COMBUSTION ENGINEERING

July 29, 1988
LD-88-066

Docket No. STN 50-47[illegible]
(Project No. 675)

Mr. Frank J. Miraglia
Associate Director for Projects
Office of Nuclear Reactor Regulation
Attn: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Subject: Advanced Reactor Severe Accident Program (ARSAP) - Topic Paper Set 3

References: (A) Letter, LD-87-067, A. E. Scherer (C-E) to F. J. Miraglia (NRC), dated November 24, 1987.

(B) Letter, LD-88-038, A. E. Scherer (C-E) to F. J. Miraglia (NRC), dated June 6, 1988.

(C) Letter, LD-88-042, A. E. Scherer (C-E) to F. J. Miraglia (NRC), dated June 17, 1988.

Dear Mr. Miraglia:

In Reference (A), Combustion Engineering submitted ARSAP proposed resolutions for Topic Paper Set 1 (Resolved NRC/IDCOR Issues), and in References (B) and (C) proposed resolutions for Topic Paper Set 2 (Plant Response Under Severe Accident Conditions) were submitted. This letter provides proposed resolutions for the following Topic Paper Set 3 (Probabilistic Risk Assessment Methods) items:

- o External Events (ARSAP Item 3.1)
- o Success Criteria (ARSAP Item 3.2)
- o Accident Sequence Selection (ARSAP Item 3.3)

Combustion Engineering plans to adopt, in the development of the System 80+ Standard Design, the resolutions to the items listed above, as well as those transmitted in References (A) through (C). We request your early concurrence.

E003
1/1

Power Systems
Combustion Engineering, Inc.
1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095-0500
(203) 688-1911
Telex: 99297

If you have any questions or comments, please call me or Dr. Michael D. Green of my staff at (203) 285-5204.

Very truly yours,

COMBUSTION ENGINEERING, INC.

A. E. Scherer
Director
Nuclear Licensing

AES:ss

Attachment: As Stated

cc: Mr. Frank Ross (DOE - Germantown)

DOE Advanced Reactor Severe Accident Program *

ARSAP Proposed Resolutions for Severe Accident Issues - TOPIC SET 3

* The material in this attachment was developed by the ARSAP in support of C-E's Design Certification Program

ARSAP Severe Accident Issue Topic Paper

3.1 External Events

Issue Definition

The Nuclear Regulatory Commission's (NRC's) Severe Accident Policy Statement[1] specifies that a probabilistic risk assessment (PRA) shall be submitted with the application for a Final Design Approval (FDA). The PRA to be performed is required to address external events.

The definition of "external events" has evolved with PRA; generally, they are those events that result in a plant upset condition, but are not initiated by plant systems. External events typically result in multiple component or system failures. Many external events are addressed specifically in 10CFR50.[2] The General Design Criteria, Appendix A of 10CFR50, require that plant structures be designed to protect against natural phenomena (Criterion 2); that safety equipment be designed and located to minimize the effects of fire (Criterion 3); and that safety equipment be appropriately protected against missiles.

Despite these requirements, past PRAs of contemporary plants although in compliance with these criteria have identified potential plant vulnerabilities related to external events that have been significant contributors to the overall plant public health risk.[3,4] Such events illustrate the importance of including external events in the PRA.

This paper deals with the issue of selecting a process by which risk dominant External Events will be selected and screened, and defines a process by which they will be treated in the PRA for advanced PWRs as required by Reference 1. The three key elements of this issue, related to the PRA analysis are:

- o Identification of External Events. A complete set of external initiating events that will be considered in some way by the PRA analyst is required. An appropriate list exists in NUREG/CR-2300,[5] as discussed below.

- o Qualitative Screening of the External Events. Many listed external events can be excluded prior to performing a PRA by use of a qualitative screening process. Such a screening process uses past PRAs or the Standard Review Plan,[6] for example, as sources to identify external events that are not significant to risk for the advanced PWR.

- o Methodology for Evaluation of Selected External Events - Some specific external events do require more extensive evaluation in, or involving, the PRA for an advanced PWR. For these external events, such as seismic events, the specific methodology to be used for quantification or to address them in an alternative manner must be established.

Historical Perspective

The use of PRAs in the licensing process has been developing and maturing since the completion of the Reactor Safety Study.[7] For the most part, the acceptance by NRC of probabilistic methods has been on an a case-by-case basis as individual studies have been submitted. Implementation of the Backfit Rule[8] uses a risk-based cost-effectiveness test. The first formal requirement for a PRA in the licensing process was specified in NUREG-0718.[9] A requirement for a comprehensive PRA in the licensing process is included in the Severe Accident Policy Statement (see Reference 1).

Since the Reactor Safety Study, the industry has been including external events in some PRAs in an evolutionary fashion with the later PRAs providing substantially more sophistication in the completeness and manner of including external events. Many of the recent PRAs have found that external events can be significant contributors to the core melt frequency.[10] External events

have been estimated to represent as much as 66% of the total mean annual core melt frequency (see Reference 10) and typically represent from 15 to 25% of the total in recently published PRAs.

Specifically, several PRAs have indicated that a seismic event is an important contributor to overall plant risk (see References 4, 11). In these PRAs, the seismic initiating event resulted in a loss of offsite power that, when combined with other failures, led to a station blackout. The Oconee PRA (see Reference 3) identified an internal flooding sequence (an "external event" by convention), which was the dominant contributor to core damage. Further, some PRAs (see References 3, 12) have identified a core damage sequence, initiated by high winds or a tornado that resulted in the collapse of block wall structures onto important safety equipment.

A consensus listing of external events to be considered in preparing a PRA has been provided in the PRA Procedures Guide (see Reference 5); the listing was based in part on the national standard ANSI/ANS 2.12-1978.[13] These external events are presented in Table 1 and include natural phenomena (earthquakes, etc.), man-made initiators (aircraft crashes, etc.), and certain other, apparently internal, events that fit the "external" definition (fires, internal floods, and turbine missiles).

While the list in Table 1 is considered to be complete, the number of these events assessed to be potentially significant contributors to plant risk has been reduced with experience. For example, many external events have been eliminated based on improvements in plant design. The use of block wall structures that contain safety equipment is no longer an acceptable design practice. In recent vintage plants the structures that are similar in function to the block wall structures found at Indian Point 2 and Oconee are now reinforced concrete and have a much higher resistance to wind or tornado damage.

TABLE 1

POTENTIAL EXTERNAL EVENT INITIATORS
PRESENTED IN THE PRA PROCEDURES GUIDE[5]

1. Aircraft impact
2. Avalanche
3. Coastal erosion
4. Drought
5. External flooding
6. Extreme winds and tornadoes
7. Fire
8. Fog
9. Forest fire
10. Frost
11. Hail
12. High tide, high lake level, or high river stage
13. High summer temperature
14. Hurricane
15. Ice cover
16. Industrial or military facility accident
17. Internal flooding
18. Landslide
19. Lightning
20. Low lake or river water level
21. Low winter temperature
22. Meteorite
23. Pipeline accident (gas, etc.)
23. Intense precipitation
25. Release of chemicals in onsite storage
26. River diversion
27. Sandstorm
28. Seiche
29. Seismic activity
30. Snow
31. Soil shrink-swell consolidation
32. Storm surge
33. Transportation accidents
34. Tsunami
35. Toxic gas
36. Turbine-generated missile
37. Volcanic activity
38. Waves

The net impact is that many of the potential vulnerabilities of "older" generation plants are not present in recent vintage designs. PRAs on recent vintage plants have indicated that there are typically only a few external events that may produce a significant impact on plant safety. These events are:

- o Seismic Events. Significant seismic event sequences typically result in either a loss of offsite power with failure of onsite sources or a massive failure of equipment due to a much greater than design basis earthquake.

- o Internal Flooding. Significant flooding event sequences typically result in a failure of redundant safety equipment that, in turn, results in the failure of a key plant safety function such as decay heat removal.

- o Fire. Significant fire event sequences involve internal fires and typically result in damage to instrumentation for key safety systems and controls or a loss of offsite power. Areas of the plant in which fire is very important are the cable spreading room, the turbine generator building, and the reactor control room.

- o Extreme Winds and Tornadoes. Significant tornado event sequences typically cause a loss of offsite power and a resultant demand on the onsite power sources. While there is some potential of failing equipment outside the auxiliary/reactor buildings due to tornado missiles, typically the equipment failure event sequences are not important in the risk assessment.

- o Sabotage and Terrorism. Although current regulations do not require quantitative assessment of sabotage and terrorism in the PRA, none the less the qualitative insights from the PRA can be used to identify plant and system vulnerabilities which can be addressed in the facility security plan.

Another insight based on past PRAs is that the impact of an external event on a plant has at times been site- or plant-specific. For future plants, the site-specific variances will, to some extent, be addressed by the requirements of the Standard Review Plan (see Reference 6) and other siting criteria (see Reference 14, for example). Plant-specific variances will be addressed by the development of a standard (certified) design for an advanced PWR. Thus, it is anticipated that the impact of external events will become less plant-specific. The selected site in each application of a standard design will conform to the site envelope for the standardized design, or exceptions will be addressed.

The NRC is currently involved in several efforts to assess the impact of external events related to plant safety. An external events analysis is being performed for the LaSalle plant under the Risk Methodology Integration and Evaluation Program at Sandia National Laboratory.[15] This effort is scheduled for completion by the end of 1988. In addition, the NRC staff has stated that the contribution of external events will be reviewed in the implementation of the severe accident policy; the NRC has a two-step process planned to review the impact of external events.[16]

The Industry Degraded Core Rulemaking (IDCOR) Program perspective on the external events is described in the document titled "The IDCOR Position Paper on Treatment of External Events within the Severe Accident Policy."[17] The IDCOR Program focused its in-depth evaluation of severe accidents in its reference plants on a relatively small set of dominant accident sequences that are important to public health and safety and which represented the range of system responses and important phenomena. With respect to system response and phenomena, these severe accident sequences were similar to or encompassed most sequences initiated by external events. For example, the severe accident analysis for a station blackout event included the important responses and phenomena that would be associated with a seismically induced loss of electric power. IDCOR did not evaluate separate accident sequences specifically initiated by large seismic events, fires, flood, or sabotage. In part, these events are already treated by an existing body of NRC regulations and/or NRC/industry programs.

The subsequent IDCOR Individual Plant Evaluation Methodology (IPEM) utilizes PRA techniques and insights gained from PRAs to develop an approximate core damage frequency profile for specific plants. The methodology treats external events such as flooding and fire qualitatively. These initiating events are addressed by evaluation of equipment in common locations without regard to explicit common-mode failure mechanisms.

Various methodologies have been developed and demonstrated for those external events that do require more extensive evaluation. For example, seismic events have been treated quantitatively using both traditional PRA and a margin analysis approach. Both approaches have been shown to be acceptable.

One external event which has not typically been addressed by risk quantification in any PRA is sabotage. Although there have been approaches adopted to address sabotage,[18] the general consensus is that the frequency of sabotage cannot be predicted with sufficient accuracy to be beneficial in assessing overall plant risk. In the more successful approaches, PRA plays a role in protecting the plant from sabotage by identifying qualitatively the equipment that is key to plant operation and the combinations of equipment, based on proximity for example, that could be vulnerable under certain assumed scenarios. This information is then utilized in the process that develops a security and sabotage protection strategy for the facility.

In summary, the general conclusion derived from past PRA experience is that external events as a group have been shown to be important to plant risk and that their evaluation in performing an advanced PWR PRA is appropriate. However, many of the listed external events (Table 1) may not require a detailed evaluation or accident sequence quantification, because of design improvements, siting requirements, or low frequency of occurrence. For such events, a qualitative evaluation can provide sufficient information to exclude the external event from further analysis. Some external events will require a more extensive evaluation, typically involving quantification, in the advanced PWR PRA.

Technical Approach to Resolve the Issue for Advanced PWRs

Resolution of this issue involves the specification of a comprehensive approach for selecting and including external events in the PRA to be used in licensing an advanced PWR. The list of external events in Table 1 (from NUREG/CR-2300) provides the starting point. The remaining elements of the approach are: a) qualitative evaluation and screening of the identified list of external events (Table 1), considering recent PRA experience, improvements in advanced PWR designs, and margins afforded by applicable siting criteria; and b) evaluation, using appropriate methodology, of those external events that do need to be addressed by the PRA or for which the PRA provides important insights. To resolve the issue, the approach must be sufficient to ensure that, when it has been implemented, the PRA will be comprehensive in ensuring consideration of the significant severe accident risks presented by external events for the advanced PWR.

The proposed approach for selecting and including external events in the advanced PWR PRA will be comprised of the following parts:

1. The first step in the evaluation of the events identified by Table 1 is the qualitative assessment of each external event to determine if it can be excluded from the analysis based on either design features, siting criteria, or other demonstrable basis for concluding that the event will not be a significant contributor to severe accident risk for the advanced PWR facility. These assessments ("screening" evaluations) include analogies from existing PRAs based on comparison of pertinent design features and requirements; such analogies may exclude previously significant sequences for an external event based on advanced PWR design features. Information contained in the PRA Procedures Guide (see Reference 5) and the siting requirements contained in Chapter 2 of the NRC Standard Review Plan (see Reference 6), for example, support other assessments.

As a result of a preliminary qualitative screening, it is ARSAPs conclusion that only internal fire, internal flooding, seismic activity, and certain contributors to the probability of loss of offsite power require further quantitative consideration in performing the PRA for an advanced PWR. The basis for this conclusion will be presented to the NRC staff during the interactions on this topic paper. The approach for sabotage and terrorism are addressed separately below.

2. A detailed quantitative analysis will be performed on the specified external events that have not been eliminated during the qualitative evaluation. The methods used to perform the quantitative analysis will be consistent with the methods described in the Electric Power Research Institute (EPRI) PRA Key Assumptions and Ground Rules Document (see Reference 14). The selected methods will provide an evaluation of the contribution to plant risk attributed to internal fire, internal flooding, seismic activity, and loss of offsite power (as impacted by extreme winds and tornadoes, lightning and forest fire) using PRA methodology.

   The events impacting only the probability of loss of offsite power are addressed in the PRA during the determination of the initiator frequency. Additional detail regarding the specific methodology to be used for the remaining events will be provided to the NRC Staff during review of this topic paper.

3. To treat sabotage and terrorism, a comprehensive security plan will be developed which complies with all current NRC regulations and guidance regarding the physical security of nuclear power plants. Current regulations and guidance do not require a quantitative assessment of sabotage within the PRA. However, a specific effort will be established to assure that qualitative insights about plant systems and equipment gained from the PRA (both potential vulnerabilities and design features that reduce the potential for sabotage/terrorism potential) are incorporated into the analysis that supports the development of the security plan.

References

1. U.S. Nuclear Regulatory Commission (USNRC), Policy Statement on Severe Reactor Accidents, Federal Register, Vol. 50, p. 32138, August 8, 1985.

2. Title 10, Code of Federal Regulation, Part 50, Appendix A, General Design Criteria.

3. W.R. Sugnet et al., Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3, Electric Power Research Institute Report NSAC/60, June 1984.

4. Commonwealth Edison Company, Zion Probabilistic Safety Study, Rev. 1, September 1982.

5. USNRC, PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, prepared for the USNRC by the American Nuclear Society and the Institute of Electrical and Electronic Engineers, January 1983.

6. USNRC, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition, USNRC Report NUREG-0800, Washington, D.C., July 1981.

7. USNRC, The Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, USNRC Report WASH-1400, NUREG-75/014, October 1975.

8. Title 10, Code of Federal Regulation, Part 50, Section 50.109, Backfitting.

9. USNRC, Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License, USNRC Report NUREG-0718, Rev. 2, January 1982.

10. Lawrence Livermore National Laboratory, Severe Accident Policy Implementation External Events Workshop, Annapolis, MD, August 4-5, 1987.

11. Pickard, Lowe and Garrick, Inc., Seabrook Station Probabilistic Safety Assessment, Report PLG-0300, December 1983.

12. Commonwealth Edison Company, Indian Point Unit 2 Probabilistic Safety Study, Rev. 0, September 1982.

13. American Nuclear Society, Guidelines for Combining Natural and External Man-Made Hazards at Power Reactor Sites, Standard ANSI/ANS-2.12-1978, La Grange Park, Illinois.

14. EPRI, Advanced Light Water Reactor Requirement Document, Chapters 1-5 and Appendix A: PRA Key Assumptions and Ground Rules (Section 3 addresses External Events), to be issued September 1988, (Draft, August 19, 1987).

15. Sandia National Laboratory, Risk Methodology Integration and Evaluation Program (RMIEP), to be published.

16. V. Stello, Treatment of External Events in the Implementation of the Severe Accident Policy Statement, USNRC Policy Issue SECY-86-162, May 22, 1986.

17. Industry Degraded Core Rulemaking (IDCOR) Program, IDCOR Position Paper of Treatment of External Events within the Severe Accident Policy, April 1987.

18. H. Martz and M. Johnson, "Risk Analysis of Terrorist Attack," Risk Analysis - An International Journal, 1, March 1987, pp. 35-47.

ARSAP Severe Accident Issue Topic Paper

3.2 Success Criteria and Mission Time

Issue Definition

This paper provides definition for top level success criteria and corresponding mission time as required to perform a PRA for advanced PWRs. Further, it provides a methodology for their application in the PRA analysis considering two safety related functions: The prevention of core damage and the maintenance of containment integrity.

Prevention of Core Damage

The overall core integrity success criterion is to prevent core damage. In order to demonstrate that this criterion has been achieved, a numerical success criterion based on core neutronic/thermal/hydraulic conditions is defined and then used to determine the minimal system configurations required to function in order to prevent severe core damage. To do this, the frontline systems are first evaluated for each accident scenario to determine those system configurations necessary to satisfy the defined criterion. As the event trees and fault trees evolve for the PRA, the support systems are also addressed within the framework of the acceptable configurations for the frontline systems. Hence, the defined core integrity success criterion, when applied, yields lower-level core integrity success criteria in the form of acceptable configurations for the frontline and support systems.

Given the success criteria, a core integrity mission time is also defined to provide an acceptable means of calculating accident sequence probability. The mission time value is used directly to calculate the time-dependent failure probability for the components analyzed in the PRA. During the quantification portion of a PRA, the core integrity mission time is multiplied by the time-dependent failure rate for each component to determine the time-dependent failure probability. Using Boolean expressions based on

potential failures and the acceptable configurations, these time-dependent failure probabilities are mathematically combined with demand failure probabilities, initiating event annualized frequencies, and human error probabilities to approximate the annual core damage frequency in the PRA. To properly estimate the core damage frequency for an advanced PWR design, an appropriate value for the core integrity mission time must be selected.

Maintenance of Containment Integrity

The overall qualitative success criterion for the containment is to maintain integrity for a specified time period. This qualitative success criterion can be related to a numerical success criterion by using the containment ultimate failure pressure. However, for the development of the plant damage states in the PRA the success criterion for containment integrity is effectively identical to the success criteria for the containment safeguard systems (i.e., operation of one spray pump and associated heat exchanger) because the operation of the safeguards systems in this minimum configuration is necessary and sufficient to insure that the containment parameters will be maintained below potential failure thresholds. Thus, an explicit numerical containment integrity success criterion is not required because the minimum acceptable safeguard configuration is known.

The phenomenological analysis performed as a part of the PRA does require a success criterion in order to assess the containment's ability to sustain potential containment loadings, i.e., hydrogen burns and associated pressurization, following core damage. This criterion is typically based on an assessment of the containment's ultimate capacity and is used in the development and evaluation of the containment event trees.

A mission time for containment support systems is defined to be the minimum time required for the safeguard systems to function in order to maintain containment integrity and prevent an unacceptable offsite release should a core damage event occur. Similar to the core damage mission time,

the mission time for containment support systems is used to quantify the time-dependent failure probabilities for containment systems.

This paper defines the above-described success criterion and mission times, together with a methodology for their use in deriving lower-level success criteria. The defined parameters will be used to develop and quantify PRAs, as called for in the NRC Severe Accident Policy Statement,[1] for advanced PWR designs submitted for NRC certification.

Historical Perspective

The use of PRAs in the licensing process has been developing and maturing since the completion of the Reactor Safety Study.[2] In general, the NRC has evaluated the acceptability of probabilistic methods on a case-by-case basis as individual studies have been submitted. The NRC has published several guides[3,4] on probabilistic methods, but the basis for and application of success criteria and mission time have not been specifically addressed.

Prevention of Core Damage

The PRA Procedures Guide (see Reference 4) states that the core integrity success criteria "... are based on a combined neutronics and thermal-hydraulics calculation of the plant response to postulated conditions." The guide also states, "Deterministic analyses may be required in some cases to define the success states realistically since much of the prior analyses of the plant may have been based on the conservative assumptions required by the licensing process." Finally, it stipulates that "... either FSAR analyses or FSAR success criteria ..." may be used in the absence of an integrated thermal-hydraulics analysis.

The traditional approach to satisfying these statements has been a combination of conservative regulatory requirements and best estimate deterministic thermal-hydraulic analyses. For example, some systems, such as the core flood system at Babcock and Wilcox (B&W) plants, are called upon

very early in an accident sequence. Since this state is modeled simplistically by the thermal-hydraulic codes for severe accidents (such as the Modular Accident Analysis Program or MAAP), the model-independent licensing criterion that 2-out-of-2 trains are required has been used as the success criterion for this system. For most other systems, severe accident thermal-hydraulic models were used to evaluate the overall response of different combinations of frontline systems to the postulated accidents.

Core damage has typically been assumed at the time of core uncovery for PWRs. More recently, the Electric Power Research Institute (EPRI) PRA Key Assumptions and Groundrules Document[5] has defined core damage based on the peak clad temperature; the threshold is defined to be 2200°F, a value established in 10CFR50.46.[6] Accident sequences that exceed this temperature tend to involve loss of long-term core cooling or inadequate inventory (loss of makeup). While this temperature is considered to be conservative, generally, the sequences that exceed 2200°F will, in a relatively short time, also exceed the 2800°F transition temperature at which the steam/Zircaloy reaction turns strongly exothermic. For these reasons, the 10CFR50.46 value is used in the EPRI Requirements Document as a core damage threshold applicable to best-estimate calculations.

The PRA Procedures Guide (see Reference 4) states that "system failures can represent...failures of components to operate throughout a specified interval...," where the "specified interval" is the core integrity mission time. Historically, the core integrity mission time has varied from 24 hours for the Reactor Safety Study (see Reference 2) to 8 hours for the Browns Ferry Unit 1 IREP.[7] Regulatory documents do not dictate a value or a selection process; the most commonly used value has been 24 hours, based on the precedent set by the Reactor Safety Study and judgments that it yields appropriate time-dependent failure probabilities. Finally, the EPRI PRA Key Assumptions and Groundrules Document (see Reference 5) specifies a 24-hour core integrity mission time, unless a specific component or system has a duty cycle that justifies a shorter time. The selection of 24 hours is based on a decision that "successful diagnosis of the problem and definition of the

necessary recovery actions to continue to provide the necessary function is judged to be very likely within this time."

Maintenance of Containment Integrity

Prior PRAs typically have defined a success criterion related to maintaining containment integrity in terms of the containment ultimate capacity. The core integrity mission time has been used for the development of accident sequences that included pertinent containment isolation and safeguards systems response. Thus, a conditional containment performance mission time given core damage was approximated based on the 24-hour core integrity mission time. No guidance has been provided by either the industry or the NRC for a separate mission time to model more accurately the maintenance of containment integrity.

The EPRI Requirements Document[8] defines a severe accident release goal, establishing a target for containment performance, as a maximum of 25 rem (over 24 hours) with a frequency of less than 1.0×10^{-6}/yr. However, a mission time to assure containment integrity that could be used for severe accident quantification has not been addressed.

Technical Approach to Resolve the Issue for Advanced PWRs

The technical approach to resolution of the success criteria issue is presented below. This section defines the methodology for determining core integrity success criteria, core integrity mission time, containment integrity success criteria and the mission time for the containment support functions.

1.0 Prevention of Core Damage-Success Criterion

The definition and methodology for establishing the core integrity success criterion and mission time will be a combination of regulatory

guidance and best-estimate analyses. The methodology is based on the following five key steps:

1. A peak cladding temperature of 2200°F will be used as the threshold for severe core damage when applied to best estimate calculations performed using a model with adequate spatial detail* to identify conditions sufficiently adverse to affect a significant fraction of the core (as distinct from a local perturbation such as results from a typical rod-ejection analysis). This value is significantly below the 2800°F exothermic transition temperature for steam/Zircaloy reactions, but this conservatism is expected to have little impact on PRA analyses since sequences that exceed 2200°F will typically also exceed 2800°F. Best-estimate inventory calculations demonstrating that there is no core uncovery afford an alternative means of conservatively demonstrating that the core integrity success criterion is satisfied.

2. Using a deterministic, best-estimate analysis code, the next level of core integrity success criteria for frontline systems will be determined. This realistic assessment is accomplished through an iterative process which varies the number and combinations of safety-related equipment trains. The outcome of this iterative process is the minimum equipment combinations that are capable of maintaining the peak clad temperature below the acceptance threshold defined in step 1.

3. Event trees will be developed based on the frontline systems core integrity success criteria to model pathways to core damage. Again, exceeding the threshold defined in step 1 will be the definition of a severe core damage condition.

---

* As an example, the typical MAAP nodal resolution (involving seven radial core rings with ten axial nodes in each) is sufficient.

4. Using best-estimate analyses, fault trees will be developed for each system. The fault trees will also provide a link between the frontline systems (safety injection, emergency feedwater, etc.) and the support systems (service water, power, etc.). This linkage enables the analyst to establish the lower-level support systems success criteria in association with the frontline systems success criteria.

5. As needed, the best-estimate analyses will be supplemented by hand calculations and computer codes to evaluate the required support system success criteria based on the status of the equipment and system conditions such as heat loads, degraded flow, and seal leakage.

This integrated approach links the lower-level core integrity success criteria (i.e., acceptable system configurations) for frontline and support systems, and ultimately individual components, to the top level definition of a numerical success criterion based on severe core damage. Sequences that fail to maintain the peak clad temperature below the acceptance threshold defined in step 1 will be treated as core damage sequences and will be addressed in subsequent phenomenological and consequence analyses.

2.0 Prevention of Core Damage - Mission Time

The determination of the mission time is based on the conditions of decay heat and available utility resources after an accident has occurred. Equipment that is required to function for extended time periods will be assessed for a core integrity mission time of 24 hours based on the following considerations:

1. The decay heat generation rate will have dropped to less than one percent of full power after 24 hours. This reduced heat load will decrease the demands placed on heat removal systems, as well as their support systems. Also, in the event of a loss of heat

removal, an extended period of time will be required before the temperature limit for severe core damage is reached. Therefore, the likelihood of recovering heat removal capability is high.

2. Based on operating plant histories, substantial utility resources may be mobilized to recover failed systems within 24 hours. For example, experience has shown that offsite power has been recovered within a maximum of 11 hours.[9] Similar timeframes for other crucial components are considered reasonable, given the prompt response customarily associated with such accident conditions.

3. Increasing the core integrity mission time to 48 or even 72 hours will only moderately affect the final results and will reduce the relative importance of demand failures; reducing the mission time to 8 or 10 hours tends to reduce the relative importance of time-dependent failures.

4. Equipment that is required to operate for less time may be assigned a reduced core integrity mission time, with justification, to give more realistic results. For example, if the high-pressure safety injection pumps were required to operate for only 6 hours during a particular accident sequence, after which time the decay heat removal system would satisfactorily handle the same function, then the core integrity mission time for the safety injection pumps can be reduced to 6 hours. This type of adjustment makes the analysis more realistic and increases confidence in the results.

To reiterate, the core integrity mission time will be defined as 24 hours, with reduced core integrity mission times, when justified, for equipment not required for the 24 hour period.

3.0 Maintenance of Containment Integrity - Success Criteria

The containment success criterion is comprised of two distinct criteria which are related to different tasks in the PRA. The containment success criteria for the development of the plant damage states will be based on the success criteria for the containment safeguards systems (i.e., operation of one spray pump and associated heat exchanger). This is appropriate because successful operation of these systems will preclude the loss of containment integrity.

The containment success criteria for the phenomenological assessment will be based on the calculation of the ultimate containment capacity. This value will be developed using a best-estimate analysis described in Section 4 of EPRI PRA Key Assumptions and Ground Rules Document (see Reference 5). That document describes the characteristics of the required analysis needed to determine the containment ultimate capacity.

4.0 Maintenance of Containment Integrity - Support Systems Mission Time

The containment support systems mission time for maintaining containment integrity is based on the plant conditions and available utility resources after an accident has occurred. Containment support systems equipment that is required to perform an active function for extended time periods will be assessed for a containment support systems mission time of 24 hours based on the considerations presented in Section 2.0.

However, the deterministic containment analysis shall not necessarily end at 24 hours. Instead, these analyses shall extend until either the situation has been stabilized or the containment has been breached.

References

1. U.S. Nuclear Regulatory Commission (USNRC), Policy Statement on Severe Reactor Accidents, Federal Register, Vol. 50, p. 32138, August 8, 1985.

2. USNRC, Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, USNRC Report WASH-1400, NUREG-75/014, October 1975.

3. R. A. Bari et al., Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815, USNRC, August 1985.

4. USNRC, PRA Procedures Guide- A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, ANS/IEEE, January 1983.

5. Electric Power Research Institute, Advanced Light Water Reactor Requirements Document, Appendix A: Key Assumptions and Groundrules, Palo Alto, CA, (Draft, July 1987).

6. Title 10, Code of Federal Regulations, Part 50.

7. S. E. Mays et al., Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant, NUREG/CR-2802, EGG-2199, U.S. Department of Energy, July 1982.

8. Electric Power Research Institute, Advanced Light Water Reactor Utility Requirements Document, Chapter 5: Engineered Safeguards Systems, Palo Alto, CA, December, 1987.

9. H. Wyckoff, Losses of Off-Site Power at U.S. Nuclear Power Plants--All Years Through 1986, Electric Power Research Institute Report NSAC/111, May 1987.

ARSAP Severe Accident Issue Topic Paper
3.3 Accident Sequence Selection

Issue Definition

The Nuclear Regulatory Commission (NRC) requires in its Severe Accident Policy[1] that a comprehensive probabilistic risk assessment (PRA) be conducted as part of the licensing of an advanced pressurized water reactor (PWR). An important step in conducting PRA will be the selection of accident sequences to be analyzed. This paper addresses the need for a standardized well defined method for accident sequence selection that assures that potentially important contributors to risk are included and that insignificant sequences are eliminated from further analyses.

The selection of accident sequences for advanced PWR analysis involves the following four steps:

- Identification of the plant operational states (e.g., full power, low power, etc.) to be considered in developing the accident sequences

- Identification of the initiating events for analysis considering the plant operational states identified

- Identification for analysis the plant systems and operator actions that significantly affect the response of the plant to each of the identified initiating events

- Selection of the cut off value to be used in the PRA to finalize the sequence selection.

When these four steps are implemented for an advanced PWR PRA, the accident sequences selected will represent the significant sources of risk (including the dominant sources) for the facility. The following discussion briefly describes each of these steps and shows the relationships among them.

The first step is the identification of the plant operational states (e.g., full power, less-than-full power, start-up, cold shutdown, or refueling conditions) to be considered in the PRA. The plant operational states impact which initiating events are assessed, and in turn, identify which systems must respond, or are available to respond, to the initiating events. Thus, the appropriate operational states must be defined in order to assure a comprehensive PRA.

The second step in the selection of accident sequences involves the identification of initiating events that could occur and warrant consideration for the identified plant operational states. Topic Paper 3.1 deals with the extent and manner in which external events are addressed in the PRA; this paper will therefore address only internal initiators. The internal initiators are identified by analyzing the potential failures of plant-specific systems (e.g., loss of service water), by reviewing available listings of initiators (e.g., the generic lists in the PRA Procedures Guide, previous PRAs, or studies of similar plants), and by investigating the operating history for the plant or similar plants. The identification of potential initiating events must be sufficiently complete to ensure that all of the important accident sequences will be determined.

The third step in sequence selection identifies those few plant systems and operator actions that significantly affect the response of the plant to each initiating event. The approach taken recognizes that each initiating event presents certain challenges to the attainment of a safe-shutdown condition. The plant functions necessary to achieve safe shutdown (e.g. inventory maintenance, core cooling, and containment integrity) in the face of these challenges are identified; event tree and fault tree logic models are then constructed to address the challenges and the functions for each initiating event. In these models, the successes and failures of the plant systems that must or may respond (under manual or automatic control) to the initiating events are depicted. The logic models, based on the applicable success criteria (addressed separately in Topic Paper 3.2), include the event elements that are both necessary and sufficient to determine the event outcome (including success or failure of the required functions).

In constructing the logic models, the ability of a plant system to respond to an initiator may be dependent upon the plant's state of operation and different combinations of systems may be required to function for different initiating events. For a complete analysis, the appropriate systems and operator actions must be included. Whenever the design of some of these systems, such as the Balance of Plant (BOP) systems, will not be completed for use in the analysis, a methodology for their consideration must nevertheless be provided.

The result of the first three steps is a large number of accident sequences defined by the event tree logic models. To finalize the sequence selection (step four), these accident sequences are quantified by combining the logic models with the data for initiating frequencies, operator error probabilities, and component failure probabilities. Part of the quantification process is the discrimination between potentially risk significant sequences (and cutsets) and the large number of insignificant contributors to the overall frequency of occurrence of core damage or radioactive release. A probability cutoff value is typically established to eliminate the insignificant contributors in the logic models. The probability cutoff value should be high enough to eliminate insignificant accident sequences (and cutsets) and thus control the scope of the analysis, but must not be so high that potentially significant contributors are eliminated.

In practice, the four steps are interconnected and are iteratively applied. Illustrating the interconnection, early quantification estimates are used in defining the relevant operational states, the initiating events to be considered, and the necessary breadth and depth of logic model development.

The above four steps define the accident sequence selection process necessary for completing the PRA and licensing of an advanced PWR design. The issue is summarized by the following questions:

- What plant operational states must be considered in the PRA?
- What internal initiating events must be analyzed in the PRA?
- What plant systems and what associated operator actions should be modeled in the PRA?
- What probability cutoff value should be used in the PRA to finalize the sequence selection?

This paper addresses these four questions and provides a technical approach for resolving the issue.

Historical Perspective

The use of PRAs in the nuclear power industry licensing process has been developing and maturing since the completion of the Reactor Safety Study.[2] The selection of accident sequences requiring analysis is important in performing such a PRA. The following sections discuss how each of the four steps for resolution of the accident sequence selection issue has been handled in past studies.

Plant Operational States

A nuclear power plant can operate at full power or at some lower power level; the plant can be starting up, shutting down, or refueling. The majority of completed PRAs have addressed events occurring when the plant is operating at full power with the expectation that these cases envelop any credible lower power, shutdown, or refueling cases.

A few PRAs have evaluated plant risks under low power and shutdown conditions. Long Island Lighting Company conducted three PRAs on its Shoreham Nuclear Power Station for three different plant operational states. The plant states analyzed were full power,[3] low power (up to 25% of full

power),[4] and start-up (up to 5% of full power).[5] Comparisons of these analyses demonstrated that the lower-power-state events were bounded by the full power analyses for this station.

Other studies also support an emphasis on full power conditions. An NRC investigation[6] found that the risk to the public and the potential for core melt conditions were considerably lower for plant operations under start-up conditions than had been calculated in the PRAs for full power operations. In addition, the Electric Power Research Institute (EPRI) report, EPRI NP-2230, states: "In general, transients occurring when plants are at low power levels have less potential for initiating significant consequences than those occurring when plants are at higher power levels."[7]

Nevertheless, potential events at low power conditions deserve some evaluation. This is true because the plant conditions in the shutdown state are different than when the plant is at full power. NSAC-52[8] identifies the differences by stating that, "Systems, procedures and administrative controls that are designed to ensure safe operation at power are not always adequate for safe operations during shutdown. Both safety priorities and operating philosophy can be significantly different when a reactor is in cold shutdown or refueling mode."

During shutdown and refueling, for example, the residual heat removal (RHR) system is used to remove the decay heat generated by the fuel and alternative systems may even be disabled for maintenance. Failure of the RHR system during shutdown or refueling, which would cause a loss of decay heat removal, could be a significant contributor to plant risk. Initiating events, such as this one, resulting in a failure to remove decay heat and consequent core heatup have been the main focal point for most of the studies that have investigated accidents during shutdown. Factors such as the low probability of being in the more vulnerable configurations and the long response times afforded by low decay heat levels for shutdown conditions must be considered, however, in assessing the risk significance of such potential event sequences, compared to full power events.

Identification of Internal Initiating Events

A set of initiators sufficiently complete to envelop risk-significant accident sequences is necessary for a comprehensive PRA. The identification of a specific set of initiating events to be used in a PRA requires a detailed knowledge of the applicable results of prior analyses and of plant-specific designs. Thus, internal initiators are usually identified by reviewing generic listings, by reviewing prior PRAs and studies of similar plants, by reviewing the operating history of the plant or of other similar plants, and by analyzing the design-specific systems to identify any unusual initiators of potentially significant events.

The internal initiating events typically identified consist of transients, loss of coolant accidents (LOCAs), steam generator tube ruptures (SGTRs), and design-specific initiators. The PRA Procedures Guide[9] discusses the identification of accident initiating events (transients). This guide and the Probabilistic Safety Analysis (PSA) Procedures Guide[10] both reference the EPRI report, EPRI NP-2230 (see Reference 7), on nuclear power plant operating experience as a starting point for identifying transients. The EPRI approach used industry operating experience to identify the various types of transients and the report presents an extensive list of initiators.

The identification and analysis of LOCAs in current PRAs have typically been conducted in accordance with the PRA Procedures Guide.[9] The various LOCA break sizes are usually established using thermal-hydraulic codes on a plant-by-plant basis. In addition, the reactor coolant system and its interfaces with other systems are investigated to determine if the reactor coolant inventory could be lost by other means. An SGTR is actually a special case of the LOCA with the additional facet that the lost reactor coolant inventory is not recovered. (It is also a sequence in which containment may be bypassed.)

The design-specific initiators are typically special transients that are caused by a failure of one of the support systems (e.g., service water). A review of plant-specific support systems and other unusual design features and their design bases is a typical starting point in identifying design-specific initiators.

Identification of Plant Systems and Operator Actions

The PRA Procedures Guide (see Reference 9) and the PSA Procedures Guide (see Reference 10) discuss the identification and analysis of important plant systems. Present PRAs have basically followed these guides, with the majority of them using event tree and fault tree logic models to depict the significant functional responses of the plant to the initiating events. The functions are built into the logic models in terms of the required systems and operator actions to perform them.

Quantification Cutoff Value

The use of a truncation or quantification cutoff value is discussed in the PRA Procedures Guide (see Reference 9) and the PSA Procedures Guide (see Reference 10). The latter guide references NUREG/CR-2728[11] for a suggested truncation value of 1.0×10^{-9}/yr, but allows the value to be relaxed provided accident sequences on the order of 1.0×10^{-6}/yr are not neglected.

The quantification cutoff value used in recent PRAs is typically between 1.0×10^{-6} and 1.0×10^{-8}. Because most PRA results have a core melt annual probability on the order of 1.0×10^{-4}, this cutoff value is between two and four orders of magnitude lower than the expected results. The EPRI Requirements Document[12] states that advanced PWR designs will have a frequency goal of 1.0×10^{-6}/yr for the large releases and a goal of 1.0×10^{-5}/yr for core damage. Therefore, it is reasonable to expect that the probability of core damage for the advanced PWR design dominant sequences will be on the order of 1.0×10^{-6} per year. This expected core damage probability must be factored into the decision on an appropriate cutoff value.

Technical Approach to Resolve the Issue for ALWRs

This section recommends a technical approach for resolving the issue of accident sequence selection for advanced PWRs. Each of the four selection steps is addressed for completeness.

Plant Operational States

The PRA will consider full power as the base case for analysis. As shown in previous studies (e.g., the Shoreham PRAs), the consequences of low power accidents, including start-up accidents, are typically not significant and are adequately bounded by the analysis of full power operations. To ensure that significant accidents, if any, during plant shutdown and refueling (primarily involving the failure of decay heat removal) are not overlooked, a review of design-specific support systems and any other new or innovative plant design features will be performed. If any potential vulnerabilities are identified for low power or shutdown conditions, they will be investigated as a special case during performance of the PRA.

Identification of Initiating Events

As recommended in the PRA Procedures Guide (see Reference 9), the list in EPRI report EPRI NP-2230 (see Reference 7) will be used as a starting point for identifying potential transients. The EPRI listing has been modified for this purpose by removing event 41 (fire within plant), which is considered to be an external event and is discussed in Topic Paper 3.1. The modified EPRI listing is provided as Table 1. The identification of the various LOCA locations and break sizes will be based on best-estimate thermal-hydraulic codes.

In addition, to ensure that all potentially significant initiating events are captured, the following three activities will be conducted:

TABLE 1
PWR TRANSIENT CATEGORIES

CATEGORY	TITLE
1	Loss of RCS Flow (1 Loop)
2	Uncontrolled Rod Withdrawal
3	CRDM Problems and/or Rod Drop
4	Leakage from Control Rods
5	Leakage in Primary System
6	Low Pressurizer Pressure
7	Pressurizer Leakage
8	High Pressurizer Pressure
9	Inadvertent Safety Injection Signal
10	Containment Pressure Problems
11	CVCS Malfunction - Boron Dilution Chemical Volume and Control System
12	Pressure/Temperature/Power Imbalance - Rod Position Error
13	Start-up of Inactive Coolant Pump
14	Total Loss of RCS Flow
15	Loss or Reduction in Feedwater Flow (1 Loop)
16	Total Loss of Feedwater Flow (All Loops)
17	Full or Partial Closure of Main Steam Isolation valve (MSIV) (1 Loop)
18	Closure of All MSIV
19	Increase in Feedwater Flow (1 Loop)
20	Increase in Feedwater Flow (All Loops)
21	Feedwater Flow Instability - Operator Error
22	Feedwater Flow Instability - Misc. Mechanical Causes
23	Loss of Condensate Pump (1 Loop)
24	Loss of Condensate Pumps (All Loops)
25	Loss of Condenser Vacuum
26	Steam Generator Leakage
27	Condenser Leakage
28	Misc. Leakage in Secondary System
29	Sudden Opening of Steam Relief Valves
30	Loss of Circulating Water
31	Loss of Component Cooling
32	Loss of Service Water Systems
33	Turbine Trip, Throttle Valve Closure, EHC Problems
34	Generator Trip or Generator Caused Faults
35	Total Loss of Offsite Power
36	Pressurizer Spray Failure
37	Loss of Power to Necessary Plant Systems
38	Spurious Trips - Cause Unknown
39	Automatic Trip - No Transient Condition
40	Manual Trip - No Transient Condition

1. The design will be analyzed for potential design-specific initiators that are caused by the failure of plant systems.

2. Past operating experience for the particular type of design will be reviewed, where available, for additional design-specific initiating events.

3. The reactor coolant system boundary will be searched for potential ways of losing reactor coolant inventory (e.g., reactor coolant pump seals), in addition to line breaks.

Identification of Plant Systems

To ensure that the proper plant systems are modeled, the available operating and emergency response procedures will be reviewed to determine the most likely systems to respond to an accident condition. This effort is closely related to the derivation of lower-level success criteria discussed in Topic Paper 3.2. In addition, available simulator data for similar designs will be utilized to aid in the modeling of the actions of the operator.

The plant systems that require analysis will be analyzed in accordance with the PRA Procedures Guide (see Reference 9). For the systems that are not fully defined, if any, at the time of a PRA supporting an application for design approval or certification (these will typically be BOP systems), sensitivity analyses will be conducted to determine the potential impact these systems could have on the plant within the performance envelope afforded by the requirements established for the systems. These sensitivity analyses will address various possible system configurations, based on designs outlined in the EPRI Requirements Document[12] and reasonable extensions of these system designs, consistent with the specified interface requirements.

Quantification Cutoff Value

Initiating events, accident sequences, and cutsets that fall below an annual probability or frequency of occurrence of 1.0×10^{-8} will be eliminated from further analysis in the PRA. This quantification cutoff value is two decades below the design goal for large releases and three decades below the core damage frequency goal established by EPRI for advanced PWRs. For the expected level of detail in the event trees, events and sequences that occur less frequently than this quantification cutoff value are considered to be either not credible or not significant when determining the overall probability of core damage or radioactive release.

Caution must be exercised in applying the cutoff value, however, in that overpruning of the logic models could result in deletion of portions of the overall model that might later prove significant as the PRA evolves or as sensitivity studies are performed. To ensure that the application of the cutoff value does not lead to such a result, the cutoff frequency will only be applied if the calculated frequency for elements being deleted (i.e., cutsets or accident sequences) is at least two orders of magnitude below the cumulative frequency of comparable elements being retained (i.e., other cutsets for the same accident sequence or other accident sequences resulting in the same plant damage state).

References

1. U.S. Nuclear Regulatory Commission (USNRC), Policy Statement on Severe Reactor Accidents, Federal Register, Vol. 50, p. 32138, August 8, 1985.

2. USNRC, Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, USNRC Report WASH-1400, NUREG-75/014, October 1975.

3. Shoreham Nuclear Power Station Full Power PRA, Long Island Lighting Company, June 1983.

4. Shoreham Nuclear Power Station Low Power PRA (Up to 25% of Full Power), Long Island Lighting Company, March 1987.

5. Shoreham Nuclear Power Station Low Power PRA (Up to 5% of Full Power), Long Island Lighting Company.

6. USNRC, Safety Evaluation Report, LaSalle County Station (Units 1 & 2), Docket Nos. 50-373; SSER #3.

7. Electric Power Research Institute (EPRI), ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI NP-2230, January 1982.

8. Nuclear Safety Analysis Center (NSAC), Residual Heat Removal Experience Review and Safety Analysis - Pressurized Water Reactor, NSAC-52, January 1983.

9. American Nuclear Society (ANS)/Institute of Electrical and Electronics Engineers (IEEE), PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, January 1983.

10. USNRC, Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815, August 1985.

11. USNRC, Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, July 1982.

12. EPRI, Advanced Light Water Reactor Utility Requirements Document, Palo Alto, CA, In review.