1 of 1

NEGG/IND037 022290-Del. Ver.

SAVANNAH RIVER SITE PROBABILISTIC RISK ASSESSMENT HIGH-LEVEL REVIEW

Savannah River Site
Aiken, South Carolina 29808

DISCLAIMER

DOE Contract No. **DE-AC09-89SR18035**

"DELETED VERSION"

SAVANNAH RIVER SITE PROBABILISTIC RISK ASSESSMENT

HIGH-LEVEL REVIEW

Committee Chairperson
B. John Garrick (PLG, Inc.)

Committee Members
Dennis C. Bley (PLG, Inc.)
Robert J. Budnitz (Future Resources Associates, Inc.)
Helmut Filacchione (Scientech, Inc.)
Karl N. Fleming (PLG, Inc.)
R. Niall M. Hunt (EG&G Idaho, Inc.)

Prepared for
U.S. DEPARTMENT OF ENERGY
Washington, D.C.
February 1990

"DELETED VERSION"

DISCLAIMER

ACKNOWLEDGEMENT

The SRS PRA Review Committee is very grateful to the technical assistance provided by Mr. John P. Kindinger of PLG, Inc., and Mr. Harry J. Reilly of EG&G Idaho, Inc. We wish to also acknowledge the advice and direction we received from Mr. Kenneth G. Murphy of the U.S. Department of Energy, Washington, D.C.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. EXECUTIVE SUMMARY

1.1 BACKGROUND

A review of the Savannah River Site (SRS) Probabilistic Risk Assessment (PRA) has been performed by a review committee organized by the U.S. Department of Energy (DOE) and its contractor, EG&G Idaho, Inc. The High-Level Peer Review Committee (referred to as "the Committee" in this report) members are identified in Section 2. The main purpose of the review has been to provide assurance that the SRS PRA is responsive to safety issues associated with the restart and continued operation of the Savannah River reactors.

The Committee members are all experienced practitioners of PRA, and several of the members have been deeply involved in a concurrent, detailed review of the SRS PRA.

Source material and expertise available to the Committee included the SRS PRA document itself issued August 31, 1989, and interaction with key PRA and plant experts at both the Savannah River Site and the Los Alamos National Laboratory (LANL), who had performed an independent PRA evaluation of the SRS K-reactor. The cooperation and support received from those connected with the review were outstanding.

1.2 MAJOR CONCLUSION

The Committee does not see any safety issues resulting from the SRS PRA that would be cause for delaying restart of the K-reactor at the Savannah River Site. Moreover, the Committee has not observed any ongoing restart activity that would be inconsistent with the PRA that has been performed, although our review was limited in this regard.

1.3 FAVORABLE IMPRESSIONS

In the course of the review by this Committee, there were a number of very positive observations concerning the SRS PRA, the risk analysis team assembled, and the strong management support from Westinghouse Savannah River Company (WSRC). There is strong evidence that the risk management program at the Savannah River Site will be successful. The principal underpinning of that evidence is the commitment displayed by management to support the risk activity as an ongoing and essentially real time function.

The risk analysis group has evolved into an outstanding team. This team definitely thinks PRA in its daily activities; i.e., when looking at the plant, it puts equipment design and performance as well as procedures and operator aids in the context of the PRA. Its focus is clearly on risk management, not simple compliance.

The risk model appears to be a good representation of the K-reactor. The PRA team has been effective in reaching out for engineering analyses that have already been made on the plant, using innovative methods for identifying initiating events and modeling electric power, and consulting with outside experts where plant capability was not clear.

1.4 SRS PRA ENHANCEMENT OPPORTUNITIES

There are a number of areas in which the SRS PRA could be improved, even though they are not believed to be the kinds of improvements that will significantly change the PRA results. The recommended improvements will enhance the utility of the PRA and thus the ease and effectiveness of the PRA as a risk management tool.

Perhaps the most significant opportunity for improvement of the SRS PRA is in the area of documentation. The Committee had to depend heavily on direct communication with the risk analysis team to resolve numerous issues. These issues included the basis of the success criteria, the confidence (uncertainty) in the results, the use of computer codes, the fine structure of the quantification process, the completeness of the event tree model, the details associated with data handling, the method of initiating event identification, and the role of procedures and human actions in the modeling process.

On the technical side, there are several improvement opportunities that would greatly enhance the usefulness of the PRA, especially by safety professionals who are not a part of the risk analysis team. (These include operational and engineering experts connected with the reactors who will have much to say about the success of the use of the PRA to perform meaningful risk management of the plants.) Prominent among these improvement opportunities are the need for a model that is much easier to requantify for risk management applications, a more comprehensive description of the key sources of uncertainty to facilitate interpretation of the results, a clearer presentation of equipment dependencies including human interaction, a more up-to-date treatment of data and human performance analysis, a more convincing case for the extremely low contribution to risk from fires, a consideration of alternative seismic hazard information in the seismic analysis, and a clearer logic structure for supporting the choice of initiating event categories. It is also clear to the Committee that a better interface needs to be established between the Level 1 and Level 2 portions of the risk model.

These improvements are believed to be important to place the PRA in its proper perspective. In its current form, there is an implied precision in the results that could compromise decisions on corrective actions. In particular, the rank order of contributors as they are currently presented probably overfocuses on what is really most important to risk. In the final analysis and if the results were decomposed somewhat differently, probably the most important issues would relate to operator training, procedures, proper equipment inspection and surveillance, and emergency response.

1.5 FINAL COMMENTS

This leads to a final observation that suggests that when the risk assessment is completed, risk analysis and risk management just begin. The point is that it is extremely important to carefully examine those events now identified as contributors to risk to understand, at a more basic cause level, just what they mean. It is the analysis at this level that will provide the basis for the most effective decisions for controlling risk.

The Committee is aware that LANL has a DOE contract to perform independent probabilistic safety analyses of the K-reactor and that the LANL PRA team has prepared an Engineering Insights Report based on these analyses. This Committee recommends that LANL's findings

be reviewed by DOE to ensure that none of the findings are of such significance that they would warrant resolution before restart.

2. INTRODUCTION AND PURPOSE

EG&G Idaho, Inc., under contract to DOE, has organized a High-Level Peer Review Committee to review the SRS PRA covering the K-reactor. This is a report covering that review.

The objective of this report is to provide an independent, high-level review of the SRS PRA to ensure that:

- All potentially significant scenarios identified in the PRA have been addressed in the K-reactor restart program.
- Any results, insights, or other information that might be taken from the SRS PRA can be confidently used to augment the safety analysis in the resolution of items required for the SRS restart.
- No known restart activities have a negative impact on the results of the PRA.

The review by the Committee covers the Level 1 PRA for both internal and external events. The approach taken by the Committee is to focus on key issues affecting the safety of the K-reactor and to conduct the review from the top down. The members of the Committee and their affiliations are as follows:

B. John Garrick, PLG, Inc. (serving as chairperson of the Committee)
Dennis C. Bley, PLG, Inc.
Robert J. Budnitz, Future Resources Associates, Inc.
Helmut Filacchione, Scientech, Inc.
Karl N. Fleming, PLG, Inc.
R. Niall M. Hunt, EG&G Idaho, Inc.

The review of this Committee is separate from, but dependent on, a detailed review of the SRS PRA being conducted by EG&G Idaho, Inc., with support from PLG and Scientech.

The key questions that have guided this review are as follows:

- What are the key issues, according to the SRS PRA?
- Are these issues well founded technically?
- In the judgment of the Committee, what issues, if any, have been overlooked?
- In the opinion of the Committee, do any of the issues impact the safe restart and operation of the reactor?

The first question was answered by the SRS PRA and is highlighted in Section 3. The remaining questions are addressed in Section 7, with additional backup in Sections 4 through 6.

3. KEY RESULTS OF THE SRS PRA

The core damage frequency results for the SRS Level 1 PRA are dominated by internal and seismic events. Table 1 lists the total core damage frequency from seismic and internal events and the percentage contribution of each SRS initiating event class to these totals.

Table 2 lists the seismic sequences that are most important to core damage. Table 3 lists the corresponding internal event sequences that are most important to core damage risk. Table 4 presents the components or class of components having the highest importance to core damage frequency. Table 5 presents the major insights derived from the internal events results by the SRS PRA team. Finally, Figure 1 graphically depicts the high-level breakdown of core damage contributors by initiating event categories.

Table 1. SRS Level 1 PRA Summary of Results		
Description	**Seismic**	**Internal Events**
Total Core Damage Frequency per Reactor-Year	2.4×10^{-4}	2.1×10^{-4}
Contributors		
Loss of Coolant Accident	21%	58%
Loss of Pumping Accident	59%	23%
Transients	0%	8%
Loss of River Water	1%	6%
Loss of Heat Sink	19%	5%

Table 2. Important Seismic Sequences (P-Reactor As-Is Results)		
Sequence	**Description**	**Mean Frequency**
1	Loss of Process Water Flow and ECS	4.48-5
3	Loss of D_20 Inventory and ECS	4.91-5
26	Failure of Underground Cooling Water Piping and In-Building Piping	1.39-4
All Others		< 1.0-6
	Total	2.37-4
Note: Exponential notation is indicated in abbreviated form; e.g., 4.48-5 = 4.48×10^{-5}.		

Table 3. Dominant Internal Events Sequences		
Sequence Description	**Annual Core Melt Frequency**	**Percentage of Total**
Bellows Break in Process Water System and Failure To Inject Emergency Coolant	6.6×10^{-5}	28
Large Cooling Water System Pipe Break and Failure To Inject Emergency Coolant following Flooding	4.2×10^{-5}	18
Bellows Break in Process Water System and Overthrottling of Emergency Coolant	1.9×10^{-5}	8
Transient with Failure To Shutdown	1.6×10^{-5}	7
Large Process Water System Inlet Plenum Pipe Break in Line Containing ECS Path with Throttling	1.5×10^{-5}	6

Table 4. Internal Events Component Results Summary	
Component or Component Class	**Core Damage Frequency (percent)**
Piping	82
Expansion Joints (bellows)	61
Manual Incident Action	49
[redacted] Series Valves	17
Throttling ECW [redacted] Series Valves)	10

Exemption (b)(3)

Exemption (b)(3)

Table 5. Internal Events Insights

- Manual incident action is a driver (50% of core melt frequency).
  - Extending response times improves result ([PEL] pump trip). Exemption (b)(3)
  - Adding AIA and/or MRS (for LOCA response) improves result.
- Electric power system is not a driver.
  - Gravity flow and dedicated process water diesels reduce LOSP significance.
- The [PEL] ECS valve reliability is low (compared with [PEL] Exemption (b)(3)
  - Additional testing/maintenance is required.
- Expansion joint breaks dominate risk (60% of core melt frequency).
  - Initiator frequency is more than 90% attributable to expansion joints.
  - MRS is a significant benefit.
- Operator interface is important to plant risk.
  - Improved training and procedures are required.

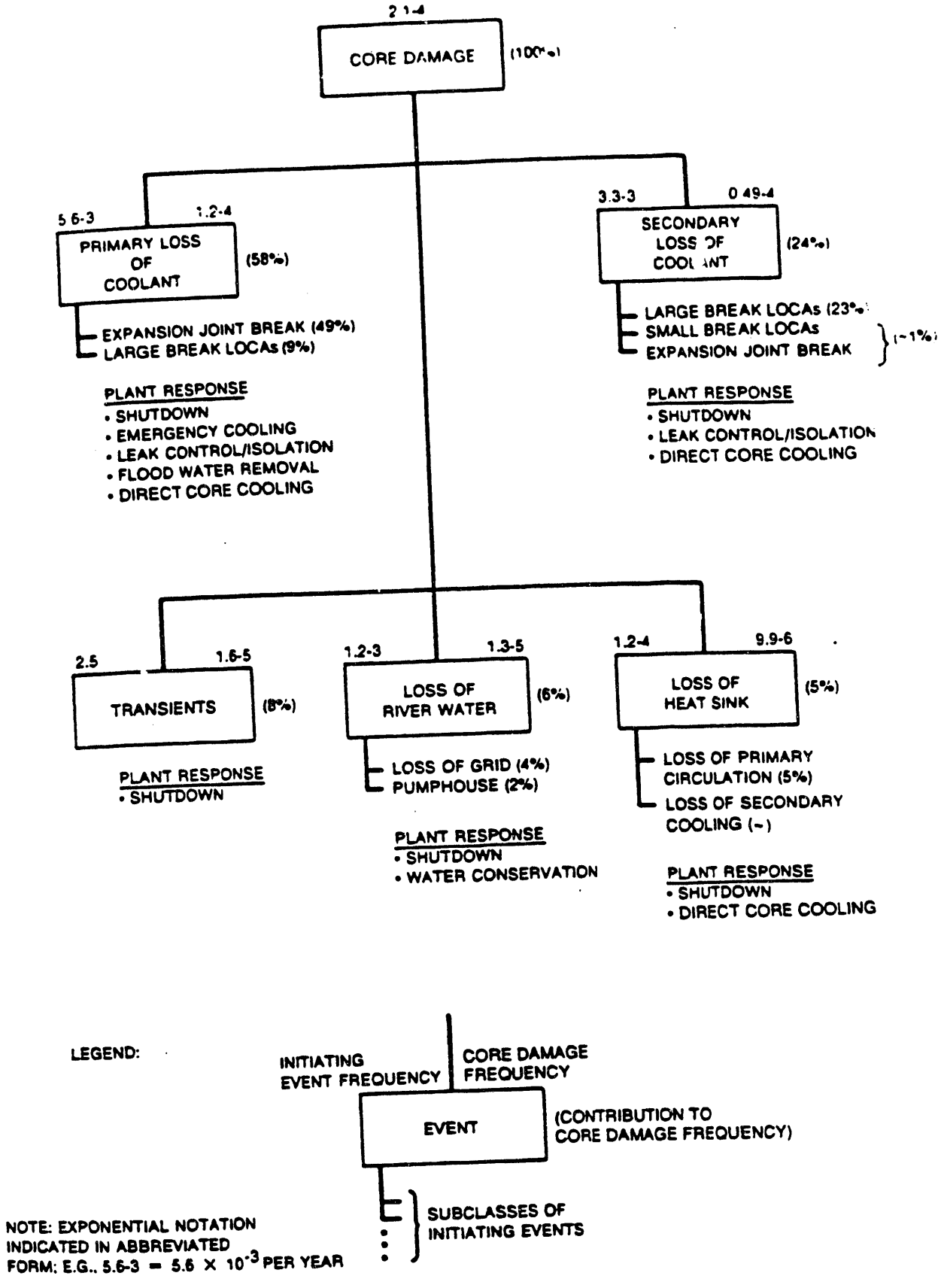


Figure 1. Summary of SRS PRA Results Initiating Events (Internal Events Only)

4. METHODOLOGY

4.1 MODELING APPROACH

For the Level 1 analysis of internal events, the PRA effort was defined in terms of seven major task areas. Figure 2, taken from the SRS PRA, identifies these seven areas and illustrates the general flow of information among them. The methods employed to define the contents of these tasks and to perform the calculation of results generally follow what is termed the "linked fault tree" approach to PRA as defined in NUREG/CR-2300, "PRA Procedures Guide." One area in which the internal events model departs from typical PRA practice is in the use of a separate Markov model for the analysis of the electric power system. (Details of this model were not included in the PRA report for review.)

External initiating events are evaluated individually for the SRS PRA, using different methods for each type of external event. It has become more common in recent light water reactor PRAs to examine external events using the same event tree/fault tree logic model developed for internal events, with special boundary conditions to account for the effects of the external initiators. This practice eases analysis of concurrent random unavailability and helps to ensure consistency in modeling internal and external events.

Another important methodological feature of the SRS PRA was the definition of the end state for the Level 1 analysis. The Level 1 SRS PRA ends with the determination of core damage: that is, each event tree sequence ends in "melt" or "no melt." In many Level 2 and Level 3 PRAs, the Level 1 analysis is expanded beyond the melt/no melt determination to examine the status of containment (or confinement) conditions. The end states of the Level 1 analysis are then called "plant damage states," and they communicate important information regarding the status of containment integrity and availability of active containment/confinement systems to the Level 2 analysis. By ending the Level 1 SRS PRA at melt/no melt, the definition and calculation of plant damage state frequencies are deferred to the Level 2 work.

4.2 QUANTIFICATION

A number of conservative screening values and cutoff probabilities were used during the quantification process. The use of screening data is mentioned in several sections of the SRS PRA, but there is no indication as to whether the screening values were reevaluated after the initial quantification to ensure that overly conservative values (e.g., the values for common cause failures and the assumption of 0.33 failures for no experienced failures), individually or collectively (cumulative effect), do not affect the overall core damage frequency and the core damage profile.

The SRS PRA states that the fault tree gate cutoff probability was set at 10^{-9}, with two exceptions where a value of 10^{-8} was used. The SRS PRA team told this Committee that a bar chart technique was used to trace the increments in frequency with increasing orders of cutsets to ensure that truncation of higher order cutsets does not lose important information.

The fault tree models contain an unusual number of flags to change the tree structure for sequence-specific boundary conditions. A spreadsheet was developed to keep track of the flags and to ensure their correct setting. The SRS PRA does not state whether the

spreadsheet underwent a quality assurance process, and it does not discuss the process used to ensure that the proper values for the flags in a sequence were used. Independent basic events were combined in consolidated basic events (modules) for the purpose of reducing the size of fault trees without losing information.

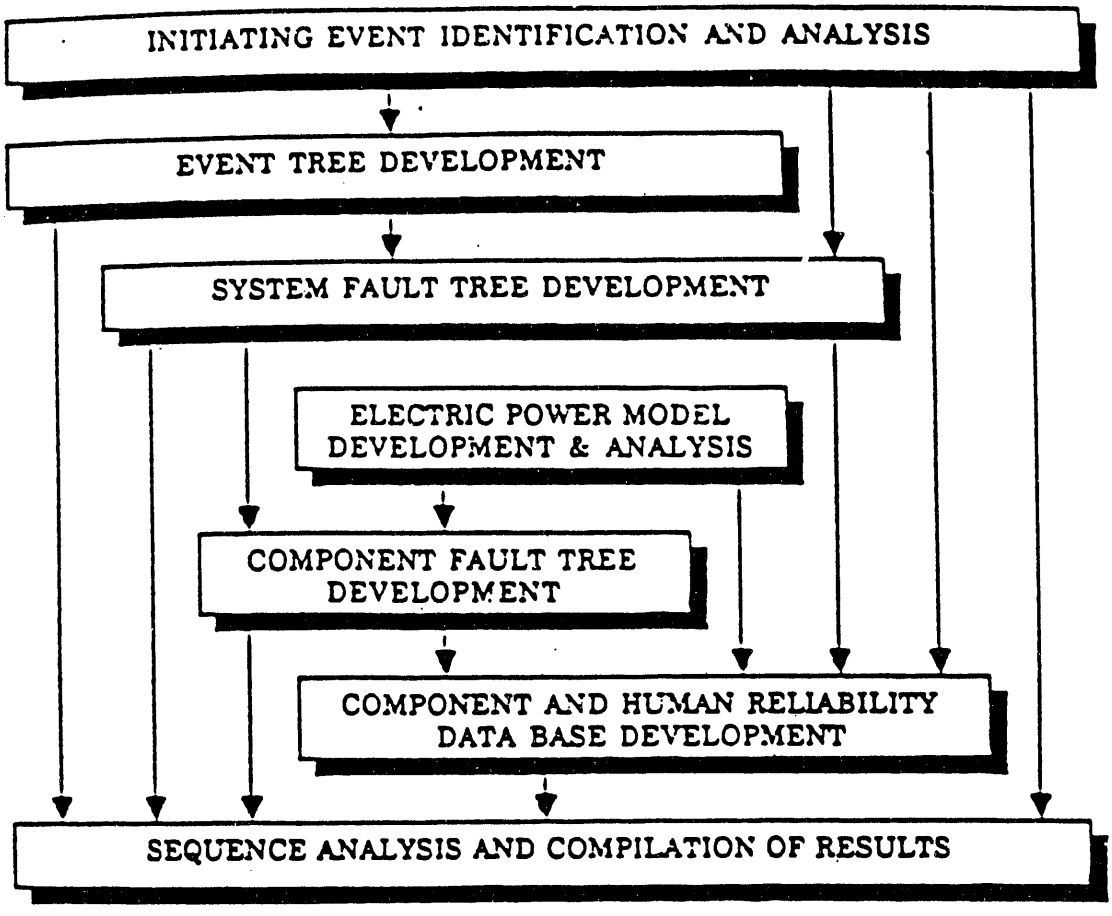


Figure 2. Overview of Level 1 PRA Methodology Information Flow

5. ANALYSIS OF SRS PRA

5.1 EVALUATION OF THE METHODOLOGY EMPLOYED IN THE SRS PRA

5.1.1 Internal Events Analysis

The PRA solves linked event tree/large fault tree models to identify the sequence cutsets and their frequencies. Each constituent part of their analysis will be evaluated individually below.

1. **Initiating Events.** A brief examination of initiators identified by the dendograms and the MLD and a comparison with those identified within a generic, high-level, hierarchical, core damage prevention description showed no omissions. However, there is no evidence presented in the PRA to indicate that an exhaustive search for initiating events that originate within plant support systems and lead to plant transient events was conducted. These "special initiators" can be important because they not only trigger the need for mitigative actions but also can simultaneously reduce the availability of plant safety systems or the availability of information needed by the plant operators as they respond to the event.

2. **Event Trees and Success Criteria.** Based on discussions with the PRA team, success criteria were primarily extracted from information contained in plant procedures (DPSOLs). That information was tempered by judgment of the PRA team based on experience with the plant, review of existing SRS engineering/physics analysis, and some recent analysis done in support of the PRA. Therefore, it appears that the current event tree models generally exhibit good fidelity to the real plant. In some cases, success criteria are probably conservative, or at least represent the high end of the SRS uncertainty band for risk of severe core damage. In other cases, there may be specific scenarios within an event tree sequence for which the success criteria are optimistic. If so, the judgment is that such cases are unlikely; i.e., they are not expected to have substantial impact on the mean frequency of severe core damage.

   To reduce the complexity of the PRA and to minimize the number of scenarios to be evaluated, four simplifications were instituted: eliminate most accidents beginning at shutdown, eliminate compound initiating events, forgo analysis of low probability events, and regroup LOCAs into a few subclasses.

   a. ***Accidents Beginning at Shutdown.*** Because the reactors spend more time at power than at shutdown and because there is a "somewhat narrow window of vulnerability to damage, namely, the interval after shutdown when fission product decay power is high enough to cause damage quickly," the PRA team expects the shutdown risk to be small, and they dismissed most shutdown scenarios. However, they included shutdown events for rod withdrawal transients and loss of heat sink initiating events, by adding "the contribution from shutdown accidents...to the initiating event frequency...at full power."

      Without additional analytical support, these arguments are not convincing for two reasons. The first argument is similar to that previously used in

commercial PWR PRAs. It was found to be optimistic there, when shutdown risk was analyzed more carefully. This was because, during shutdown,

- Many systems are disabled.
- Certain leak paths and possibilities for interrupting cooling exist that are not present at power.
- Almost all response is manual.
- Many accident conditions are not alarmed and can easily be missed for long periods of time, especially on back shifts.

The second argument, that shutdown scenarios can be included by elevating the "at-power" initiating event frequency, suffers from some of the same problems enumerated above. While the cooling requirements may be less stringent, the initiating event frequency and the unavailability of plant systems may be less favorable than at power. It is not clear to us that such possibilities received sufficient consideration. Also, a review of the master logic diagram leads to the conclusion that important initiating events at shutdown could originate as operator errors (crane accidents—A.3.11, and events 65, 32, 46 41, 21, 22), which lead to loss of control of process water system integrity. There does not seem to be sufficient justification to eliminate these events without a more detailed estimation of their likelihood and effects.

b. ***Compound Initiating Events.*** The transient event tree was simplified to consider only failure of the shutdown system; failure of the normal cooling system was eliminated because no significant contribution to risk was expected from cooling system unavailability due to its short mission time. The arguments for this approximation are convincing. However, for a similar scenario in the fire analysis, shutdown was considered to be negligible (dropped from the model), and only loss of normal cooling was modeled. It appears that failure to shut down should be included in the fire analysis.

c. ***Forgo Analysis of Low Probability Events.*** The PRA team assumed failure of certain systems, where significant simplification does not introduce appreciable pessimism into the quantification. The claim that this assumption is always conservative sounds reasonable to us. However, care must be applied; could it be possible, for certain unlikely scenarios, that system success actually aggravates the accident or complicates operator response?

d. ***Subclasses of LOCAs.*** An attempt to identify all pipe failure possibilities that have different success criteria or different impact on the probability of failure of plant equipment led to many classes of secondary LOCA—17 at power and 22 when shutdown. A similar, but less extensive, situation applied to primary LOCAs. A reduced number of leak sizes was selected, but no details about the basis for selection of success criteria is given in the report.

3. **Systems Analysis.** Fault tree analysis was performed on SRS systems. There are several aspects of the system modeling that raise our concern.

a. ***System Modeling and Identification of Intersystem Dependencies.*** Functional or intersystem dependencies are described qualitatively within the system descriptions found in Appendix I of the SRS PRA. The system and component fault trees then display, as basic events, those systems required as support for the system or component of interest. The modeling of intersystem dependencies appears to have been performed reasonably well for dependencies on AC electric power and cooling water, but not as comprehensively for other support systems such as instrument air or DC power. This observation appears to be confirmed by the LANL PRA results, which reportedly have identified some sequences involving support system failures that were not evident in the SRS PRA.

The methods employed in construction of the fault trees that are consistent with those used in other commercial reactor PRAs appear to have been implemented properly by the plant technical staff. One of the less conventional approaches used in the PRA, the combination of the Markov electric power models with the system fault trees, raises concern because of the need for high levels of quality control to ensure that the complexity of the solution does not result in the introduction of errors. However, that analysis has not been available for review, and the results seem to be reasonable.

b. ***Data.*** The extent to which the PRA team has used plant-specific information to develop failure probabilities is admirable. However, there does not appear to be a great deal of evidence to show that time-dependent failure rates are not a factor of importance as the plants age. The PRA does not provide evidence to indicate that extensive data trending was performed, and it does not show that estimates of failure probabilities generated from historical statistics will be effective predictors of future hardware performance.

The database also appears to focus primarily on the contribution to component unavailability from failures and corrective maintenance, whereas little is said of unavailability due to preventive and scheduled maintenance. There is no documentation in the PRA to indicate that the plant operating cycle allows sufficient opportunities for maintenance during shutdown and that component unavailability due to planned or scheduled maintenance at power is not important.

Of additional concern is the process by which failure probability estimates were generated for plant data, when no previous failures have been identified. In these cases, an effective value of 0.33 (or 1/3 of a full failure) was assumed for the numerator. This value, which drives the frequency of core damage for the K-reactor, is generally conservative, except for the possibility of aging. The selection of this value is not adequately supported, and the Committee recommends the calculation and/or selection of more objective values based on plant experience (partial failures and expert opinion). This is especially important for the dominant sequences that include equipment for which there is zero failure experience. For example, the contribution of primary loss of coolant accidents (LOCA) represents more than half of the total frequency of core damage, but the estimated frequency for a primary LOCA is directly driven by the assumed value of 0.33. This indicates the importance of the need for a less subjective estimate in these cases.

c. ***Common Cause Analysis.*** Common cause or common mode failure mechanisms are addressed in the SRS PRA at the component fault tree level. Contributors to common cause failure for a group of like components are identified under a "group consolidated" basic event within a component fault tree. These contributors may be either hardware- or human-related failure mechanisms. For hardware-related common cause contributors, a beta factor approach was used to quantify their likelihood. Conservative screening values of .1 for two components or .05 for three or more components were used for the value of beta.

The Committee believes that the common cause analysis for system failure probabilities was generally performed systematically and that the quantitative values used are conservative. The common cause events in the fault tree were quite thorough and more complete than most PRAs. However, it appears to be necessary to replace the existing beta factors with a set derived from plant data, particularly for those common cause failures that are significant contributors to core damage frequency. The PRA team can find suggestions in NUREG-CR/4780 on how to accomplish this.

The method used for common cause analysis of equipment whose failure leads to an initiating event appears to be incorrect, as described below, and should be revised. This would affect the transient initiating event frequencies used in the PRA.

The Level 1 PRA report states that the beta factor conservatively estimates the frequency of initiating events, when the mission time is approximately 1 year. Therefore, a time-dependent expression was used to replace the conventional beta factor model. This model assumes that the probability of common cause failure is equal to the probability that one component will fail randomly, sometimes before the mission time, T_M, times the probability that the remaining components will fail during the repair time, T_R, of the first component. It is assumed that the rate of failure during repair of the first component would be increased by a common mode factor (CMF), which accounts for the possibility that failure of the first component may have been due to a causative reason that would affect other components, and would fail other components at a higher rate. This model is not a probabilistic or physical representation of time-dependent common cause failures, and does not represent common cause phenomena and failures.

The Committee recommends that the PRA team use a different model than that proposed, and revise its time-dependent common cause calculations by employing either the more conservative beta factor model or a more accurate, but also more elaborate, time-dependent model, such as the Mosleh and Zikria model.

4. **Human Reliability Assessment (HRA).** The techniques used in the HRA of the SRS PRA appear to be less than the current state of the art. This is of particular concern since human actions are an integral and important contributor to the safe operation of the facility.

THERP was the predominant technique used in the assessment of the human error probabilities, and was justified, in part, by the fact that operators do not have extensive diagnostic tasks to perform and operate predominantly in the rule-based region of human behavior. THERP is a good tool under these circumstances.

However, the plant is currently developing symptom-based procedures to augment the existing event-based procedures. Presumably, this is being done to ensure that the operators remain in the rule-based region, even when they are unable to diagnose the specific nature of the event with which they are dealing. This tends to imply that there are conditions under which diagnostic requirements exist, and contradicts the "non-diagnostic" character assumed with THERP.

Since the human reliability analysis described in the PRA does not address this seeming contradiction, the omission of diagnostic error contributions to the calculated human error probabilities would appear to introduce the potential for underestimation of the error probabilities.

If the above inferences are correct, attempts to modify the existing HRA to include the implementation of the new symptom-based procedures will show no net benefit, unless it is in the form of enhanced probabilities for recovery actions. It is our understanding that significant improvements to the HRA are planned.

5. **Quantification.** The quantification process follows the general approach used with the large fault tree linking method. Of concern is the complexity of the analysis, which is increased by the use of a Markov model for the electric power system. This led to the need to use "flags" to turn on and off various parts of the models on and off to accommodate the various possible plant electrical system states and sequence success criteria. No practical way could be found to check the computations, apart from an independent requantification, which was beyond the scope of this or the detailed review.

The PRA indicates the general use of 1×10^{-9} as a cutset truncation value, with two exceptions in which 1×10^{-8} was used. To provide a measure of the likely effects of truncation and to verify that the cutoff was not set at too high of a value, a plot of increasing frequency versus numbers of cutsets was made. Even though this approach to checking seems to be reasonable, there is the possibility that the mechanical check of cutset importance may have overlooked dependencies between the defined failure events (common cause, human errors, etc.). Since these types of dependencies could have an impact on assessed sequence frequency, the methodology should have included such a check.

The PRA followed the general practice of combining independent basic events to form consolidated basic events (modules) to reduce the size of fault trees. It is very important that a basic component of one module is not also contained in another module. The PRA does not explain how this independence of consolidated basic events was assured.

Several computer codes were developed by the PRA team for the quantification process. The PRA discusses neither whether these codes were verified and validated nor the described methodology used for verification and validation. The PRA also fails to describe what steps were taken to ensure that data transfer between computer codes was made without error.

5.1.2 External Events Analysis

Each external events analysis seems to be independent of other aspects of the PRA. The Committee believes that the analysis of external initiators (principally of earthquakes and internal fires) is inadequately integrated with the analysis of internal initiators. The current practice of tying all of these analyses into an expansion of the plant model for internal events ensures consistency and proper handling of correlated and independent failures. Our comments on the existing, individual evaluations are given below.

1. **Internal Fire Analysis.** The Committee believes that the method used for internal fire analysis employs up-to-date approaches, including some methodological enhancements that Sandia has only recently developed, such as an improved approach to analyzing fire brigade manual suppression response times. While the methodology still has some shortcomings, these are generic to all fire PRA analysis and are not specific to this application of the methodology.

2. **Seismic Analysis.** The Committee believes that the method used for this analysis is state of the art in its basic structure. Furthermore, the analysis team is well-known and competent, which provides ipso facto a level of confidence that is comforting to the Committee.

    a. **Seismic Hazard Analysis.** The hazard analysis uses the EPRI methodology and results. As is widely known, two different seismic hazard models are now in the literature, the other being the so-called NRC-Livermore methodology (NUREG/CR-5250). The common opinion in the seismic research community is that it is difficult, in an objective way, to choose either of these over the other. See Section 5.3 for the Committee's recommendation on handling this problem.

    b. **Human Error Rates after an Earthquake.** From the Committee's review, it appears that the human error rates used after large earthquakes are identical to those used in the internal initiators analysis. This could be an erroneous assumption, especially when multiple operator actions are involved, and the Committee believes that this could lead to substantially nonconservative results for core damage frequencies. The Committee understands from the PRA team that the seismic human error rates are being revised for the final draft PRA.

5.2 EVALUATION OF MODELS AND RESULTS

The point estimate results of the SRS PRA appear to be reasonable and to flow logically from the analysis. Moreover, the presentation is clear, placing the results in the context of the event tree sequences. The Committee's confidence in the PRA was greatly enhanced by meeting with the SRS PRA team—an impressive group of individuals with appropriate analytical, engineering, and operations skills. Their knowledge of the reactors and their openness in discussing limitations of the PRA were encouraging. Perhaps most impressive is the effective use of the PRA by WSRC to examine the benefits of potential plant changes; i.e., a risk management program using the PRA is already functioning.

While the PRA is already serving a useful function, we believe that it should be possible to gain further insights into risk and effective risk management by cutting (regrouping) the results of the PRA in different ways. An example is given later in this section. In addition,

we have some concerns about the bases for the PRA model, some of the techniques used in the analysis, and the quality of the documentation. None imply that the PRA is not the best available tool for addressing safety issues at the SRS reactors; rather, they voice a sentiment that the current PRA report cannot stand alone; that the documentation does not make a convincing case that the PRA truly represents the risk. Perhaps, when the uncertainty analysis is complete, it will answer many questions we raise about the analysis.

The Committee's comments are based primarily on review of the PRA report (which included internal events and all external events except earthquakes), a walkdown of L-reactor at the SRS on January 11, 1990, and presentations by the WSRC PRA team on January 12, 1990. The seismic risk results (representing about half of the total core damage frequency) were only available in viewgraphs presented at the January 12 meeting.

1. **Results.** The point estimate core damage frequency was calculated to be 4.5×10^{-4} per year, almost equally divided between internal events (2.1×10^{-4}) and seismic events (2.4×10^{-4}), with other external events contributing a negligible amount. Estimates of the potential reduction in internal and seismic risk to be gained from plant improvements, either already in place or anticipated before startup, are substantial (perhaps a factor of 4).

   The point value results of the PRA appear to be reasonable and are easy to follow. More than 80% of the internal event contribution is assigned to 22 sequences reported in the PRA. More than 99% of the seismic contribution comes from 3 sequences. Thus, more than 92% of the total core damage frequency is fully explained in the documented results of the PRA.

   To gain confidence in the results, we will discuss representative sequences (i.e., essentially all initiators and failures are covered) from the list of 22 dominant sequences presented by the PRA team:

   - ***Sequence 1 — Process Water Bellows Break with MIA System Hardware Failure.*** While the Committee has some concern that the approach used for estimating the initiating event frequency is overly pessimistic, we have little doubt that this is an important sequence. Given the fact that SRS used a expert panel to review the bellows issue, it is likely that the frequency of bellows break used in the PRA is a high end estimate but neither impossibly high nor as low as the median frequency. The uncertainty analysis may alter the importance of this and similar scenarios to some extent.

   - ***Sequence 2 — Large, Unisolable, Sided Cooling Water System Break with Operator (human) Failure To Actuate MIA.*** Again, we are not comfortable with the approach used to quantify the frequency of the LOCA, based on zero failures at SRS. However, the conservatism of that approach, even for low-pressure, ductile, carbon steel piping, may be offset by the effects of aging or maintenance errors such as overtorquing of flange bolts. We are also concerned with the details of the human reliability analysis, as explained elsewhere. Nevertheless, while the sequence may shift in importance when uncertainties are considered, it is likely to remain important.

   - ***Sequence 4 — Transient with Failure of Automatic Scram System.*** This sequence is straightforward. While the scram system model is not presented in the PRA report, it is taken from an earlier analysis that appears to be reasonable.

- ***Sequence 5 — Process Water Plenum Break in Loop with ECS.*** This sequence has not been confirmed by detailed review. However, based on the concern of the PRA team that bellows breaks are significant primarily because of their assumed low leak rate that requires manual actuation of ECS (MIA), the hypothesis of a double-ended guillotine break (DEGB) may be obscuring the real risk from process water pipe breaks. Even if true, however, given the other current contributors, we would not expect a major change in core damage frequency.

- ***Sequence 6 — Process Water Bellows Break With Common Mode Throttling Failure of ECS Valves.*** Although there may be some conservatism in the modeling of common cause failures, little change in the importance of this sequence is expected.

Other sequence groups contribute little to the internal events core damage frequency. Turning to the seismic results, while we have not seen all of the details of the analysis, we are impressed with the quality of the seismic PRA based on what we have seen and on the experience of the consultants retained to assist in that work. Three seismic scenarios dominate the risk:

- ***Sequence 1 — Loss of Process Water and Failure of ECS (19%)***
- ***Sequence 3 — D_2O Seal Head Tank Rupture and Failure of ECS (21%)***
- ***Sequence 26 — Failure of Underground Cooling Water Piping and In-Building Piping (59%)***

While the seismic model looks reasonable in a configuration sense, use of the Livermore hazard curves instead of the EPRI hazard curves could lead to much higher (as much as a factor of 10 higher) core damage frequency. In addition, we are concerned that other seismic sequences that contain multiple seismic-initiated failures could be worse due to correlation. We have not had an opportunity to examine this issue because the seismic PRA section is not yet available.

The contribution of other external events was found to be negligible. We believe that the results of the fire analysis may be optimistic. Given the low value of the calculated scenarios (about 1×10^{-7}), some of the scenarios initially screened out of the analysis may be more important than those analyzed. Nevertheless, the total contribution of fires is probably negligible compared with the current dominant sequences.

2. **Another View of the Results.** As one demonstration of the ways in which the results can be rearranged, we offer the following tabulation:

Scenario Group	Percent of Core Damage Frequency
Seismic Scenarios	50
LOCA and Hardware	20
LOCA and People	20
Transient and Hardware	4
Loss of Pumping Accident and People	2
Loss of Offsite Grid and Onsite AC Power	1
Loss of Offsite Grid and People	1
Loss of River Water and People	1

From this point of view, we see that human error is involved in about 25% of the core damage scenarios; i.e., half of the internal core damage frequency. Also note that 80% of the internal contribution involves LOCAs. The nonseismic LOCA scenarios (40% of the total core damage frequency) break down in the following way:

- **LOCA and Hardware (20%)**
  - 18% Process Water LOCA: Bellows Rupture (6×10^{-3}) and MIA (6×10^{-3})
  - 2% Cooling Water LOCA: Large Pipe Rupture (6×10^{-4}) and MIA (6×10^{-3})
- **LOCA and People (20%)**
  - 10% Process Water LOCA:
    - 6% Bellows Rupture (6×10^{-3}) and Low Stress MIA (4×10^{-3})
    - 4% Bellows Rupture (6×10^{-3}) and Over Throttle (1×10^{-3})
  - 10% Cooling Water LOCA:
    - Large Pipe Rupture (6×10^{-4}) and High Stress MIA (6×10^{-4})

It is interesting to note that, following the LOCA, the subsequent failures are equally split between hardware failures and human errors. From this breakdown, it is possible to see clearly the impact of possible changes such as reducing the estimated frequency of bellows failure, eliminating the need for MIA; i.e., qualifying the moderator recovery system or improving procedures and training.

3. **Concerns.** Several aspects of the PRA model leave us less than comfortable.

   a. ***Integration of Internal and External Events.*** As noted in Section 5.1.2, the Committee believes that the analysis of external initiators (principally of earthquakes and internal fires) is inadequately integrated with the analysis of internal initiators. Without such integration, the two aspects of the study cannot be readily used side by side for decision making since an integrated, overall risk perspective is lacking.

b. ***Human Reliability Analysis***. The approach used for incorporating the results of the HRA into the PRA assumed the independence of multiple human actions. The HRA events, with the exception of throttling and stopping a leak, were embedded into the fault trees. Clearly, this leads to serious underestimation of the frequency of sequence cutsets involving multiple human actions. Because such sequences are usually of low frequency when calculated correctly, the impact on the overall results is uncertain. The PRA team has given some thought to this problem but seems to have performed no sensitivity studies to investigate the true impact.

The modeling of the impact on human performance of procedures, experience, training, and changes to hardware, procedures, and personnel seems to be superficial. From what we have been told, this aspect of HRA modeling will be much improved in the future.

c. ***Data***. The source data for many of the basic events in the PRA are either missing or presented in summary form. It is difficult to evaluate the quality of the data collection and analysis effort. Other sections of this review have expanded on the Committee's concerns (see Sections 5.1.1 and 5.3).

d. ***Uncertainty***. Currently, there is no uncertainty analysis. A well-conceived approach to both modeling uncertainties and data uncertainties is vital to putting the PRA in proper perspective. Many of the issues raised by the Committee can be thoroughly explored by examining and reporting on the full range of possible results and the bases for estimations of the likelihoods of all points in that range. Section 5.3 provides details on the Committee's views on how to enhance the uncertainty analysis of the SRS PRA.

e. ***Other Concerns***. The additional areas of concern listed here are discussed in the following section and elsewhere in our report:

- Success criteria (including LOCA classification schemes) are not well documented.
- The quantification process is not scrutable, especially if:
  - Common elements deep in the fault trees may be inappropriately truncated.
  - Connections and labeling of the component fault trees as they fit into the system fault trees are obscure.
  - The flagging system used to link together fault trees into the simplified event trees is difficult to follow and may be difficult to implement without error.
- Success criteria may differ on a sequence-by-sequence basis.
- Dismissal of shutdown events occurs without sufficient justification.
- Seismic event trees and internal event simplified event trees have good sequence descriptions but fail to discuss the basis for organization and success criteria.

5.3 ANALYSIS ENHANCEMENTS

In this section, various recommendations are made for enhancements to the PRA. While none of these is sufficiently important that the PRA results are considered to be invalid, each suggested enhancement is considered to be a useful addition to the PRA, and one, the uncertainty analysis, is actually a central aspect of the whole effort.

Please note that some of the subjects treated here have also been mentioned in other sections of this report.

1. **Uncertainty Analysis.** The method to be used for the overall uncertainty analysis was described to the Committee, but because it has not been completed, we cannot provide any specific comments about either the method or the results. However, a few key recommendations seem to be in order about this part of the overall analysis:

   a. The uncertainty analysis presumably includes not only the study of numerical uncertainties to the input information, including both data and models, but also the propagation of these through the analysis to produce an overall "uncertainty" in the final numerical results. It is crucial to keep in mind that the uncertainties, analyzed and displayed as distributions, represent a much fuller description of what is known from the overall PRA than any "point estimate" can represent. As such, the careful handling of these distributions is vital to the validity of the work.

   b. In our experience, many of the most important engineering insights gained from the entire effort emerge from the uncertainty analysis. This is because the robustness of various "results" or "insights" differs from one to the next, and the uncertainty analysis is one key way for the analysts, and later, the decision makers, to understand the robustness issues more fully. In this regard, it is not only the numerical aspects of the uncertainty analysis but also the structural aspects that must be done and documented well.

   c. Uncertainty in some issues is best treated by a set of "sensitivity" analyses rather than by a formal numerical uncertainty analysis. (One example is the seismic hazard analysis. We have recommended here that this analysis be done two ways and the results displayed both ways because the experts cannot now differentiate between two different approaches to this issue.) The number of sensitivity analyses that could be done is vast, of course, and resources cannot support all of them, at least not initially. We recommend that careful thought be given, up front, to selecting which key issues and insights require sensitivity analyses, with emphasis on the applications that will be attempted soon. In our experience, decision makers can understand sensitivity analyses easily, which therefore makes them a very useful tool in the decision process. It is helpful to go further, using the sensitivity analyses and expert judgment to establish a probability distribution over the results.

2. **Success Criteria.** The Committee recommends that the success criteria, especially those tied to thermal-hydraulic issues, be revisited to ensure that they correctly represent the reactor. Of special concern is the possibility that there may be some small number of sequences for which the broader success criteria may not apply, whose existence has not been identified in the work to date. While we have identified no such sequences, our experience indicates that a careful review, on a sequence-by-sequence

basis, is necessary to ensure that all of the key sequences have been properly classified in this regard. Section 5.4 offers the Committee's view on how to improve the documentation on success criteria.

3. **Aging of Hardware.** It appears that no formal trend analysis has been performed in determining failure rates. The limited data that we reviewed indicate the possibility of an increasing trend in the number of equipment failures at these old Savannah River plants over time. An increasing trend can be attributed to two major factors: aging and declining quality of maintenance and repair. Especially in light of the age of the reactors, the Committee recommends that a trend analysis be performed for all those classes of components that are susceptible to either of these two factors.

4. **Analysis of the Final PRA Results in Different Ways.** The Committee believes that additional insights can be obtained by analyzing the final PRA results from a number of different perspectives. This is in addition to the perspective presented to us, which emphasizes a list of the "top 20" accident sequences and their significance. For example, pulling out and studying all sequences involving significant control-room errors, or all sequences beginning with bellows ruptures, or all sequences with MIA hardware failures, can provide engineering insights different from those already presented in the report.

   While the Committee is reluctant to propose specific alternative ways to slice up the information, we suggest that the study of several recent PRAs completed at commercial nuclear plants can give some ideas of novel and instructive approaches to analyzing and presenting the results.

5. **Enhancements of the HRA Methodology.** The Committee is very pleased and encouraged by the plans that were described to us for enhancing the human reliability analysis (HRA) aspect of the PRA. The use of simulator data to describe the distribution of times needed by the operating crews to respond successfully to various challenges, as modified with the success likelihood index to correct for expected accident conditions, will be a significant enhancement. These new approaches represent the latest technology and are probably the best way to assess expected human error rates in accident conditions.

6. **Dependency Matrix.** The assembling of complete dependency matrices (to display how each key system/function depends on each support system, and how the support systems depend on each other) would be a major enhancement to the PRA. These matrices form a bridge between the qualitative descriptions of the plant systems and the PRA systems displayed in the fault trees. There are two advantages to this work: first, the building of these matrices requires a thorough and systematic examination of the support system issues, which enhances confidence in the work; and second, these matrices are invaluable tools in subsequent use of the PRA.

7. **Shutdown Events.** Initiating events during shutdown were not included because either the plant shutdown duration is much shorter than the period of operation or, in some cases, they were judged to be subsumed under specific events that can occur at power. The validity of these assumptions involves not only the likelihood of various shutdown initiators but also their progression to a particular potential plant damage state. Since scheduled maintenance during shutdown could put the plant in a vulnerable state, the exploration of these issues is important, even though the low levels of stored energy

and decay heat seem to make these issues much less important than in a commercial power reactor. We believe that a thorough review of these issues would be an enhancement to the overall PRA. Especially important may be a review of operator errors during shutdowns that can lead to loss of control of process water systems inventory through unusual or unexpected value alignments, or dropped loads.

8. **Plant-Specific Data, Especially for Zero-Failure Categories.** The use of Savannah River plant-specific data, wherever applicable, is a major and positive feature of this PRA. However, several important categories of the data contain zero failures within the history of these plants, leading to a dilemma on the part of the analysts on how to treat these categories since, without a model, there is no rigorous way to proceed. The approach selected (using 1/3 failures for 0 in the database) seems to us to be unsatisfactory without also taking into account the additional information from other applicable data, especially from the commercial LWR industry. For example, an approach using a Bayesian updating of the site-specific data (or another similar method) to account for applicable generic LWR data could enhance the database, yet seems not to have been used. The Committee recommends that an approach along these lines be attempted.

9. **Enhanced Dependent Failure Analysis.** In addition to the dependency matrix, other steps could be taken to improve the analysis of dependencies and interactions. The documentation would benefit from a systematic search for dependencies that are unique to the SRS reactors. In particular, more consideration should be given to the identification of more support system failures that could cause an initiating event and also affect the operability of systems needed in response to the initiating event.

10. **Seismic Hazard Analysis.** For the reasons given in Section 5.1.2, the Committee recommends that the PRA take the approach, used in NUREG-1150, of using both the EPRI and LLNL hazard curves separately, and presenting the results two ways. While the numerical results for core damage frequency will differ, these numerical differences are not the only issues: certain engineering insights may be different, too, such as a possible different ranking of the key seismic-initiated sequences. The additional insight available to decision makers using this dual approach could be helpful.

11. **Internal Fire Analysis.** As noted in Section 5.1.2, the fire PRA methodology still has some shortcomings, which are widely known in the community and many of which have been discussed recently in Sandia's "Fire Risk Scoping Study" (NUREG/CR-5088). The Committee suggests that additional analysis could be useful to understand how sensitive the fire analysis insights are to various issues, including how the manual suppression times were determined; sensitivity to the assumptions in the fire propagation analysis that was done with the upgraded COMPBRN code; whether the results are sensitive to ignition threshold assumptions; and whether fires much larger than the 3-foot, 10-gallon fires (the largest analyzed in the PRA) could be of concern even though their likelihood is very small.

5.4 SRS PRA DOCUMENTATION ENHANCEMENTS

The overall organizational structure of the Level 1 PRA report is adequate, but it could be improved through more clear and effective documentation. The current documentation format does not meet the informational needs of different audiences, which will range from top DOE and WSRC management to safety analysts and plant operations personnel. The decision

makers will use the PRA information to obtain reasonable assurance that the operation of SRS is safe. The safety analysts will use the PRA information for a variety of applications throughout the life of the reactors.

The primary objectives for a PRA main report, together with its appendices, are to provide a clear and traceable presentation of the PRA tasks, analytical techniques, important data, and recommendations and conclusions that can be drawn from the results. It should also provide sufficient detail so that a reviewer or PRA analyst can reconstruct at least the important accident sequences. Our comments on the documentation are aimed at providing help to achieve these objectives.

The documentation of the PRA consists of two reports: the report on external events, and the report on internal events. The present external events report does not contain any quantitative results from the seismic analysis. In the main report for the analysis of internal events, the documentation of the human reliability analysis needs to be rewritten with improvements in organization and completeness. The documentation of the analysis of the electric power system, including documentation of the Markov model and the procedures used for validation and verification of the Markov analysis code, is insufficient for even a high-level review and is unacceptable in its present form. Also, the interfaces with the fault tree models need to be documented. The methodology to be used for the uncertainty analysis is addressed in Chapter 3 of the PRA. However, Chapter 12, Uncertainty Analysis, is not included in the PRA since the uncertainty analysis had not yet been done at the time that the PRA was published.

The success criteria are stated in Appendix I of the Level 1 PRA: however, the bases for the success criteria and the underlying assumptions are not provided. For example, the LOCA classification scheme and the condensation process are not described in the PRA. This is a serious shortcoming of the documentation since the reviewers cannot verify the realism and validity of the success criteria. In a similar manner, the major assumptions in Section 1.6 of the PRA and other assumptions throughout the report are stated mostly without their bases or a discussion on their potential impact on the analysis results. The PRA shows a general lack of references to back up material and data sources.

Important and related information is, as in any PRA, contained in many sections and appendices of the report. A lack of cross-references in the report makes it difficult to trace the analyses and to integrate important pieces of information. In particular, the report does not contain sufficient information and cross-references to make the quantification process, including the important process of quality assurance, transparent and traceable. The Committee considers this a serious shortcoming in the documentation.

While the seismic event trees and the simplified event trees are described well, the descriptions fail to provide a discussion of the reasons for the organization of the event tree headings, a comprehensive discussion of the success criteria (including timing considerations) associated with each event tree heading and accident sequence, or a description of the accident sequence phenomenology. The PRA presents four kinds of internal event tree models. However, the progression from one model to the next is not described. A discussion on these event trees and their linkages would enhance the understanding and reviewing of the final event tree models that were used for the quantification.

The description of the fault trees is restricted to the top logic of the trees. It fails to provide specific information on transfers to support systems. We found that the traceability of the system interdependencies through the logic models is very difficult and requires examination of the SETS input files to verify, for example, the dependencies on electrical busses. This is a result of including in the report only the generic component fault trees, without any description, tables, or other means that would allow readers to connect the system interdependencies to specific events in the system fault trees. A comprehensive system dependency matrix would greatly enhance traceability of system interdependencies.

The fault trees include a large number of flags or house events so that the fault trees can be used for a number of accident sequences with different success criteria by only setting flags. The documentation is insufficient to review the correctness of the flag settings in the quantification process; in particular, a discussion of the quality assurance process is missing.

The uncertainty analysis was about to start when the PRA was published. However, the interpretation of the analysis results would have been greatly enhanced by a qualitative discussion of the uncertainties associated with the results. Such a discussion would have helped in the interpretation of the importances and rankings of contributors to core damage frequency.

6. APPLICATION TO RISK MANAGEMENT

The first objective of the SRS PRA may have been to gain an "improved understanding of the potential risk of reactor operation," but the real value and future of the PRA is as a "tool which can be used to assess effects of reactor design and operational changes on plant safety." This second objective of the PRA effort, risk management, is already underway at SRS. We believe that WSRC ought to be commended for the quality and vigor of the current program.

1. **Management Commitment.** The management commitment to PRA and active risk management at SRS is among the strongest we have observed anywhere in the world. The quality, size, and range of experience of the staff involved with PRA and safety issues is exceptional. Because of the competent work that has been accomplished to date, it appears that the benefits of PRA are becoming evident to and accepted by SRS management and operations personnel. PRA is being used in the decision process with key PRA managers sitting on each of two Issues Management Teams that review and approve all plant modifications.

   In the area of management commitment, we applaud the efforts thus far and urge continued support. We believe that it is important to sustain the current PRA risk management team. To that end, we hope that SRS can maintain and extend its interactions with the greater technical community. In that way, it will remain current with the state of the art and help it grow, bringing credit to SRS and DOE.

   The applications-oriented philosophy now in the group is right on target and will ensure that the team returns value far exceeding its cost. Moreover, we believe that a strong PRA risk management program is essential to maintaining a positive interaction with DOE on all levels.

2. **Current Risk Management Results.** The PRA has already affected ongoing activities at SRS, with its results being incorporated into the planning process. One important activity that will lower the risk at SRS, increasing the confidence of the operators in dealing with accidents, is the plan to upgrade the moderator recovery system (MRS) to handle LOCAs up to 1,400 gpm. Upgrading may involve actual hardware changes. Operator training and plant emergency procedures are currently being revised. Personnel who are involved in that effort are aware of the results of the PRA and are bringing its lessons into the process. There are plans for using the PRA in simulator training, maintenance planning, and other areas.

3. **Recommendations for the Future.** We see many areas where the PRA can be applied to plant activities. To enhance its value in the risk management process, we recommend the following activities. These are not viewed as requirements for startup, but as enhancements for the future, and are listed in order of priority.

   a. Enhance the Level 1 PRA with qualitative discussion of all uncertainties, and add qualitative or semiquantitative Levels 2 and 3 analysis (i.e., assign sequences to reasonable consequence categories) to aid in decision making now, before the final Level 2 and uncertainty analyses are completed.

b. Recast the PRA model for rapid recalculation to understand its sensitivity to changes in data and logic.

c. Update the PRA to reflect the restart configuration.

d. Maintain the PRA on a continuing basis.

e. Institute a program to confirm that the "as analyzed" plant and PRA modeling assumptions (including aging) continue to remain valid.

f. Plan for things not modeled in the PRA; e.g., failure of controls, instruments, instrument air, etc. While a long-term goal might be to incorporate explicitly such aspects into the model, much can be gained by brainstorming the potential impact of such occurrences. The results of such activities could be to set priorities among a list of concerns, to develop procedures and diagnostic aids to help operators during troublesome scenarios.

7. FINDINGS AND CONCLUSIONS

7.1 OVERALL CONCLUSION REGARDING RESTART

The Committee does not see any safety issues resulting from the PRA that would be cause for delaying restart of the K-reactor at the Savannah River Site. Moreover, the Committee has not observed any ongoing restart activity that would degrade the risk assessment that has been performed, although our review has not been extensive in this regard.

7.2 MOST IMPORTANT ACTIONS FOR SUSTAINING SAFETY

The Committee is satisfied that the risk of a major accident at the Savannah River Site from operation of the K-reactor is extremely small and in the same low frequency range as the highly regulated commercial nuclear power plants. Nevertheless, an important question to ask is, However remote the possibility of a core damage accident, if one were to occur, what is the Committee's opinion of its most likely cause?

On the basis of our review of the PRA and our understanding of the intended configuration of the plant for restart, it is our judgment that the chance of a core damage accident is extremely remote. However, if one should occur, we believe that the most likely cause of an accident would involve a hardware failure initiating event, followed by some combination of mistakes or deficiencies involving personnel, procedures, and training. It is this opinion that leads us to believe that the most important actions to sustain safety at the Savannah River reactors are the following:

- Assurance that the personnel training program is comprehensive, up-to-date, and focused on the safety issues that have been identified by the PRA. Care should be taken not to relax existing training and preparations for accident sequences not highlighted by the PRA results because of the credit taken for staff preparedness.
- Continuation of the upgrading of the procedures, especially in the area of emergency response.
- Continuation of the plan to manage the contribution to risk from seismic events.
- Recognition that the scope of the PRA, as with all PRAs, is not 100% complete for scenario detail; thus, specific planning is advisable for events that are not accounted for in the PRA. Examples of such events may be those deriving from the plant instrumentation system and its support systems, such as the instrument air system.
- Implementation of an inspection and surveillance program on critical hardware identified by the PRA to ensure control of any possible performance degradation that may occur from such phenomenon as aging. Hardware of particular interest include the process and cooling water piping; specific piping components such as bellows, other joints, and flanges; and the process and cooling water pumps and valves.
- Confirmation of the "as analyzed" plant and the validity of the PRA modeling assumptions. Clearly, it is essential that the model be truly representative of the plant.

- Qualification of the moderator recovery system (MRS). Because of the impact that the MRS can have on core damage frequency without requiring emergency cooling, it is crucial to understand its reliability so as to have confidence in it as a safety system.

- Adoption of an attitude of always viewing the results from a critical perspective. Be aware of the underlying assumptions, simplifications, and limitations of the models, and be prepared to let go of them as improvements arise. Continually challenge those aspects of the models that are not well supported. Allow the results to change as new evidence is introduced.

7.3 SPECIFIC FINDINGS THAT IMPRESSED THE COMMITTEE

1. Perhaps the most outstanding feature of the SRS risk assessment is the risk analysis team that has been assembled to do risk analysis and to maintain the models. It appears to be highly qualified, enthusiastic about its mission, and very dedicated. Two additional qualities stand out: size of the team and the mix of expertise. This appears to be one of the few instances of adequate staffing to implement meaningful, real time quantitative risk management. The mix of expertise is very encouraging in that appropriate analytical, engineering, and operations skills appear to be on the team. Often risk teams are lacking crucial expertise and knowledge about plant operations, an essential part of the knowledge base to perform meaningful risk management. This team definitely thinks PRA in its daily activities; i.e., when looking at the plant, it puts equipment design and performance as well as procedures and operator aids in the context of the PRA. Its focus is definitely on risk management, not simply on compliance.

2. In general, it appears that careful thought has gone into development of the models and restructuring them to facilitate quantification. The PRA team has studied existing engineering analyses of the plant, developed some new analyses to support the PRA, and consulted with both in-house and outside experts in areas where plant capability has not been clear. The risk analysis team has shown a certain amount of boldness in the use of innovative approaches. Examples are the use of dendograms to identify initiators and the Markov modeling of electric-power systems. Their use of well-proven methods and highly qualified consultants for the earthquake and fire analyses is another demonstration of their willingness to reach out for help.

3. The PRA has had sufficient time (more than 3 years) to shake out their team and to get familiar with the various methodologies in the PRA field. The analysts themselves, by now, have an excellent understanding of their plant, and that shows. The risk team has been subject to various reviews and review groups, has worked well with subcontractors, and benefits from excellent top-level support from its management, both in the early stages with DuPont and later with Westinghouse. The team has come through all of this with a very positive viewpoint and a willingness to accept advice and criticism in the future.

7.4 SPECIFIC FINDINGS THAT SUGGEST OPPORTUNITIES FOR IMPROVING THE SRS PRA

1. The documentation in the current draft of the PRA is inadequate. The basis for the success criteria is not given. Uncertainty in the end state of each sequence is hinted, not explained. While there is no documentation in the PRA to convince the reader (or future users) that the event tree model is a realistic representation of K-reactor response to upset, meetings with the SRS PRA team provided us with a great deal of confidence. It appears that, for the most part, success criteria are extracted from information contained in plant procedures (DPSOLs), tempered by judgment of the PRA team based on experience with the plant, review of existing SRS engineering/ physics analysis, and some recent analysis done in support of the PRA. Some backup calculations are documented in SRS calculation notes. More documentation should be provided in the PRA, including descriptions and discussions of analytical methods used to derive success criteria.

2. There is some concern that the PRA results in their present form put too much emphasis on the importance ranking of specific events. In other words, there is great temptation to have too much confidence in very narrow aspects of the results. An example is the importance of a bellows break in the process water system, a large pipe break in the cooling water system, and failure of the emergency cooling system. These separate events on the surface appear to dominate the risk, and thus there is great temptation to concentrate on corrective actions involving them. We believe that a different cut of the results might suggest a different strategy. Such a cut may suggest that the emphasis be on operator training, or reanalysis of specific events, or the upgrading of specific procedures. The point is that we have to be extremely careful not to "overbelieve" the results from a PRA and to be confident that they are in proper perspective for such factors as human performance and operating procedures.

3. An issue of great importance to any PRA is the uncertainty in the results. This importance is magnified when using the PRA as part of a risk management program. In particular, if corrective actions are going to be developed for the purpose of reducing or controlling risk, the choice of actions can be dramatically impacted by the level of uncertainty associated with both the contributor to risk in question and the proposed fix. It is not uncommon for the uncertainty analysis to completely alter the strategy for taking corrective actions. While uncertainty analysis is on the agenda for the SRS PRA (and expected to be included in the next revision of the PRA), it is not necessary to wait for that analysis to obtain some insight into the effect of uncertainty on the existing results. In particular, it would enhance the value of the current PRA results if they were discussed in a manner that shared the current state of knowledge about the confidence that the risk analysis team has in its specific findings. This additional insight would greatly facilitate the use of the results by the decision makers by providing them with the most informed knowledge base possible at this point in time.

4. The PRA model, partly out of necessity, is very complex in our being able to comprehend it in a risk management sense and to unravel the results. At some point, the utility of the PRA would be greatly enhanced if a superset of the detailed model was recast for the explicit purpose of management applications; that is, there needs to be a risk manager version of the PRA. The approach that has worked well in the past in this regard is to develop an "important sequence model." The resulting sequences, or

scenarios, are structured to represent essentially the whole model but at a coarser level, to facilitate easier manipulation of the model for developing quick insights on the effect of candidate fixes. The "risk manager" should involve real plant language as much as possible and be strongly tied to plant activities. Of course, it should be user-friendly and very scrutable to a broad range of professionals who are associated with operating and managing the plant. The PRA in its present form is very limited in this regard.

5. The Committee was not completely comfortable about the treatment of dependencies, even though some aspects of this subject were treated very well. Most of the problem is believed to be related to documentation, as covered in item 1. However, the treatment of dependencies is enough of a technical issue to be discussed separately. In particular, the usability and scrutability of the SRS PRA would be greatly enhanced if a dependency matrix, or other equivalent tool, were developed to document the intersystem dependencies at the K-reactor. The dependency matrix would form a bridge between the qualitative descriptions of the plant systems and the PRA systems displayed in the fault trees. The usability of the SRS PRA would also be improved if support systems were specifically indicated on the system and component fault trees. Currently, support systems are only shown generically (e.g., electric power rather than specifically; e.g., 480V MCC 14).

6. In the data area, the Committee saw some opportunities for increasing the defensibility of the SRS PRA. In addition to the uncertainty issue discussed above, the biggest deficiency of the data-handling activity was not adopting the current state-of-the-art Bayesian method of handling data. This was particularly true for the method of handling the probability of events that are not observed in the plant-specific database. The Bayesian methods for doing this are straightforward, widely used, tested in the hearing room, and very scrutable. The Bayesian methods are particularly helpful to determine trends, including the effect of aging. The absence of a comprehensive data analysis is more of an opportunity missed than a serious flaw in data handling. The availability of an extensive plant-specific database reduces the impact of generic data, and thus the absence of a full database treatment is not as serious as it might be otherwise. Still, there is the matter of defensibility and the state of the art. A specific criticism is the treatment of zero failures. The approach selected (using 1/3 failures for zero failures observed in the database) seems to the Committee to be unsatisfactory. For such failures, it is especially important to reach for other sources of data, such as the commercial reactor field, to establish a logical and defensible choice of failure rates.

7. The Committee has three comments on the matter of fires and earthquakes. The evidence is strong that fires are not an important risk issue at the Savannah River reactors but not so strong as to support the very low numbers presented in the PRA. This may be only a matter of documentation, but the Committee is not completely clear on the detailed scenarios that formed the basis for the very low contribution to core damage from internal fires. The Committee suggests (see Section 5.3) that additional information would be helpful on the technical basis of the fire analysis.

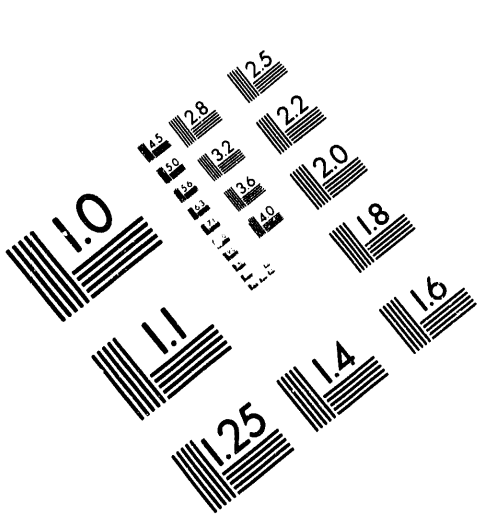
   In the seismic area, it is well-known that there are two different seismic hazard methodologies in the recent literature: the EPRI methodology, which was used in the SRS PRA, and the so-called NRC-Livermore methodology, NUREG/CR-5250. The common opinion in the seismic community is that it is difficult, in an objective way, to choose either of these over the other at this time. Therefore, the Committee recommends that the PRA take the approach, used in NUREG-1150, of using both the

EPRI and LLNL hazard curves separately and presenting the results two ways. While the numerical results for core damage frequency will differ, these numerical differences are not the only issues: certain engineering insights may be different, too, such as a possible different ranking of the key seismic-initiated sequences. The additional insight available to decision makers using this dual approach could be helpful.

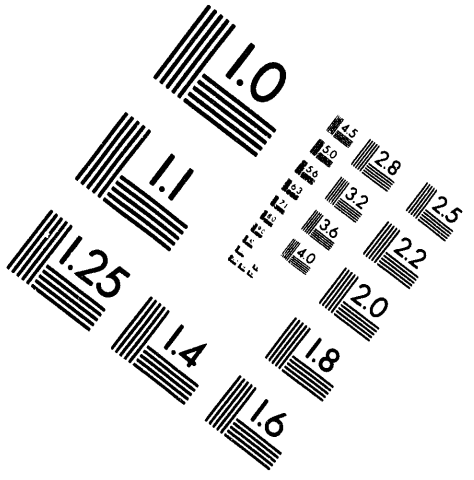
Finally, as pointed out in Sections 5.1.2 and 5.2, the Committee believes that the analysis of fires and earthquakes are inadequately integrated with the rest of the risk model.

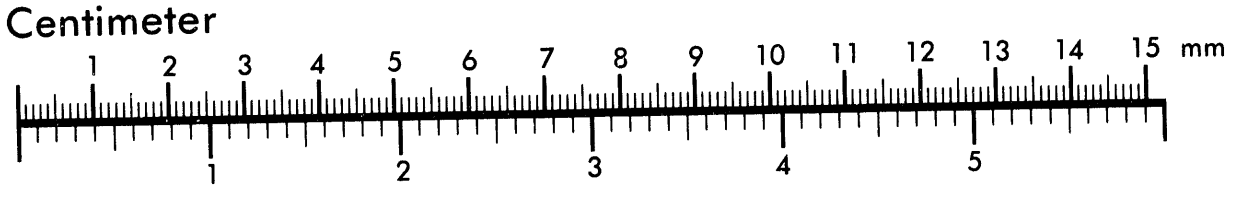
8. The Committee has some concern about the completeness of the initiating event set. The concern centers around the fact that the development of the initiating event set did not follow strict rules to maintain hierarchical relationships between events and conditions. Discussions with the PRA team provided considerable reassurance that there are no serious omissions and that, again, the problem may be more a matter of documentation than anything else. The absence of a dependency matrix made it difficult to verify that initiating events that originate in plant support systems were, in fact, identified. It was also not possible to verify that initiating events that are expected to occur during shutdown were systematically identified. An area of particular interest to the Committee relates to the possibility of a crane accident during shutdown that can lead to a dropped load on critical equipment or systems.

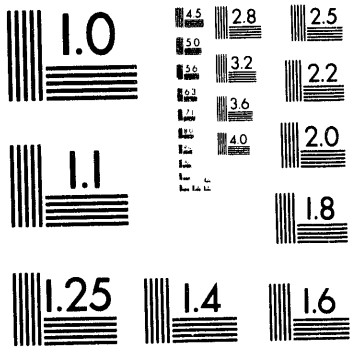
9. In the area of human reliability assessment, the techniques appear to be less than state of the art, particularly since human actions are an integral and important contributor to the safe operation of the Savannah River reactors. The Committee during its visit to Savannah River was very pleased and encouraged by the plans to enhance the human reliability analysis in the PRA. The analysis as it now stands in the PRA is based principally on THERP, which is, to a large extent, an outdated methodology. It was very encouraging to learn that the simulator will be used to obtain data to describe the distribution of times needed by the operating crews to respond successfully to various challenges, as modified with the success likelihood index to correct for expected accident conditions. It is important that these enhancements be performed to have confidence in the overall human reliability assessment in the PRA.

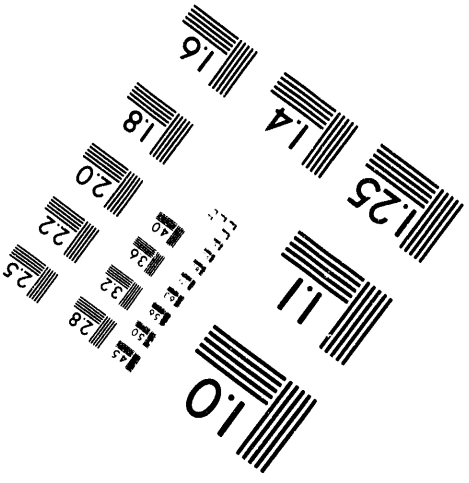


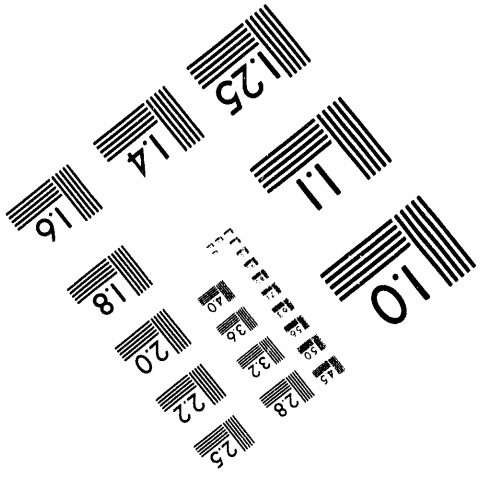
Association for Information and Image Management
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202











DATE
FILMED
12/13/94
END