurs, the containment will fail sooner that it would have due to overpressurization from non-condensible gases. If containment isolation has not been successful, a containment steam explosion will increase the containment leak rate and will result in a greater release of fission products.

TABLE I 4-8 FOOTNOTES

(a) Failure to remove heat through the residual heat removal heat exchangers causes the containment to pressurize and ultimately to fail due to the almost adiabatic addition of decay heat to the containment atmosphere. As discussed in Appendix VIII, containment failure is predicted to occur at a pressure of 177 psia. Since the water in the suppression pool will be at the saturation temperature associated with the partial pressure of steam within the containment, the rapid depressurization which occurs upon containment failure will cause the water in the suppression pool to flash and cause cavitation of the LPCI and CS pumps. These pumps will then have insufficient NPSH to continue operating. Hence, the core will not be maintained in a reflooded condition, the water remaining in the core region will be vaporized, and the core will melt.

(b) With both CSRS and LPCRS failed independently, the core is not maintained in a reflooded condition. The water in core region will be vaporized and the core will melt.

(c) Without heat removal through the residual heat removal heat exchangers, the temperature of the water in the suppression pool will increase. Since the containment has a leakage of greater than 100% per day, the LPCI and CS pumps will have inadequate NPSH to continue operating after 4 to 26 hours, depending on the magnitude of the containment leakage. Hence, the core will subsequently melt.

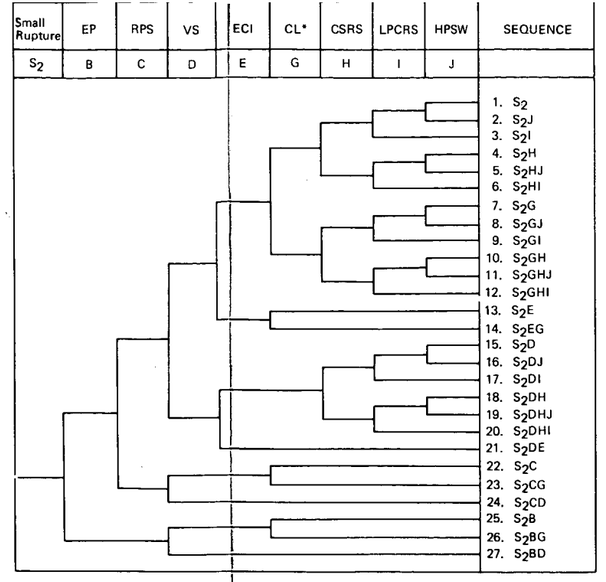
(d) Since the emergency core cooling injection system fails to operate successfully, it is assumed that core meltdown will result. Success of LPCRS and CSRS will have no effect on core damage since melting would be in progress when these systems were operating.

(e) Without heat removal through the residual heat removal heat exchangers, the temperature of the water in the suppression pool will increase. The failure of vapor suppression causes a massive failure of the containment structure and a high leakage rate. The LPCI and CS pumps will have inadequate NPSH after about 7 hours and the core will melt.

(f) With a small LOCA and no scram, the reactor will tend to remain at relatively high power immediately following the accident. Once steam flow to the turbine has been terminated due to the closure of the turbine stop valve or the main steam line isolation valves, the reactor pressure will increase. The increase in pressure will reduce the steam volume fraction in the core, the power level will increase, and reactor system pressure will increase further. Ultimately, the small LOCA will become a large LOCA, or the reactor vessel will fail.
With a large LOCA and no scram, the low pressure ECCS will attempt to reflood the core. The resulting rapid increase in reactor power, once the core reaches criticality, might result in a vessel failure, or might cause the reactor to "chug" (go from subcritical to some significant power level and back to subcritical) for some period of time. This is assumed to eventually result in massive fuel cladding failures and a core melt.
With a vessel failure, the ECCS system will probably not be able to prevent a core melt, either because a floodable volume is not maintained or because the ECCS lines will fail.

(g) A steam explosion may occur as the molten fuel drops into the residual water in the lower pressure vessel plenum. This will fail the containment, if it has not already failed, and will significantly increase the release of activity to the environment.

(h) A steam explosion may occur as the molten core melts through the reactor vessel and drops into the water that would be remaining at the bottom of the drywell immediately below the reactor vessel. This is a possible mechanism that will result in containment failure. If a steam explosion in the containment occurs, the containment will fail sooner that it would have due to overpressurization from non-condensible gases. If containment isolation has not been successful, a containment steam explosion will increase the containment leak rate and will result in a greater release of fission products.



*Containment Leakage less than 100% / day.

FIGURE I 4-10 BWR Small LOCA (S2, approximately 1/2-2 1/2 inch diameter) in RCS

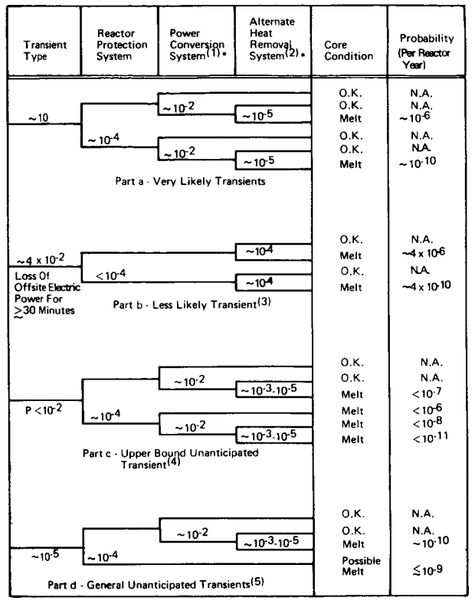
TABLE I 4-8 BWR SMALL LOCA S_2 SYSTEMS STATUS AND CONTAINMENT FAILURE MODES

SEQUENCE	SNO	S_2 LOCA	B EP	C RPS	D VS	E ECI	G CL	H CSRS	I LPCRS	J HPSW	CORE MELT	α	β	γ	δ	ε	εζ	εη	εθ	δζ	δη	δθ	FOOTNOTES
S_2	1	f									N												
S_2J	2	f						f_J	f_J	f	Y	X		X									a, g
S_2I	3	f							f^J	O_I	Y	X		X									a, g
S_2H	4	f						f			N												
S_2HJ	5	f						f	f_J	f	Y	X		X									a, g
S_2HI	6	f						f	f^J	O_I	Y	X	X	X									b, g, h
S_2G	7	f					f				N												
S_2GJ	8	f					f	f_J	f_J	f	Y	X	X		X	X	X	X	X	X	X	X	c, g, h
S_2GI	9	f					f		f^J	O_I	Y	X	X		X	X	X	X	X	X	X	X	c, g, h
S_2GH	10	f					f	f			N												
S_2GHJ	11	f					f	f	f_J	f	Y	X	X		X	X	X	X	X	X	X	X	c, g, h
S_2GHI	12	f					f	f	f^J	O_I	Y	X	X		X	X	X	X	X	X	X	X	d, g, h
S_2E	13	f				f		O_E	O_E		Y	X	X	X									d, g, h
S_2EG	14	f				f	f	O_E	O_E		Y	X	X		X	X	X	X	X	X	X	X	d, g, h
S_2D	15	f			f		Z_D				N												
S_2DJ	16	f			f		Z_D	f_J	f_J	f	Y	X		X									e, g,
S_2DI	17	f			f		Z_D		f^J	O_I	Y	X		X									e, g
S_2DH	18	f			f		Z_D	f			N												
S_2DHJ	19	f			f		Z_D	f	f_J	f	Y	X		X									e, g
S_2DHI	20	f			f		Z_D	f	f^J	O_I	Y	X		X									b, g
S_2DE	21	f			f	f	Z_D	O_E	O_E		Y	X		X									d, g
S_2C	22	f		f							Y	X	X	X									**f**, g, h
S_2CG	23	f		f			f				Y	X	X		X	X	X	X	X	X	X	X	f, g, h
S_2CD	24	f		f	f		Z_D				Y	X		X									f, g
S_2B	25	f	f			Z_B		Z_B	Z_B	Z_B	Y	X	X	X									d, g, h
S_2BG	26	f	f			Z_B	f	Z_B	Z_B	Z_B	Y	X	X		X	X	X	X	X	X	X	X	d, g, h
S_2BD	27	f	f		f	Z_B	Z_D	Z_B	Z_B	Z_B	Y	X		X									d, g

KEY: f - FAILURE
F_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" FAILURE
Z_N - FAILURE PREDICATED BY FAILURE OF "N"
Y - YES
N - NO
X - POTENTIAL CONTAINMENT FAILURE MODE

FOOTNOTES ON APRON

Fig. I 4-10
Table I 4-8



*Numbers in parentheses refer to notes

NOTES

1. The power conversion system (PCS) essentially consists of: the main feedwater and condensate system. The failure probability is estimated without benefit of rigorous analysis; however, the value chosen is on the low side so as not to bias the results. PCS is not shown in part b of Fig. I 4-11 since it cannot operate without off-site electric power.

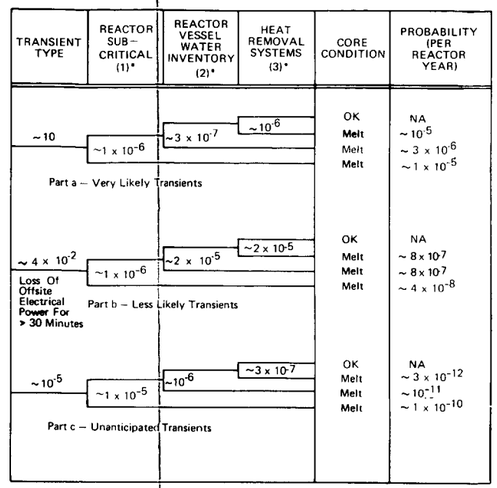
2. The alternate heat removal system is the auxiliary feedwater system (AFWS). Figures a and b indicate different failure probabilities because of its dependence on a diesel generator that is shared between two facilities when off-site power is lost. (See Appendix II.)

3. The value of 4 x 10^{-2}/year for the probability of loss of off-site power for longer than about 30 minutes is derived from data on electrical systems in the U.S. in addition to nuclear systems.

4. Figure I 4-11c shows an arbitrarily chosen transient of some type that has not yet occurred in the 150 reactor years of operation of commercial nuclear power plants.

5. Figure I 4-11d shows a tree that covers such unanticipated transients as rod ejection and steam generator rupture; their probability is very low, but they have the characteristic that PCS cannot serve a useful function if RPS fails.

FIGURE I 4-11 Simplified PWR Transient Event Tree



*Numbers in parentheses refer to notes

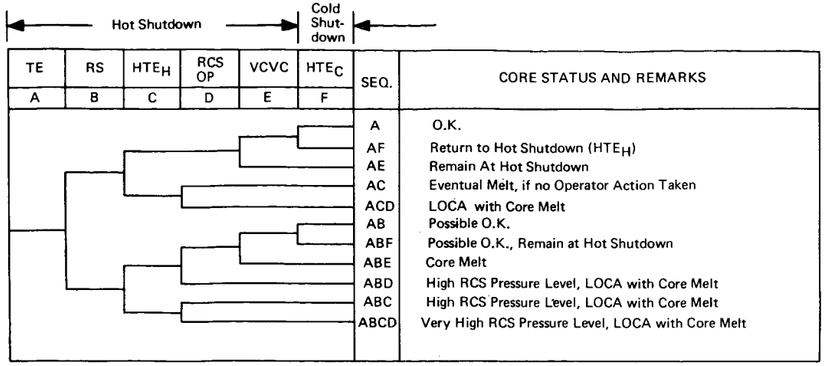
NOTES

1. The systems available to make the reactor subcritical are: (1) the scram system and (2) the combination of reactor coolant pump trip and soluble poison injection. Either of these systems is sufficient for the very likely and less likely transients. However, there may be some very rapid unanticipated transients for which only the scram system operates quickly enough to be effective. Therefore, the probability of failing to make the reactor subcritical is higher for the unanticipated transients.

2. The systems available to maintain an adequate inventory of water in the reactor vessel are the feedwater system, the high pressure coolant injection system (HPCIS), the reactor core isolation cooling system (RCICS), and the low pressure emergency core cooling systems. The loss of off-site power increases the probability of failure of some of these systems, as indicated in Fig. I 4-12b.

3. The systems available to transfer fission product decay heat to the environment are: (1) the power conversion system and (2) the combination of the residual heat removal (RHR) system and high pressure service water (HPSW) system. The loss of off-site power increased the probability of failure of both of these systems, as indicated in Fig. I 4-12b.

FIGURE I 4-12 Simplified BWR Transient Event Tree



Legend:

A: TE – Transient Event
B: RS – Reactor Subcritical
C: HTE$_H$ – Heat Transfer to Environment During Cooldown of RCS to ~150°F and 400 psia
D: OP – Overpressure Protection of Reactor Coolant System
E: VCVC – Reactor Vessel Coolant Volume Control
F: HTE$_C$ – Heat Transfer to Environment During Cold Shutdown of RCS from $\lesssim$150°F and $\lesssim$ 400 PSIA (This function is shown for completeness but is of limited interest to this study of PWR transient events)

FIGURE I 4-13 Functional Event Tree - PWR Transient Events

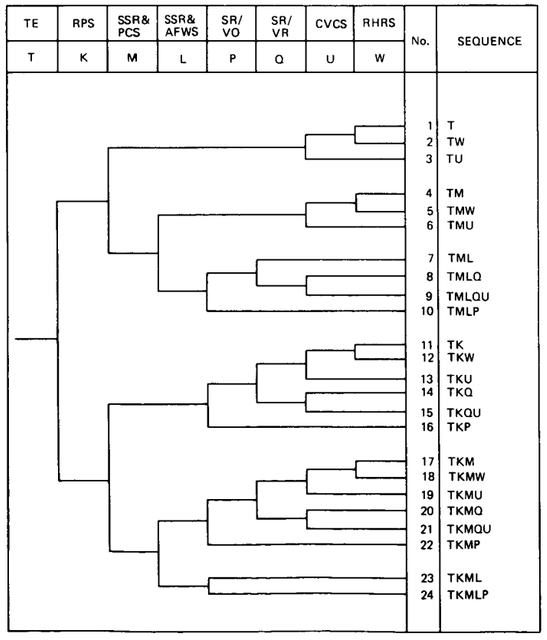


FIGURE I 4-14 PWR Transient Event Tree

TABLE I 4-9 PWR TRANSIENTS

Likely Initiating Events	Unlikely Initiating Events
1. Turbine Trip	1. Rupture of High Energy Piping in Secondary Coolant System, a) Rupture of Main Feedwater Lines, b) Rupture of Lines in Main Steam System[a]
2. Spurious Signals from SICS	2. Rupture of Steam Generator (See Preceding Discussions in section 4.1.5 for Coverage)
3. Loss of Condenser Vacuum	3. Rupture of Control Rod Mechanism Housing on Reactor Vessel Leading to Small LOCA and Control Rod Ejection (See Preceding Discussions in sections 4.1.3 and 4.1.4 for Coverage)
4. Inadvertent Closure of Main Steam Line Isolation Valves	4. Abrupt Seizure of All Main RCS Recirculation Pumps
5. Loss of Main Station Generator with Failure to Relay Auxiliary Loads (e.g., Main Feedwater Pumps, Condensate Pumps) to AC Power Incoming from Offsite Network.	5. Startup of Inactive Reactor Coolant Loop with Abrupt Opening of Both Isolation Valves in One RCS Loop in PWR Plants Employing RCS Loop Isolation Valves
6. Loss of Main Circulating Water Pumps for Condenser Cooling	
7. Loss of Main Feedwater Pumps	
8. Loss of Condensate Pumps	
9. Loss of AC Power Incoming from Offsite Network	
10. Inadvertent Opening of Steam Generator Power-Operated Relief Valves (~10% Sudden Load Demand)	
11. Increase in Main Feedwater Flow; Malfunctions in Feedwater Flow Control	
12. Malfunctions of Control Resulting in Inadvertent Opening of All Turbine Steam Bypass Valves (~40% Sudden Load Demand)	
13. Uncontrolled Rod Withdrawal a) At Full Power, b) At Startup	
14. Control Rod Assembly Drop	
15. Boron Dilution by Malfunctions in Chemical Volume and Control System	
16. Startup of Inactive Reactor Coolant Loop (in PWR with No RCS Loop Isolation Valves)	
17. Accidental Opening of Pressurizer Safety or Relief Valves	
18. Loss of RCS Coolant Flow (Main RCS Circulating Pump Malfunctions)	

[a] These ruptures are included somewhat arbitrarily within the Unlikely Event Category. However, failures of lines in the PWR secondary coolant systems have occurred principally during plant testing and start-up periods. These types of failures have included inadequate initial design of relief valve headers in the steam supply lines, discharge of secondary coolant from leaking feedwater valves, discharge of secondary coolant from cracks in main feedwater lines, etc. The RCS cooldown transients stemming from these failures would be less severe than those included under No. 12 of the Likely Event Category above. The potential impact of such high energy line failures in specific locations of the plant, since they might commonly interact with and affect availability of the plant ESFs, was considered as part of this study. Refer to Appendices II and IV.

TABLE I 4-10 PWR TRANSIENT EVENTS FUNCTIONAL & SYSTEMS RELATIONSHIPS

FUNCTIONS							
RS		HTE_H [a]		RCS-OP		VCVC		HTE_C [a]	
(1)	Reactor Protection System	(1)	Power Conversion System (Pumps) with Steam Relief via Either the Turbine Bypass System to the Condenser or the Main Steam Safety or Relief Valving	(1)	Pressurizer Safety Valves	(1)	CVCS	(1)	Residual Heat Removal System
(2)	Chemical Volume & Control System Operating in Emergency Boration Mode [CVCS(EB)]	(2)	Auxiliary Feedwater System with Steam Relief via Either the Main Steam Safety or Relief Valving	(2)	Pressurizer Safety and Relief Valves	(2)	HPIS	(2)	Option to Reinstitute HTE_H
(3)	Chemical Volume & Control Pumps Operating in HPIS Mode [HPIS]	(3)	Containment Heat Removal Systems with Occurrence of LOCA					(3)	Containment Heat Removal Systems with Occurrence of LOCA

LEGEND

RS - Reactor Subcritical
HTE_H - Heat Transfer to Environment During Cooldown of RCS to ~150°F and 400 psia
OP - Overpressure Protection of Reactor Coolant System
VCVC - Reactor Vessel Coolant Volume Control
HTE_C - Heat Transfer to Environment During Cold Shutdown of RCS from ~150°F & 400 psia

(a) The VCVC Function is Required for Cooldown from Hot, Pressurized RCS Conditions (HTE_H) to Cold, Depressurized Conditions (HTE_C) to Adjust Coolant Volume Change due to Contraction and to Ensure Increases in Boron Concentration are Made for Shutdown Margin of ≥1% Δk/k.

TABLE I 4-11 PWR SYSTEMS STATUS AND CONTAINMENT FAILURE MODES FOR TRANSIENTS

SEQUENCE	SNO	T	K RPS	M SSR&PCS	L SSR&AFWS	P SR-VO	Q SR-VR	U CVCS	W RHRS	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	FOOTNOTES
T	1	f			O_M	O_M	O_M			No		X				
TW	2	f			O_M	O_M	O_M		f	No		X				a
TU	3	f			O_M	O_M	O_M	f	O_U	No		X				b
TM	4	f		f		O_L	O_L			No		X				
TMW	5	f		f		O_L	O_L		f	No		X				a
TMU	6	f		f		O_L	O_L	f	O_U	No		X				b
TML	7	f		f	f	O_L	O_L	O_Q	O_U	Yes	X	X	X	X	X	c
TMLQ	8	f		f	f		f		O_U	Yes	X	X	X	X	X	d, e
TMLQU	9	f		f	f		f	f	O_Q	Yes	X	X	X	X	X	c, e
TMLP	10	f		f	f	f	O_P	O_P	O_P	Yes	X	X	X	X	X	c
TK	11	f	f		O_M					No		X				
TKW	12	f	f		O_M				f	No		X				a
TKU	13	f	f		O_M			f	O_U	No		X				b
TKQ	14	f	f		O_M		f		O_U	Yes	X	X	X	X	X	c, e, f
TKQU	15	f	f		O_M		f	f	O_U	Yes	X	X	X	X	X	c, e
TKP	16	f	f		O_M	f	O_P	O_P	O_P	Yes	X	X	X	X	X	c
TKM	17	f	f	f						No		X				
TKMW	18	f	f	f					f	No		X				a
TKMU	19	f	f	f				f	O_U	No		X				b
TKMQ	20	f	f	f			f		O_U	Yes	X	X	X	X	X	c, e, f
TKMQU	21	f	f	f			f	f	O_U	Yes	X	X	X	X	X	c, e
TKMP	22	f	f	f		f	O_P	O_P	O_P	Yes	X	X	X	X	X	c, e
TKML	23	f	f	f	f		O_{KML}	O_{KML}	O_{KML}	Yes	X	X	X	X	X	c
TKMLP	24	f	f	f	f	f	O_{KML}	O_{KML}	O_{KML}	Yes	X	X	X	X	X	c

KEY: f - FAILURE
f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" OPERATION OR FAILURE
Z_N - FAILURE PREDICATED BY FAILURE OR OPERATION OF "N"
X_N - POTENTIAL CONTAINMENT VESSEL FAILURE MODE

TABLE I 4-11 FOOTNOTES

(a) Plant must be maintained at hot shutdown because RHR is unavailable.

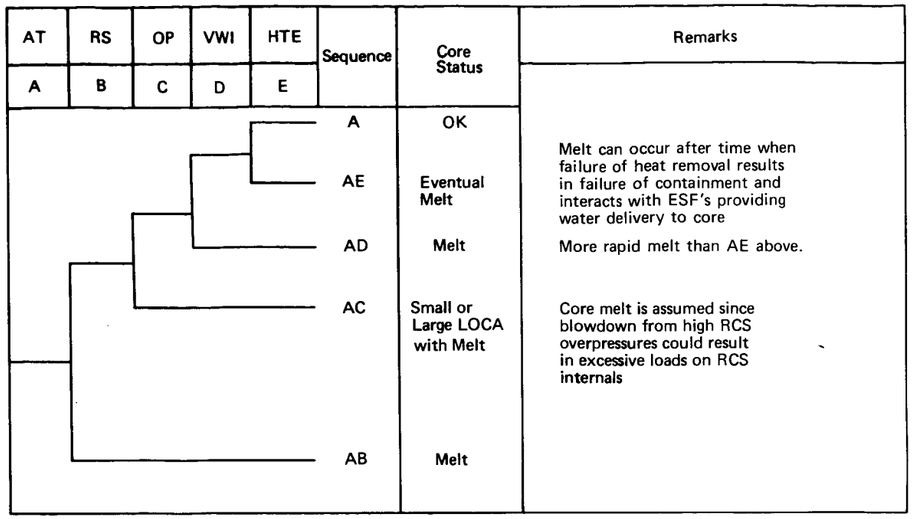
(b) Plant must be maintained at hot shutdown conditions. It is assumed that cold shutdown cannot be achieved if CVCS is not available to compensate for coolant contraction on cooldown.

(c) Primary system is exposed to high internal pressure and is assumed to fail. Because blowdown forces are above design values, core melt is assumed. Containment engineered safety features may function to mitigate consequences. This sequence thus enters the reactor vessel failure tree as a contributor to the initial event.

(d) Sequence results in a small LOCA from stuck-open safety valves. This sequence is conservatively assumed to lead to core melt since failure of all feedwater supply represents a path to core melt as indicated on the small LOCA, S_2, tree. If the opening size of the stuck valves (or LOCA) is large enough, the dependency on feedwater supply would not exist. Core melt could be prevented by the core cooling ESFs as represented by the small LOCA, S_1, tree, and this sequence could thus enter the S_1 tree as a contributor to the initial event.

(e) Failure of the primary system safety valve to close permits system depressurization.

(f) Failure to trip with the safety valve remaining open causes core melt.



Legend:
A. AT – Anticipated Transient
B. RS – Reactor Subcritical
C. OP – Overpressure Protection
D. VWI – Vessel Water Inventory
E. HTE – Heat Transfer to the Environment

FIGURE I 4-15 Functional Event Tree - BWR Transient Events

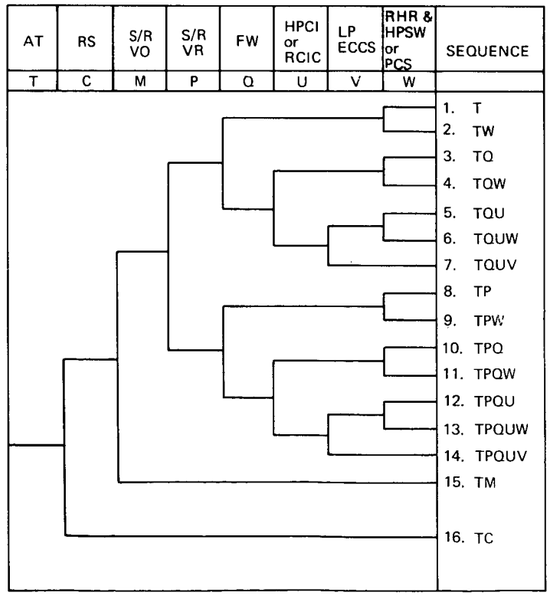


FIGURE I 4-16 BWR Transient Event Tree

TABLE I 4-12 BWR TRANSIENTS

Likely Initiating Events	Unlikely Initiating Events
1. Rod Withdrawal at Power	1. Rod Ejection Accident[(a)]
2. Feedwater Controller Failure - Max. Demand	2. Rod Drop Accident[(a)]
3. Recirculation Flow Control Failure (Increasing Flow)	3. Compound Initiating Events Such As a. Seizure of Two Recirculation Pumps b. Startup of Idle Recirculation Pump Simultaneously with Turbine Trip c. Rod Withdrawal and Simultaneous Startup of Idle Recirculation Loop
4. Startup of Idle Recirculation Pump	
5. Loss of Feedwater Heating	
6. Inadvertent HPCI Pump Start	
7. Loss of Auxiliary Power	
8. Loss of Feedwater Flow	
9. Electric Load Rejection (Turbine Valve Closure)	
10. Turbine Trip (Stop Valve Closure)	
11. Main Steam Line Isolation Valve Closure	
12. Recirculation Flow Control Failure (Decreasing Flow)	
13. Recirculation Pump Trip (One Pump)	
14. Recirculation Pump Seizure	
15. T-G Pressure Regulator Failure - Rapid Opening	

(a) BWR plants have design features provided which make the probabilities for occurrence negligibly small.

TABLE I 4-13 BWR TRANSIENTS-FUNCTIONAL/SYSTEM RELATIONSHIPS

FUNCTIONS:	RS	OP	VWI	HTE
	(1) Reactor Protection System	(1) Safety Valves	(1) Power Conversion System	(1) Power Conversion System
	(2) Reactivity Control System	(2) Safety/Relief Valves	(2) High Pressure Coolant Injection (HPCI) System	(2) High Pressure Service Water System
	(3) Standby Liquid		(3) Reactor Core Isolation Cooling (RCIC)	(3) Residual Heat Removal System
	(4) Recirculation Pump Trip		(4) Relief Valves	
			(5) Low Pressure Emergency Core Cooling System	

LEGEND: RS - Reactor Subcritical
OP - Overpressure Protection
VWI - Vessel Water Inventory
HTE - Heat Transfer to Environment

TABLE I 4-14 BWR SYSTEMS STATUS AND CONTAINMENT FAILURE MODES FOR TRANSIENTS

SEQUENCE	SNO	AT T	RPS C	S/R VO M	S/R VO P	FW Q	HPCI or RCIC U	LP ECCS V	RHR & HPSW or PCS W	CORE MELT	α	γ	FOOT NOTES
T	1	f								N			
TW	2	f						f_W	f	Y	X	X	a, d
TQ	3	f				f				N			
TQW	4	f				f		f_W	f	Y	X	X	a, d
TQU	5	f				f	f			N			
TQUW	6	f				f	f	f_W	f	Y	X	X	a, d
TQUV	7	f				f	f	f	O_V	Y	X	X	b, d
TP	8	f			f					N			
TPW	9	f			f			f_W	f	Y	X	X	a, d
TPQ	10	f			f	f				N			
TPQW	11	f			f	f		f_W	f	Y	X	X	a, d
TPQU	12	f			f	f	f			N			
TPQUW	13	f			f	f	f	f_W	f	Y	X	X	a, d
TPQUV	14	f			f	f	f	f	O_V	Y	X	X	b, d
TM	15	f		f						See Foot-note (e)			e
TC	16	f	f			O_C	O_C	O_C	O_C	Y	X	X	c, d

KEY: f - FAILURE
f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" FAILURE
Y - YES
N - NO
X - POTENTIAL VESSEL FAILURE MODE

TABLE I 4-14 FOOTNOTES

(a) Following a transient with a successful reactivity insertion to bring the core to a subcritical condition, and with the core maintained in a flooded condition, fission product decay heat is transported to and stored in the suppression pool. This will increase the pressure in the containment. If heat rejection to the environment is not initiated within about 27 hours, the containment pressure will reach its predicted failure pressure of 177 psia. Since the water in the suppression pool will be at the saturation temperature associated with the partial pressure of steam within the containment, the rapid depressurization which occurs upon containment failure will cause the water in the suppression pool to flash and cause cavitation of the low pressure ECCS pumps. These pumps will then have insufficient NPSH to continue operating. Hence, the core will not be maintained in a reflooded condition, the water remaining in the core region will be vaporized, and the core will melt.

(b) With the feedwater, HPCI, RCIC, and low pressure ECC systems failed independently, the core is not maintained in a reflooded condition. The water in core region will be vaporized and the core will melt.

(c) With the reactor not made subcritical (by the control rods or by a combination of recirculating pump trip and soluble poison injection), the reactor will tend to remain at a relatively high power level. After steam flow to the turbine is terminated due to the closure of the turbine stop valve or the main steam isolation valve, the reactor pressure will increase. This pressure increase will lead to a rise in power which, in turn, will further increase the primary coolant system pressure. The opening of the primary system relief and safety valves will limit the pressure increase; the peak pressure attained will be a function of the transient power history and the setpoints and capacities of the safety and relief valves. A peak primary system pressure of 1550 psia has been predicted (Ref. 5) for a plant of the type considered here. Recirculation pump trip combined with the loss of moderator through the relief and safety valves will tend to reduce the reactor power level. The power is expected to stabilize at about 30 percent of nominal. At some time into the accident, the HPCI system will start to add water to the primary system. At power levels significantly above decay heating, the boiloff rate will be greater than the capacity of the HPCI; thus, the water level in the primary system will decrease and eventual core meltdown can be expected.

(d) A steam explosion may occur as the molten core melts through the reactor vessel and drops into the water that would be remaining at the bottom of the drywell immediately below the reactor vessel. This is a possible mechanism that will result in containment failure. If a steam explosion in the containment occurs, the containment will fail sooner than it would have due to overpressurization from non-condensible gases.

(e) If an insufficient number of safety and relief valves fail to open, the reactor coolant pressure will exceed the design pressure of the system piping. A core melt is assumed to result.

Section 5

Analysis of Potential Accidents Not Involving the Core

As indicated earlier, this section will discuss potential releases of radioactivity from sources other than the core.

The sources to be covered are the Spent Fuel Storage Pool (SFSP), the Spent Fuel Shipping Cask (SFSC), the refueling process, the Waste Gas Storage Tank (WGST) and the Liquid Waste Storage Tank (LWST). As will be seen in the discussions below, for those locations involving fuel elements (SFSP, SFSC and the refueling process), design features are provided both to reduce the likelihood of releasing radioactivity from the fuel and to mitigate the consequences of such releases. When the radioactive inventories are very much smaller (see Table I 3-1) such as in the WGST and LWST, fewer safety features are provided.

The releases and probabilities presented below represent rough estimates unlike the quantifications performed in the other appendices. Probability estimates in this section are largely based on engineering judgement considering plant experience to date and the results of detailed analyses of other similar systems. They are not supported by fault tree analysis.

The assumptions used in calculating releases are presented below in the discussions of the various accidents. The calculated releases represent extrapolation and modification of the results of the analyses presented in Appendix VII. Detailed analyses of radioactive release, retention and removal under the specific conditions of the accidents considered below have not been performed. However, we have attempted to utilize the Appendix VII analyses in a conservative manner and anticipate that the releases presented represent upper bound estimates of potential atmospheric releases from these accidents.

As discussed in Appendix VI, the releases presented below result in minor off-site consequences in comparison with other accidents analyzed and represent only a very small contribution to overall risk. Detailed analyses of both the probability of occurrence of these accidents and of their consequences must be performed at a later time if it is desired to determine this contribution with greater accuracy.

5.1 SPENT FUEL STORAGE POOL (SFSP)

SFSPs are located adjacent to the plant primary containment building to provide an underwater path through which spent fuel removed from the reactor can be moved to the pool for storage. These pools are designed so that there will be a small likelihood of releasing radioactivity from the stored fuel. Release of radioactivity can potentially occur by either melting or by mechanical damage to the fuel that will release the radioactivity from the fuel pin gap. The pools are also located in buildings provided with ventilation systems and filters to remove radioactivity that might be released from the fuel.

Fuel melting can only occur if (1) water is lost from the pool or (2) the fuel in the pool is rearranged into a configuration where criticality is achieved and power is generated beyond the capability of the SFSP cooling system. This can occur by means of:

a. Drainage of water from the pool due to mechanical damage to the pool. For example the spent fuel shipping cask (SFSC) weighing about 100 tons, could grossly damage the fuel pool integrity if it were to fall into the pool.

b. Loss of cooling of the pool water followed by subsequent boil-off of the pool water.

Significant mechanical damage to the fuel can only be caused by dropping a heavy load from the crane while it is traveling over the pool. Fuel rearrangement into a critical configuration which would generate additional power can potentially result from the dropping of a heavy item on the stored fuel or from seismic forces.

The design features provided to keep the likelihood of loss of pool water and recriticality small are:

a. The fuel building concrete structure, the spent fuel storage pool, the spent fuel storage racks, the SFSP cooling system, and the supports for the spent fuel handling trolley are designed to withstand seismic forces so that an earthquake as large as the safe shutdown earthquake will not cause loss of water or recriticality.

b. Fuel storage racks are designed to keep the fuel widely enough separated so that stored fuel will not achieve criticality.

c. The pool is designed to prevent inadvertent loss of water from the fuel by drainage through connected piping systems. Although a pool cooling system is connected to the pool to remove fuel decay heat, it is designed to prevent siphoning of the pool water. A connection exists between the SFSP and the pressure vessel head through the fuel transfer pathway which is provided with physical barriers to prevent SFSP drainage when not in use. The pools are generally sized so that the fuel remains covered to at least half its height even if the fuel transfer pathway is inadvertently opened.

d. Should water inventory in the pool fall below a pre-set level or increase in temperature, multiple water level, water temperature and radioactivity monitors would actuate alarms in the control room. A make up water system is provided to keep up with small leaks.

e. Procedures and interlocks are provided to keep the crane from passing over the pool with heavy loads.

f. The fuel building and the SFSP are designed to accomodate the forces which might result from winds and missiles that might be generated by a tornado. Further, the spent fuel storage racks and the SFSP cooling system are protected by structures designed to withstand these forces.

The sections which follow will consider the various potential accident sequences that can occur in the SFSP and estimate their probability of occurrence and size of radioactive release.

5.1.1 LOSS OF SPENT FUEL POOL COOLING

Fuel handling cannot commence for at least three days following shut down due to the time required to prepare for refueling, to remove the vessel head, and to remove the upper vessel internals. Due to shipping cask design, fuel must be held approximately 150 days before transport. For shipment by truck, fuel transfers would be scheduled twice per week. Thus, considering a two-unit site with refueling of about 1/3 of the core of each unit every 360 days, the average inventory in the pool is 1/2 of a core loading, consisting of 1/3 of a core loading with 75 days decay and 1/6 of a core loading with 241 days decay. To account for the possibility that refueling intervals for the two units may not be evenly spaced, we have assumed an average inventory composed of 1/3 of a core loading with 60 days decay and 1/6 of a core loading with 150 days decay.[1] The decay heat generation rate for this pool loading is approximately 1.6 Mw. Approximately 50,000 cubic feet of water are located above the stored fuel in the pool for radiation shielding. Fuel damage cannot occur after loss of pool cooling until all water has boiled off. For this average pool inventory, this time period is approximately 3.8 weeks. The pool loading immediately following refueling has also been considered. This consists of 1/3 of a core 150 days after shutdown, and 1/3 of a core loading with 3 days decay. This loading would allow approximately 9 days for the cooling system to be repaired and/or water makeup to be accomplished.

The probability of fuel damage resulting from loss of spent fuel pool cooling is clearly quite small in view of the ample time for repairs to be made or for water to be added. The probability of SFSP coolant system failure has not been analyzed in detail, however it is estimated to be less than 0.1 per year. The failure to identify the need for water makeup over either the 3.8 week or 9 day period is estimated to have a probability of at least 10^{-6} considering the fuel shipments are made on a weekly basis and that multiple water level

[1] The discussion above is based largely on PWR operations. The BWRs refuel about 1/4 of the core each year. This difference in refuel practice will not significantly affect the inventories presented herein.

water temperature and radiation level monitors are provided, all of which alarm in the control room. The probability of not being able to provide makeup water to the pool, given the knowledge that makeup is required, is estimated to be at least 10^{-6} for the 3.8 week case and 10^{-5} for the 9 day case. Assuming the SFSP heat loading will approach that of the 9 day case 1/10 of the time, the probability of fuel damage due to loss of pool cooling is estimated to be approximately 1 x 10^{-7} per year for either case.

In the event of an accident in the SFSP, the ventilation system will process all gases released from the pool through high efficiency particulate (HEPA) and charcoal filters. Based on information presented in Appendix VII, it is assumed that these will reduce the elemental iodides, the organic iodines, and particulate species by 99%. This leads to the atmospheric releases presented in Table I 5-1 for both the maximum and average pool loadings discussed.

5.1.2 DRAINAGE OF FUEL POOL

With the exception of the fuel transfer pathway, there are no piping penetrations which, if open could drain the spent fuel storage pool. Further, there are no potential paths for siphoning water from the pool. Thus, to inadvertently drain the pool, the pool liner must fail causing leakage of water from the pool, or the fuel transfer tube must be open. Because of the physical arrangement of the refueling canal, it is impossible to drain the water to below half the fuel height. Thus, time is available for corrective action prior to complete boil-off of pool water (approximately 1.2 days immediately after refueling extending to 3.6 days for the average condition). The probability of pool drainage to the refueling canal is small. It must consider the following failures:

a. Inadvertent opening of the fuel transfer pathway requiring multiple errors to drain the SFS pool,

b. The need for makeup is unrecognized, or makeup water cannot be obtained.

The releases from the meltdowns are as stated in section 5.1.1. However, in view of the many simultaneous faults which must occur, it is estimated that the probability of occurrence is significantly lower than for the case identified in section 5.1.1.

5.1.3 DROPPING OF HEAVY ITEM INTO SFSP

As previously noted, pool drainage can also occur if the pool liner is damaged. A postulated means of damaging the liner is the dropping of a heavy load, such as a fuel transfer cask, in the spent fuel storage pool. The fuel storage pool is protected in the cask handling area by a pad of energy absorbing material designed to accommodate impact of the cask on the pad. However, two mechanisms for pool damage were considered: (1) a cask drop that causes a 1/2 inch diameter hole in the bottom of the pool, and (2) a cask drop that completely ruptures the pool. Both cases eventually lead to a meltdown of the stored spent fuel. Consequences will be the same as for the case examined in section 5.1.1. A discussion of the probability of occurrence follows, using a crane failure probability of $3(10^{-6})$ per operating hour:

Two shipments per week are anticipated for this two-unit site. Assuming the crane is in use over the pool 10 minutes per shipment, a crane failure rate of 5.2 (10^{-5})/year is predicted. Further, it is assumed that the probability of causing a leakage path equivalent to a 1/2" diameter hole due to the cask drop is 0.1, yielding combined failure probability of 5 (10^{-6})/year. For a 1/2" diameter hole, approximately 9 days will elapse before fuel is uncovered with no makeup. This must be combined with the probability that the operator will fail to recognize the need for water or makeup from any source in the nine day period. Thus, for this accident, the probability of meltdown is significantly lower than that estimated in section 5.1.1.

We have also considered the gross failure of the spent fuel storage pool by impact of a dropped fuel cask. Since the bottom of the pool in the area of interest is provided with an energy absorbing pad designed for such impact, we have considered only impact on the edge of a vertical pool wall causing gross cracking and failure of the pool. The period of time the cask is in the proper position for gross pool damage is assumed to be 10 seconds per shipment. Therefore, a pool failure rate of 9 x 10^{-7} per year is predicted. Since gross damage is assumed, makeup cannot prevent fuel melting. The probability of melting the stored fuel in the pool is 9 x 10^{-7} for the average inventory and 9 x 10^{-8} for the maximum inventory, considering that the inventory approaches the maximum amount about 1/10

of the time. The consequences are as discussed in section 5.1.1.

Administrative procedures and interlocks prevent the passage of heavy loads over the spent fuel storage pool. However, if these were defeated there is a possibility that a crane failure could cause a heavy item to drop, damaging one or more fuel assemblies. To conservatively evaluate consequences, a heavy load is assumed to drop on fuel elements equivalent to the maximum and average fuel pool loadings identified above, leading to release of all gap activity under water. Assuming a water partition factor of 760 for all isotopes other than the noble gases, 0.7% organic iodides, and filtration of the fuel building ventilation as discussed above, the releases presented are calculated for the maximum and average inventory:

	Release (Ci)	
Elements	Max. Inventory	Avg. Inventory
Noble Gases	1.37×10^{6}	1.74×10^{4}
Halogens	3.41	1.18×10^{-2}

The probability of occurrence is a function of the following: (1) violation of administrative procedures in passing heavy loads over the fuel, (2) interlock failure permitting a heavy load to pass over the fuel, and (3) crane failure while over the pool with heavy loads. If we postulate that heavy loads will only be positioned over the fuel for 5 minutes per act, the failure rate will be at least 2.5×10^{-7} per year even if the combined operator error and interlock failure is assumed to occur once per year. Thus, the probability of occurrence is quite small while the releases are much less severe than those estimated for fuel melting in section 5.1.1.

The dropping of a heavy item into the pool could potentially cause enough mechanical damage to the fuel storage racks to cause the stored fuel assemblies to move into a critical configuration that would generate power beyond the capability of the SFSP cooling system. This has the potential to result in a more rapid boiloff of pool water than that considered in section 5.1.1 of this Appendix. In the PWR, the coolant in the SFSP is borated to such an extent that even if the stored fuel were put into the same spacing as existed in the core, the pool would remain subcritical and would not generate additional power. The BWR, however, relies on spacing without additional poison addition to eliminate power generation. Thus, it is conceivable that the dropping of a heavy item at a BWR could lead to some increase in the radioactivity in the fuel and to more rapid boiloff of core water. This does not represent a situation significantly different than that analyzed in section 5.1.1, as indicated below.

The probability of causing power generation as a result of dropping of a heavy item can be computed as the probability of heavy loads being positioned over the pool (estimated at 2.5×10^{-7} per year act, above), times the probability of operator error, with interlock failure, times the probability of rearranging the fuel into a configuration which would generate additional power. Even if it is assumed that the probability of interlock failure and unfavorable fuel configuration are each 0.1/act and that the operator attempts to move a heavy item over the pool once per year, the probability of fuel melting by this mechanism is far smaller than that estimated in section 5.1.1 (1×10^{-7}/reactor year). Since the energy required to boil off the SFSP water is less than that generated by 20 minutes operation at full power, very few additional fission products would be generated in this period. Thus, this type of accident would not contribute to the overall accident risk because it would be lower in probability and no larger than that calculated in section 5.1.1.

The events discussed above relating to pool drainage and the dropping of heavy items on the fuels stored in the SFSP could also be caused by external events, such as missiles generated by tornadoes or turbine failures and earthquakes. Bush (Ref. 1) has estimated that the probability of turbine failure with generation of a turbine missile is approximately 10^{-4}/year. He also indicates that the limiting strike probability for the SFSP, given an energetic missile, is about 4.1×10^{-3}. Thus, the probability of damage to the spent fuels from the turbine missile should be less than 10^{-6}.

As discussed in section 5.4 of the Reactor Safety Study Report, the probability of a design basis tornado striking the reactor site is estimated to be about 5×10^{-6}/year. Since this must be coupled with the probability of spent fuel damage from missiles, given a tornado of this magnitude, the probability of fuel damage is clearly lower

than 5 x 10^{-6}/year. This is so since structures protecting the SFSP and its cooling system are designed to withstand the tornado.

As indicated in section 5.4.1 of the Main Report, the probability of a safe shutdown earthquake is estimated to be 10^{-4} - 10^{-6} per year. Further, based on the analyses presented in Appendix X, the probability that a system designed to withstand seismic forces fails during a safe shutdown earthquake has been estimated to be approximately 0.1 and the probability of any two items failing is in the range between 0.1 to 0.01. Thus, if we consider a severe earthquake as the initiating event, rather than the model presented above, the probability of drainage of the SFSP, due to earthquake damage, with subsequent melting of stored spent fuel is 10^{-5} - 10^{-7}.

If, in addition, the fuel building air cleanup system were to fail during this earthquake, the releases of all isotopes other than the noble gases would be two orders of magnitude higher than presented in the table in section 5.1.1. This would have a probability of occurrence of 4 x 10^{-6} - 2 x 10^{-8} per year. The radioactive release fractions are presented in the Summary Table, I 5-2, at the end of this section. External events would not significantly affect the probability or consequences of the other accidents analyzed in this section.

5.2 SHIPPING CASK ACCIDENTS

Spent fuel assemblies are shipped from the facility to a spent fuel reprocessing plant in shipping casks. The shipping cask is lifted into the SFSP where it is loaded. It is then removed from the pool and positioned on its transporter (either truck bed or railcar). This portion of the study was restricted to consideration of shipping cask accidents which occur on the nuclear power plant site. Accidents which occur during transportation have been considered in Environmental Survey of Transportation of Radioactive Materials to and from Nuclear Power Plants (WASH-1238).

The largest shipping cask presently licensed can transport 7 PWR or 17 BWR fuel assemblies. This would amount to approximately 4.5% of a core loading. Dropping of the cask could potentially interfere with removal of decay heat from the cask or cause breaching of the cask. These are discussed below.

5.2.1 SHIPPING CASK ACCIDENTS IN PWR PLANTS

Shipping casks are designed to accommodate a 30 ft. drop onto a flat, essentially unyielding, horizontal surface. In general, PWR facilities are designed such that no potential exists for dropping a cask greater than 30 feet. We consider the probability of cask rupture from a drop of less than 30 feet to be so low that it need not be considered. The large shipping casks, however, must be supplied with supplemental cooling to remove decay heat from the cask, or PWR fuel in the cask may heat to the point where clad perforation occurs. Dropping of the cask could potentially impair the ability to provide such supplemental cooling. However, assuming the cask remains intact, cooling can be provided on an emergency basis (e.g., by spraying the exterior of the cask with water). We have estimated the probability of a cask drop to be 3 x 10^{-6} per year based on a crane failure rate of 3 x 10^{-6}/hour, a lift height of 30 feet, a crane velocity of 0.1 ft/sec, and an assumed 10 shipments per year. The probability of failure to supply supplemental cooling given a cask drop is very low (10^{-2} - 10^{-4}). Thus, we feel that the probability of fission product release by overheating is sufficiently low that it need not be considered.

5.2.2 SHIPPING CASK ACCIDENTS IN BWR PLANTS

WASH-1238 indicates that loss of supplemental cooling to the largest cask presently licensed will not result in cladding perforations if the cask contains BWR fuel. Thus, lack of supplemental cooling will not result in fission product release. However, BWR plants generally are designed in such a manner that the loaded cask must be lowered approximately 100 feet in order to position it on the railcar. Considering the 70 ft. of this descent during which the cask has the potential for a free drop in excess of that considered in the design, a 0.1 ft/sec lowering rate, a crane failure rate of 3 x 10^{-6} per operating hour, and 10 shipments per year, we estimate the probability of dropping a cask greater than 30 feet to be 6 x 10^{-6} per year. Considering that the cask will impact on a flatcar which should experience some yielding, we have arbitrarily assumed a probability of 0.1 that the cask will be breached sufficiently to lose the cooling medium upon impact. This leads to clad perforation due to overheating with a probability of 6 x 10^{-7} per year.

To estimate the consequences of such an occurrence, we have assumed that 10% cladding perforations occur, based on the information presented in WASH-1238. We have used the gap release and gap escape fractions presented in Appendix VII with the latter modified to reflect the lower gap temperatures experienced in this accident. We have also assumed a decontamination factor of 2.0 due to plateout within the cask for all isotopes other than noble gases. These lead to the following calculated releases:

Elements	Release (Ci)
Noble Gases	1.47×10^2
Alkali Metals	2.77×10^1

5.3 REFUELING ACCIDENT

Accidents can occur during refueling of the core which result either in mechanical damage to the fuel or in the inhibiting of heat transfer from the spent fuel being handled. Calculations indicate that even if a fuel assembly is completely withdrawn from the refueling canal or spent fuel pool, air convection cooling is adequate to prevent fuel melting.[1] However, because of the increased temperature of the clad, some cladding perforation and release of gap activity would occur. To bound the consequences of a refueling accident, we have assumed release of all gap activity from a fuel element 72 hours after shutdown. These calculations assume a peaking factor of 1.58 for the assembly. The following release is predicted:

Elements	Release (Ci)
Noble Gases	4.09×10^4
Halogens	2.65×10^2
Alkali Metals	1.59

[1] Plants are designed in such a manner that it is physically impossible to completely withdraw a fuel assembly from the water using normal refueling equipment. Although this analysis conservatively assumes that an assembly can be withdrawn, it makes little difference to the overall risk assessment.

The probability of gap activity release due to mechanical damage will likely be dominated by crane failures. Using a crane failure probability of 3×10^{-6}/ operating hour and assuming 100 hours of crane operation per refueling leads to a prediction of the probability of clad failure due to mechanical damage of 10^{-4}/year. Clad damage due to overheating can be caused by an operator error or crane fault which raises the assembly above the pool surface. We have assumed an upper limit for this failure of 10^{-3} per refueling. Thus, the probability of gap activity release to the environment through charcoal and HEPA filters from one assembly during refueling is estimated to be 10^{-3} per year.

5.4 WASTE GAS STORAGE TANK RELEASE

The waste gas storage tank is used to store radioactive gases which have been processed through the waste gas treatment system to permit time for their decay and subsequent release. For the PWR under study, the maximum inventory of noble gases in the waste gas storage tank authorized by the AEC Technical Specifications is limited to 9.5 (10^4) Ci. The corresponding halogen inventory is estimated to be 1.01 Ci.

The storage tanks are designed to withstand seismic loadings and are protected from tornado damage. Release of tank contents can be caused by tank rupture, inadvertent or improper opening of a discharge valve, opening of a tank relief valve or backflow through the system to a failure which occurs in other areas of the auxiliary building. It is arbitrarily assumed that the combination of the probabilities of occurrence of these faults is 10^{-2}.

5.5 LIQUID WASTE STORAGE TANK RUPTURE

During normal operation, the liquid waste tanks store radioactive liquids (1) to allow time for decay and (2) to provide temporary holdup until they can be processed by the liquid waste treatment system. The storage tanks are surrounded by a dike designed to withstand seismic loading to ensure any leakage resulting from an earthquake is contained. The following inventory is estimated to be representative of the contents of the liquid waste storage tanks:

Halogens	6.19×10^{1} Ci
Alkali Metals	9.06 Ci
Te, Sb	1.68 Ci
Noble Metals	2.02×10^{1} Ci

Tank failure would result in the release of the contents. It is assumed that the probability of inadvertent release by proper error or tank failure is less than 10^{-2}/year.

5.6 SUMMARY

To aid in readily understanding the above, a table summarizing the probabilities of occurrence and the curies released to the environment from the various accidents analyzed which do not involve the core is appended as Table I 5-2.

References

1. Spencer H. Bush, "Probability of Damage to Nuclear Components Due to Turbine Failures", Nuclear Safety, Vol. 14, No. 3, May-June, 1973.

TABLE I 5-1 ATMOSPHERIC RELEASES

Chemical Groups and Elements	Curies Released[a]	
	Maximum Loading	Average Loading
Noble Gases	4.56×10^{7}	5.80×10^{5}
Halogens	5.25×10^{5}	1.8×10^{3}
Alkali Metals	3.13×10^{5}	2.17×10^{5}
Alkaline Earths	7.86×10^{4}	1.88×10^{4}
Te, Sb	3.12×10^{5}	2.19×10^{4}
Noble Metals	1.42×10^{5}	4.61×10^{4}
Actinides & Lanthanides	8.97×10^{4}	1.24×10^{3}

(a) Releases less than 1 Ci are not tabulated.

TABLE I 5-2 ACCIDENTS NOT INVOLVING CORE-PROBABILITY OF OCCURRENCE AND RADIOACTIVE RELEASE[a]

	SFSP-1/3 Core Melt (without filtration)		SFSP-1/3 Core Melt (with filtration)		Dropping of Heavy Item		Refueling Accident	WGST	LWST	Shipping Cask (In-plant)
	Max. Loading	Ave. Loading	Max. Loading	Ave. Loading	Max. Loading	Ave. Loading				
Probability (Yr^{-1})	3×10^{-8}	3×10^{-7}	2×10^{-7}	10^{-6}	$<10^{-6}$	$<10^{-6}$	10^{-3}	10^{-2}	10^{-2}	6×10^{-7}
Release (ci)[a]										
Noble Gases	4.56×10^{7}	5.80×10^{5}	4.56×10^{7}	5.8×10^{5}	1.37×10^{6}	1.74×10^{4}	4.09×10^{4}	9.5×10^{4}	-	1.47×10^{2}
Halogens	5.2×10^{7}	1.8×10^{5}	5.2×10^{5}	1.8×10^{3}	3.41	-	2.65×10^{2}	1.01	6.19×10^{1}	-
Alkali Metals	3.13×10^{7}	2.17×10^{7}	3.13×10^{5}	2.17×10^{5}	-	-	1.59	-	9.06	2.77×10^{1}
Alkaline Earths	7.86×10^{6}	1.88×10^{6}	7.86×10^{4}	1.88×10^{4}	-	-	-	-	-	-
Te, Sb	3.12×10^{7}	2.2×10^{6}	3.12×10^{5}	2.2×10^{4}	-	-	-	-	1.68	-
Noble Metals	1.42×10^{7}	4.61×10^{6}	1.42×10^{5}	4.61×10^{4}	-	-	-	-	2.02×10^{1}	-
Actinides and Lanthanides	8.97×10^{6}	1.24×10^{5}	8.97×10^{4}	1.24×10^{3}	-	-	-	-	-	-

(a) Releases which are less than 1 Ci are not tabulated.