Westinghouse Independent Safety Review of Savannah River Production Reactors

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Westinghouse Independent Safety Review of Savannah River Production Reactors

This document is

PUBLICLY RELEASABLE

John Wingard (SR)

Authorizing Official

Date 11/21/83

by Donald Williamson 11/29/83

W. H. Arnold - Chairman

W. D. Leggett

W. J. McShane

Westinghouse Hanford Company

WSRC-RP--89-84

DE90 004782

N. J. Liparulo

J. D. McAdoo

L. E. Strawbridge

Westinghouse - Nuclear and Advanced Technology Division

G. Toto

Westinghouse - Nuclear Services Division

H. K. Fauske

Westinghouse Subsidiary - Fauske and Associates, Inc.

D. W. Call

D. C. Richardson - Secretary

Westinghouse Savannah River Company

April 1, 1989

Second Printing

Prepared for the U.S. Department of Energy
under Contract No. DE-AC09-88SR18035

Westinghouse

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

ps

[illegible]

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Acknowledgments

Many people have contributed to the efforts reported here, in addition to the committee and subcommittee members specifically named in the appendices. Most notable was Mr. Tom Gorrell, of E. I. du Pont de Nemours & Company (Du Pont), who with tireless good humor was able to arrange for many very busy Du Pont people to meet with and brief yet another review committee. In addition, he proved a valuable resource in his own right, as a reservoir of past and present information not otherwise readily available. Among the many Du Pont people who found space for us in the midst of incredible demands on their time and patience were the following: Bob Allen, Harvey Allen, Bill Anderson, Bob Anderson, Courtney Apperson, Keith Atkinson, Bill Awadalla, Ersin Bacinoglu, Hubert Baker, Dennis Baker, Rick Benton, Fred Beranek, Pete Boiter, Tom Britt, Mel Buckner, David Burke, John Champy, Larry Chandler, Kuo-Fu Chen, Andy Christensen, John Church, Brad Clark, Doug Cramer, Jim Crichton, Bill Croft, Sid Curry, Larry DeWitt, Mark Du Pont, James Edwards, Wayne Ehrhart, Jeff Falin, Darryl Ferguson, Bob Finley, Sam Formby, Geof Fountain, Dave Freeman, Tom French, Al Garrett, Lee Gaston, Mic Giess, Bill Graves, Hector Guerrero, Eddie Hair, Jim Hammett, Jerry Hansen, Jerry Hardin, Bill Hearn, James Hendrix, Meg Hilker, Jim Hinton, Bill Horton, Susan Hoxie-Key, Rubin Hutto, Dave Jacobs, Larry Jones, Darrel Ketcham, Andrea Kilpinski, Nick Kuehn, Gordon Leopard, Ivan Lewis, John Little, Mac Louthan, Ed Majzlik, Bill Massey, Charlie Mastromonico, Al Mink, Tom Monahan, Robert Moore, Jerry Morin, Jim Morrison, Dave Muhlbaier, Dick Murphy, Charles Nash, Ron Newman, Shelton O'Berry, Kevin O'Kula, Bob Olson, Bob Ondrejcin, Ralph Painter, Stew Petersen, Steve Pye, Brent Rankin, George Rawls, Bill Reed, David Rennie, Scott Revolinski, Geoff Reynolds, Fred Rhode, Steve Rich, George Richardson, Johnny Robertson, Marvin Ross, Bill Rubio, Joe Sabino, Rich Salizzoni, Rod Satterfield, Carl Schaumann, Tony Sealy, Bonnie Shapiro, Dave Sharp, Bob Sindelar, Jim Smith, Henry Smith, James Smith, Ron Sprayberry, Jim Stone, Kevin Stoner, Rob Swingle, Bob Taylor, Steve Topp, Al Tudor, Greg Vaughn, Phil Vormelker, Vascoe Watley, Andy White, Anatia Whittenburg, Elwyn Wingo, Dan Wood, Joe Yanek, Winston Yau, and Gary Youell. Boeing Computer Services Richland, Inc., has performed yeoman service in assisting with the publication of this report, particularly Nancy Bergman, Leslie Brown, Loraine Campbell, Shirley Garrison, Stephanie Janicek, Madhuri Pandey, Brenda Sartoris, Kristi Valdez, and Patricia Wildfang. At Westinghouse Hanford Company, George Congdon, Laura Bareither, Aleda Brogdon, and Karen LaRock have also proven invaluable to the success of the publication effort.

Abstract

Westinghouse Electric Corporation has performed a safety assessment of the Savannah River production reactors (K, L, and P) as requested by the U.S. Department of Energy. This assessment was performed between November 1, 1988, and April 1, 1989, under the transition contract for the Westinghouse Savannah River Company's preparations to succeed E. I. du Pont de Nemours & Company as the U.S. Department of Energy contractor for the Savannah River Project. The reviewers were drawn from several Westinghouse nuclear energy organizations, embody a combination of commercial and government reactor experience, and have backgrounds covering the range of technologies relevant to assessing nuclear safety.

The report presents the rationale from which the overall judgment was drawn and the basis for the committee's opinion on the phased restart strategy proposed by E. I. du Pont de Nemours & Company, Westinghouse, and the U.S. Department of Energy-Savannah River. The committee concluded that it could recommend restart of one reactor at partial power upon completion of a list of recommended upgrades both to systems and their supporting analyses and after demonstration that the organization had assimilated the massive changes it will have undergone. These recommendations are supplemental to the restart criteria formulated by the U.S. Department of Energy in November 1988 at a meeting in Charlotte, North Carolina. The committee recommendations are presented either as required before restart of the first reactor or as long term. The long-term recommendations are to be incorporated by the contractor into an aggressive reactor safety improvement program, the creation of which is itself a committee recommendation.

Executive Summary

Westinghouse Electric Corporation (Westinghouse) has performed a safety assessment of the Savannah River production reactors (K, L, and P) as requested by the U.S. Department of Energy (DOE)-Savannah River Operations. This review concentrated on the K Reactor as the candidate for near-term restart and on the Mark 22 fuel assembly (Mk22) charge used in tritium production. It was performed between November 1, 1988, and April 1, 1989, under the transition contract for the Westinghouse Savannah River Company preparations to succeed E. I. du Pont de Nemours & Company (Du Pont). The reviewers were drawn from several Westinghouse nuclear energy organizations, embody a combination of commercial and government reactor experience, and have backgrounds covering the range of relevant technologies. These include engineering design, safety analysis, severe-accident and risk evaluation, and conduct of operations. The activity itself was performed separately from preparation for operations management and thus is titled the Westinghouse Independent Safety Review (WISR). The WISR committee of nine members and a secretary was supported by one senior staff member from Du Pont and by nine topical area subgroups of two to five people each. Information was obtained from reports and files, Du Pont and subcontractor presentations and interviews, and plant visits. Where necessary, available information was supplemented by original analysis.

The committee adopted a rationale for judgment, expressed as a set of criteria. These were adapted from a draft prepared by Westinghouse Savannah River nuclear safety oversight management personnel as a part of their transition activities, so that the principles articulated are expected to carry over into the new operation. Although derived directly from commercial reactor experience, they do not impose verbatim compliance with the latest U.S. Nuclear Regulatory Commission (NRC) regulations and guidance. Such compliance would be impossible both because of the differences in technology (low-temperature heavy water versus high-temperature light water) and because of the early 1950s vintage of the design. The committee also considered how the NRC adapts its regulations to older licensed units.

The criteria used by the WISR committee in reaching its upgrade recommendations flow from four guiding principles. First is the necessity to understand the level of risk posed to the general public and plant workers and to ensure that the most likely occurrences pose little or no risk, while those with the greatest adverse consequences are least likely to occur. Second is an understanding that reactor safety is not a static art, but involves a continuing self-examination and search for excellence, evidenced in the management and workplace culture and in the maintenance and upgrades to the hardware. Third is an understanding that deterministic predictions of all conceivable adverse events are not feasible, so that the best strategy is one of defense in depth to provide tolerance against the

unpredicted. Fourth is a recognition of the interdependence among design, conduct of operations, and management, and an understanding that a strong management system must ensure an appropriate level of attention to each of these factors.

The committee judgments attempt to ensure that the risk to public health and safety from operation of the plants will be a small fraction of that from accidental occurrences in toto and that the risk to plant personnel will not exceed levels typical of industrial activities. This assurance in turn rests on the following requirements:

1. That the reactor be capable of being shut down and maintained in a safe condition (including long-term cooling and monitoring) following normal operation and all anticipated operational occurrences
2. That mitigation systems be available to limit core damage and fission product release for design-basis and more severe events. Emergency cooling is provided for design-basis leaks, and the confinement system is to provide an effective barrier to the release of fission products from design-basis accidents
3. That postaccident monitoring and accident management capabilities be available. Emergency planning must be in place to deal with the residual risk posed by beyond-design-basis events
4. That effective management systems be in place to provide confidence that the equipment and personnel are ready for safe operation. A plan for, and commitment to, continuing safety improvements must be the first priority of management.

The restart strategy proposed by Du Pont, Westinghouse, and DOE Savannah River to the U.S. Department of Energy-Headquarters (DOE-HQ) on January 13, 1989, and to DOE's Advisory Committee on Nuclear Facility Safety on January 25, involves completion of a short-term list of hardware and training items on one reactor and its operation at less than full power until completion of a long-term list of upgrades on all three units. The committee is in general concurrence with such an approach, and its comments on the required content of both the short-term and long-term lists are contained in this report. A commitment is anticipated in the near term to the committee's long-term recommendations, with the expectation that these recommendations will be pursued aggressively as part of an overall reactor safety improvement program, and implemented before a substantial portion of the remaining operational lifetime of the reactors has elapsed.

The committee's recommendations are to be understood as supplemental to the program already in place to meet the November 1988 DOE criteria (DOE 1988). A prerequisite to any restart is completion of the transition to the new management, the assimilation of the massive changes under way with particular emphasis on the training and performance of the operations staff, and an assurance that the excellent safety record to date is not jeopardized by the transition. Similarly, a precondition to full resumption of operations is that the

new organization evidence its commitment to a rising standard of excellence in nuclear safety.

Setting the allowable power level before completion of the experimental program now under way has been an area of considerable contention, centering on the ability of the emergency cooling system (ECS) to cool the core following a postulated break in the coolant boundary. A strong body of evidence supports the belief that breaks approaching the double-ended guillotine rupture of the process water pipe are beyond reasonable expectation and should not be considered as a design basis for mitigation. A prudent design basis would be the largest break that cannot be subject to full characterization and inspection, namely an expansion bellows failure, the largest of which might result in a 55-in² opening. Pending acceptance of the leak-before-break (LBB) technology to define this design basis, the committee considers it prudent to establish a power level such that core coolability would be expected, using realistic modeling, even for the hypothetical sudden double-ended guillotine break (DEGB). The committee has not attempted to determine the resulting allowable power level, but is optimistic that a practical figure on the order of 50% can be defended. Resumption of full-power operations will require further analytical and experimental data and an understanding of the risks involved through completion of on-going probabilistic risk assessments (PRA). The case is made tenable by the low system temperature and pressure, leading to low energy available to expand an opening, and the confidence in early leak detection because of the low threshold for detection of tritium contained in the heavy-water coolant.

Other areas have received special attention as well, such as survival of seismic events, protection against fires that threaten safety systems, prevention of loss of pumping from flooding, safeguards against system overpressurization caused by inadvertent actuation of emergency cooling, provisions for emergency power, provision of essential instrumentation for use during unusual occurrences, capability of the confinement system to alleviate the consequences of a severe accident, the adequacy and integrity of the information base for design, safety analysis and conduct of operations, the reflection of this information base in training and procedures, and the assimilation of all these data by the operations staff.

The report discusses the committee's investigations of these and other topical areas, organized around the nine subcommittee reports (Appendix B) and their recommendations (Section III). Suggested requirements are presented for provisional operation of K Reactor at a partial power level and for the subsequent reactor safety improvement program. In all, 50 specific recommendations are made, of which 24 are to be accomplished prior to restart of the K Reactor.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

ACRONYMS AND ABBREVIATIONS

AA3	computer code
AACS	airborne activity confinement system
AC	alternating current
A/E	architect/engineer
AEC	U.S. Atomic Energy Commission
AIA	automatic incident actuation
AIAS	automatic incident actuation system
ALARA	as low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
APOLLO	computer code
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ATWS	anticipated transients without scram
BOR	burnout risk
BR-3	(experimental power reactor in Belgium)
BWR	boiling-water reactor
CANDU	Canadian deuterium-uranium (reactor program)
CCTV	closed-circuit television
CFR	Code of Federal Regulations
CHRS	confinement heat removal system
COBRA-NC	computer code
CPL	confinement protection limit
CRBRP	Clinch River Breeder Reactor Plant or Project
CRT	cathode ray tube
CVTR	Carolinas-Virginia tube reactor
CWRSS	contaminated water removal and storage system
CWS	cooling water system
DBE	design-basis earthquake
DC	direct current
DEGB	double-ended guillotine break
DG	diesel generator
DMA	diagnosis of multiple alarms
DOE	U.S. Department of Energy
DOE-HQ	U.S. Department of Energy-Headquarters
DOE-SR	U.S. Department of Energy-Savannah River Operations Office
Du Pont	E.I. du Pont de Nemours & Company
ECS	emergency cooling system

EPA	U.S. Environmental Protection Agency
EPRI	Electric Power Research Institute
EPS	emergency power system
ERDA	U.S. Energy Research and Development Administration
ESBU	Energy Systems Business Unit
ES&H	Environmental, Safety and Health
FFTF	Fast Flux Test Facility
FI	flow instability
FLOOD84	computer code
FLOWTRAN	computer code
FSAR	final safety analysis report
GCR	gas-cooled reactor
GDC	general design criteria
GIP	generic implementation procedure
GM	General Motors
HFIR	high-flux isotope reactor
HWR	heavy-water reactor
IDCOR	Industry Degraded Core Rulemaking (program)
IEEE	Institute of Electrical and Electronics Engineers
IGSCC	intergranular stress corrosion cracking
Ink	concentrated gadolinium nitrate solution
INPO	Institute of Nuclear Power Operations
ISI	in-service inspection
LBB	leak before break
LMR	liquid-metal reactor
LOCA	loss-of-cooling accident
LOPA	loss-of-pumping accident
LWR	light-water reactor
MAACS	computer code
MCNP	computer code
MIA	magazine index assembler
Mk18	Mark 18 fuel assembly
Mk22	Mark 22 fuel assembly
MPF	maximum probable fire
MRS	moderator recovery system
NAS	National Academy of Sciences
NASA	National Aeronautics and Space Administration
NDE	nondestructive examination
NDTT	nil-ductility transition temperature
NERVA	nuclear engine for rocket vehicle applications

NQA-1	Quality Assurance Program Requirements for Nuclear Facilities (ANSI/ASME 1986)
NRC	U.S. Nuclear Regulatory Commission
NUS	NUS Corporation
OSHA	Occupational Safety and Health Administration
OSV	onset of significant voiding
P&ID	pipng and instrumentation diagram
PLC	Professional Loss Control (company)
PRA	probabilistic risk assessment
PSAR	preliminary safety analysis report
PSS	primary shutdown system
PWR	pressurized water reactor
PWS	process water system
QA	quality assurance
RCS	reactor coolant system
RELAP	computer code
REMACS	remote emergency monitoring and control system
RIA	reactivity insertion accident
RRS	reactor room spray
RRSS	reactor room spray system
RSS	reactor shutdown system
RT	Reactor Technology
RTD	Reactor Technology Department
RV	reactor vessel
SAR	safety analysis report
Saxton	experimental power reactor in Saxton, Pennsylvania
Selni	(commercial power reactor in Italy)
Sena	(commercial power reactor in France)
SPERT	(experimental reactor test in Idaho)
SQUG	Seismic Qualification Utility Group
SRL	Savannah River Laboratory
SRP	Savannah River Plant
SSS (Ink)	supplementary shutdown system

TPL	transient protection limit
TRAC	computer code
UPS	uninterruptible power supply
UT	ultrasonic testing
V	volt
Westinghouse	Westinghouse Electric Corporation
WISR	Westinghouse Independent Safety Review
WRSS	water removal and storage system
WSRC	Westinghouse Savannah River Company
Yankee Rowe	(commercial power reactor in Massachusetts)

TRADEMARKS

Bingham is a trademark of Guy S. Atkinson Company, doing business as Bingham Willamette Company.

Caterpillar is a trademark of Caterpillar Incorporated.

GM is a trademark of General Motors Corporation.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

Contents

Executive Summary	v
Acronyms and Abbreviations	ix
Trademarks	xv
Introduction	1
I. Safety Philosophy and Restart Criteria	7
Preface	7
Perspective of Risk	7
Self-Examination	8
Defense in Depth	9
Interrelations among Design, Operations, and Management . . .	9
Safety Acceptance Criteria	11
II. Application of Criteria to Savannah River Production Reactors .	15
III. Recommended Action Items	39
Appendices	
A. Westinghouse Independent Safety Review Committee Charter and Meetings	A-1
B. Subcommittee Reports	B-1
B.1. Mechanical Systems	B-2
B.2. Structures, Seismic, and Materials	B-13
B.3. Electrical, Instrumentation, and Control	B-31
B.4. Fire Protection	B-51
B.5. Core Design	B-57
B.6. Conduct Of Operations	B-71
B.7. Probabilistic Risk Assessment and Severe Accidents .	B-93
B.8. Safety Analysis Review	B-113
B.9. Power Limit and Accident Propagation	B-125
C. References	C-1

Figure

1. Fundamental Areas of Safety Influence	10
--	----

Tables

1. Safety Differences Between Savannah River Plant and Light-Water Reactors	4
2. Westinghouse Independent Safety Review Listing of Committee and Subcommittee Members	16
3. Westinghouse Independent Safety Review Summary Listing of Recommendations	39

Introduction

The three production reactors at the Savannah River Plant (originally there were five, but only K, L, and P are now candidates for restart) were designed and built by E. I. du Pont de Nemours & Company (Du Pont) in the early 1950s, upon direct request of President Harry S. Truman. Although many of the Du Pont personnel were experienced in the design and construction of the light-water-cooled, graphite-moderated reactors at the Hanford Site during the Manhattan Project, an entirely different technical concept was chosen for the Savannah River Project (SRP), optimized for the production of tritium and plutonium. The use of heavy water as moderator and coolant was not followed in commercial practice by the U.S. nuclear industry, despite the construction of a 50-MW component test reactor at SRP followed by a small-scale U.S. Atomic Energy Commission (AEC) commercial demonstration plant in the early 1960s.* The Canadian nuclear industry has implemented this combination of coolant and moderator into the current Canadian deuterium-uranium reactor program (CANDU), of which numerous examples are in successful operation in Canada, South Korea, India, Pakistan, and Argentina. The German reactor vendor Siemens, through its Kraftwerk Union subsidiary, also has built a power reactor of this general type in Argentina.

Nevertheless, the U.S. civilian reactor industry developed on different lines. The 106 currently licensed light-water reactors (LWR) generally owe their technology to the U.S. naval reactors program, via its pressurized-water (cooled) reactor (PWR) demonstration plant at Shippingport (started up in 1957). Another factor important to this choice was the availability to electric utilities of partially enriched uranium under the 1954 Atoms for Peace program; an especially attractive feature of the heavy-water reactor (HWR) in its power production version is its ability to use natural uranium so that its advantage over the LWRs, which require enriched uranium, was diminished in the United States. The predominant thrust in the development of designs, materials, analysis techniques, codes and standards, licensing practice, construction methods, and conduct of operations not only was thus outside the AEC/U.S. Energy Research and Development Administration (ERDA)/U.S. Department of Energy (DOE) organization but was also building upon a different technological base. A similar phenomenon took place internationally, although not to such an extreme degree. The current

*The Carolinas-Virginia tube reactor (CVTR) was built by Westinghouse for a group of southeast U.S. utilities and operated successfully for five years at a nominal power of 11 MW.

world count of power reactors is 329 LWRs, 28 HWRs, 46 gas-cooled reactors (GCRs), and 26 other.

This relative isolation of the HWRs at SRP did not preclude a record of safe operation. The overall history compares well with that of the civilian reactor industry in both safety and operational efficiency. The Du Pont management's attention to employee safety is reflected at SRP, and the reactors were well designed to the prevailing codes and standards. Taking advantage of the absence of equipment necessary to produce electric power and the lower temperatures and pressures thus made possible, the product of these designs is in a number of ways more forgiving than that of a standard LWR. Table 1 is a summary of some major points of difference, with emphasis on those important to nuclear safety.

A possibly more profound aspect of the isolation of the DOE reactors at SRP from the body of licensed reactor practice is in the area of conduct of operations. The Three Mile Island accident in 1979 was a major watershed for the civilian nuclear industry. In addition to a number of specific hardware upgrades, it has led to a pronounced change in the management of operations. Most particularly, it led to a growing understanding that hardware alone could not be relied upon for nuclear safety. A new discipline of operations and a rising standard of excellence, largely based on those already in place in the U.S. naval nuclear program, have been put into place in the ensuing 10 years. The U.S. Nuclear Regulatory Commission (NRC) puts great emphasis on operations management in its reviews of operating plants. The industry's own Institute of Nuclear Power Operations (INPO) provides peer review of operating plants, with no-holds-barred critiques, and shares good practices among units.

The nuclear accident at Chernobyl led to another searching look at current practices, but the U.S. civilian plants came out rather well by comparison with Soviet practice. This time the spotlight was turned to DOE reactors, particularly the N Reactor at the Hanford Site, which, like Chernobyl, has a graphite moderator. The N Reactor was shut down for a major safety upgrade and review. [Although subsequently reviewed and shown to be safe for continued operations (WHC 1987), the N Reactor remains shut down for lack of need for its principal product, plutonium.] At the same time a National Academy of Sciences (NAS) committee was commissioned to assess the safety of all DOE reactors (NAS 1987). The NAS committee (strictly speaking, a committee staffed by members of the National Academies of Science and Engineering plus other knowledgeable experts, supported by their staff agency the National Research Council) made a number of recommendations to DOE. As a result of these and

other recommendations made by additional review committees,* a massive safety improvement program was undertaken by Du Pont and the DOE's Savannah River Operations Office. At about the same time, Du Pont announced that it was no longer interested in renewal of its contract to operate Savannah River for the DOE, so the search began for a successor. Westinghouse Electric Corporation (Westinghouse) was chosen in September 1988 and was granted a transition contract to prepare for assumption of operations management on April 1, 1989. Under this contract, Westinghouse Electric Corporation was also requested to perform a review of the safety of the SRP production reactors, as it had done prior to assumption of responsibility for N Reactor at the Hanford Site. This report is the result of that review.

*Perhaps most notable are the DOE's Crawford Committee, the DOE Environmental, Safety and Health (ES&H) Technical Safety, Quality Assurance, and Design Review Committees, and the Advisory Committee on Nuclear Facility Safety.

Table 1. Safety Differences Between Savannah River Plant

Feature	Advantage to	Summary reason
Temperature and pressure	SRP	Operation at or below atmospheric boiling conditions vs 2,250 lbf/in ² means that much less energy is available to aggravate pipe breaks or challenge containment.
Maintaining cooling	SRP	The SRP main coolant pumps are supplemented by pony motors that are constantly energized by dedicated power supplies.
Independent reactivity shutdown	SRP	In addition to control rods there are separate safety rods and a pressurized means of injecting soluble poison.
Core instrumentation	SRP	Each of the hundreds of fuel assemblies has dedicated temperature and pressure instrumentation feeding information directly into a safety computer.
Simplicity	SRP	Lacking power generation equipment, the operator has considerably fewer functions to perform.
Fuel material	SRP	The use of aluminum and the operating conditions make the metal-water reaction leading to hydrogen a much less likely consequence of severe accidents than in the case of zirconium in the LWR.

Table 1. Safety Differences Between Savannah River Plant and Light-Water Reactors. (sheet 2 of 2)

Feature	Advantage to	Summary reason
Leakage detection	SRP	Detection of leakage of primary coolant is greatly enhanced by the presence of tritium formed by neutron absorption in the deuterium.
Confinement/ containment	LWR	Only a containment will prevent noble gas release following a hypothetical severe accident--the confinement will be effective for other fission products.
Natural circulation	LWR	The downflow through fuel elements and the loop layout of the SRP reactors complicate the initial stages of loss-of-cooling cases.
Uranium enrichment	LWR	Although it enhances production, the highly enriched fuel in the SRP reactor makes conceivable a recriticality condition following a hypothetical severe accident leading to core rearrangement.

SRP = Savannah River Plant.

LWR = Light-water reactor.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

I. Safety Philosophy and Restart Criteria

Preface

The safety philosophy expressed here is derived directly from commercial nuclear power industry practice, restated in terms relevant to the SRP production reactors. The commercial industry reactor safety record has been exceptional despite a wide variety of individual designs, construction techniques, and practice in the conduct of operations. Indeed, the SRP reactors themselves enjoy an excellent safety record, but their statistical base is small compared to that of the industry as a whole. Thus their own safety record does not by itself provide a sufficient level of assurance of continuing safe operation. Commercial reactor experience adds substantially to the statistical base and applies well to the HWR because of similar materials, processes, and fundamental safety objectives applied over a range of designs and design vintages. Thus we believe that the philosophy underlying this record of success will still be valid and meaningful when applied to the SRP reactors.

This safety philosophy is articulated in the section below; then restart safety acceptance criteria are formulated based on this philosophy, taking into account specific parallels with older commercial facilities where there is a recognized need to acknowledge and evaluate shortcomings relative to the latest design practices and requirements.

The concept of nuclear safety can be embodied in four fundamental principles: perspective of risk; self-examination; defense in depth; and recognition of the interrelationships among design, operations, and management.

Perspective of Risk

The paramount interest and objective of reactor safety policy is protection of public health and safety. The commercial nuclear industry has recognized the primacy of this objective by adopting qualitative and quantitative goals that are based on the principle that nuclear risks should not be a significant addition to other societal risks. The DOE is currently formulating a similar set of goals applying both to the general public and to plant workers. The qualitative goal is that individual members of the public should be provided a level of protection from the consequences of nuclear plant operation such that it poses no significant additional risk to life or health.

This quantitative goal is expressed as follows: the incremental risk of prompt fatalities and/or latent cancers leading to fatalities should not exceed 0.1% of the corresponding general background risk. This goal is an aiming point or benchmark for performance that nuclear designers and operators should strive to achieve. In this regard, the importance of mitigation of nuclear power plant

accident consequences is recognized, and containment/confinement, siting, and emergency planning are integral parts of the defense-in-depth concept associated with accident prevention and mitigation.

In applying the safety goals, it is recognized that a calculated level of risk that exceeds the 0.1% ratio does not necessarily constitute a significant additional risk. The achievement of this target value only supports an expectation that people living or working near these plants need have no special concern about the plant's proximity. The choice of a numerical value was based on the ability of the commercial nuclear industry to meet these goals for most modern plant designs, thus precluding the need to perform a detailed cost-benefit analysis to support an acceptable level of risk. In the case of older plant designs that cannot achieve the benchmark levels for acceptable risk, continued operation can be justified by performing cost-benefit evaluations of the alternatives in design and operation (including plant closure). It is also recognized that the process of quantifying the risks from operation (and severe accidents) of a facility leads to a greater level of overall safety because insights gained from the process may in turn lead to improvements in design and operation.

Self-Examination

The safety goals must be recognized as targets that describe the level of acceptable risk for long-term operation. An alternative justification can be developed for short-term operation of a facility with improvements to bring the facility to an acceptable level while the long-term goals are being pursued. Thus, while a facility of the vintage of the Savannah River production reactors may not be able to achieve the benchmark or target values set for new reactors, the attempt to quantify the risks identifies areas where improvements in safety can be implemented in a cost-beneficial manner. The comparison of plant performance in relation to the acceptable level of risk is the proper perspective for overall safety assessment.

The safety goal also has merit as an expression of intent that the incremental public risk from reactor facility operation be, in essence, negligible and that safety judgments, then, be made in that context. The result is a continuing quest for safety excellence, which may seem to be an elusive ideal, but in fact is a direct parallel to the total-quality thrust vital to success in industry today. Thus, the second principle to be tested in the SRP restart deliberation is that reactor safety is a dynamic concept involving continuous self-examination and improvement.

Defense in Depth

Defense in depth is a proven approach to the provision of extra safety, which recognizes the potential for plant challenges that, because of a special and unique complexity, cannot in every case be predefined and evaluated on a deterministic basis.

Prior to the Three Mile Island accident, the overwhelming concentration in regulation was on design and on hardware integrity and performance. The cornerstone of this thrust was the concept of defense in depth. This concept emphasizes multiple, successive barriers to fission-product release, without undue reliance on a single one of the barriers for overall adequate protection. Basic design integrity was emphasized through imposition of increasingly strict codes and standards. Extensive protection and safeguards capability were required by prescriptive and deterministic considerations over a wide range of postulated system challenges and potential failures. Management and operations practices and capabilities were given comparatively less emphasis, perhaps reflecting both the background of most of the operators and regulators and the fact that most of the adverse experience was yet to be encountered. Nonetheless, the effort on design and hardware, reflected in the defense-in-depth concept, was by no means misplaced and has served the industry well, as is indicated by the overall record. Nor was this success just luck. The extra provision of a forgiving design in large measure compensated for the lesser emphasis placed on management and the conduct of operations.

Interrelations among Design, Operations, and Management

Reactor safety, in the broadest sense, derives from balanced adequacies in each of three fundamental areas: design, operations, and management. Beyond a minimum level of adequacy absolutely necessary for each by itself, compensation in any one area can be provided by extra provision in the others so long as there are structured and enabling interfaces linking that one to the others. ('Design' here encompasses the 'as-is' plant--not just as designed, but as built and as maintained.)

Figure 1 illustrates this concept of interdependence among the three areas of required emphasis, with the enabling interfaces called out. Each area is characterized by major elements or attributes. As stated in the principle above, compensation in specific elements in one area can be provided through greater provision in specific elements of another, provided the enabling interface is adequate. An example from SRP is that extra assurance for concerns arising from primary-system boundary-integrity questions can be provided by operator action on low-threshold leakage as enabled by proper technical specifications, in turn enabled by leakage-detection enhancement because of the tritium in the coolant. A clear understanding of such interrelationships provides a capability for

Figure 1. Fundamental Areas of Safety Influence.

effecting timely safety improvements that might not otherwise be possible. This powerful tool also underlies commercial practice, especially in dealing with older nuclear plants.

Safety Acceptance Criteria

Four principles, the perspective of risk, continuing self-examination and improvement, defense in depth, and recognition of the interrelationships among the fundamental areas of influence, provide the basis and framework for the safety acceptance criteria formulated below.

The SRP restart program (DOE 1988) involves significant upgrades in each of the three major areas of safety influence--design, operations, and management. It is inherent in the principle of continuous improvement that the upgrading process not be completed in the near future. Thus we recognize that one threshold can be defined for the resumption of limited operations, another for sustained full production, while work would continue on yet longer range improvements. The fact that such work is continuing is not to be taken as a sign that all operation prior to its completion was unsafe, but rather as the natural consequence of continued striving for excellence. Indeed, the case should be made that resumption of limited operations upon proof of achievement of a required minimum level of adequacy provides the necessary arena for achieving management and operations excellence across the board.

1. The reactor must be capable of being shut down and maintained in a safe-shutdown condition, including the capability for adequate long-term cooling and essential core monitoring, for both normal and anticipated operational occurrences.

This criterion emphasizes accident prevention as fundamental to both risk reduction and defense in depth. It includes consideration of structural integrity, equipment operability, and systems performance capability in light of further specific subcriteria.

1A. Structural integrity and equipment operability must be demonstrated and maintained under normal as well as appropriate and adverse load conditions using established and accepted codes, standards, and analysis methods and programs for the following key reactor systems:

- Process water system
- Cooling water system
- Moderator recovery system
- Reactor shutdown
- Essential core monitoring.

1B. Anticipated operational occurrences from potential equipment malfunctions or operator errors must be known and understood.

1C. The reactor core must have inherent nuclear feedback characteristics that compensate for rapid and inadvertent reactivity additions.

1D. Acceptable core limits must not be exceeded during normal and anticipated transient conditions as demonstrated by verified codes and methods.

1E. The plant design must be 'robust' and equipment malfunctions and/or operator actions that result in the transition from an anticipated operational occurrence to an accident, particularly a severe accident involving core damage, must be identified and understood.

2. Reliable mitigation systems must be provided and available to limit core damage and fission-product release for postulated design-basis accident events and conditions.

This criterion is, again, responsive to the principles of risk avoidance and defense in depth. It deals with the risk of accidents regardless of preventive measures and the basic protection afforded. It also involves considerations of structural integrity, equipment operability, and systems performance capability through specific subcriteria.

2A. Appropriate design-basis events must be defined to represent extreme but credible safety challenges that in turn define mitigation system performance requirements.

A judgment must be made of the boundary between design-basis and beyond-design-basis events. This judgment will leave a very small but nonzero level of risk that requires considering the placement of these reactors on a dedicated site and also balancing, by a responsible authority, against the risk to the United States of doing without the materials that are produced when they are operating. This issue is addressed in the third set of criteria.

2B. There must be reasonable confidence that the following mitigation systems meet their functional requirements consistent with the definition of design-basis events and acceptable levels of risk:

Emergency cooling	Airborne activity control
Confinement	Confinement heat removal
Water disposal (sumps)	Reactor room spray.
Discharge machine	

2C. There should be confidence that the mitigation systems listed in 2B maintain their integrity and operability consistent with an acceptable level of reliability.

2D. Appropriate emergency response procedures, technical specifications, and administrative controls are in place to ensure mitigation system readiness and operability. Operations personnel must be thoroughly trained to understand and control off-normal events.

2E. The intrinsic characteristics of the design must be tolerant so that local faults in the core do not propagate to a core-wide situation.

3. The level of threat posed by accidents beyond the design basis should be understood using probabilistic risk assessment (PRA) methodologies combined with experience and judgment and controlled to the extent possible.

This criterion addresses the responsiveness to the acceptable risk from accidents and the extent to which the residual risk can be controlled through an appropriate combination of design, operation, and management. The risk should be addressed using currently recognized and acceptable techniques in PRA, including the evaluation of uncertainties and sensitivities. The acceptable level of risk is addressed in the following criteria.

3A. A target value that allows for acceptable levels of accident risk and that balances the need for production against the potential risks must be defined for the SRP reactors. [This criterion must be addressed by DOE--the committee has had the benefit of DOE's draft safety goals (DOE 1989).]

3B. The most frequent accident scenarios that result in damage to the reactor core must be identified, and, to the extent practicable, the frequency of such events must be controlled to an acceptably low value consistent with their consequences through a combination of design, operation, and management practices.

3C. The most frequent accident scenarios that result in releases of radioactive material that might exceed the U.S. Environmental Protection Agency (EPA) Protective Action Guidance (EPA 1975) for offsite exposure of the public must be identified, and, to the extent practicable, their frequency must be controlled to an acceptably low level through a combination of design, operation, and management practices.

3D. The operations personnel must be trained in the prevention and mitigation of severe accidents.

4. A strong and continually improving safety management system must be in place and functioning.

This criterion recognizes the importance of management as it underlies both the design and operations areas. Management provides the guidance and criteria to sustain a safety-dedicated culture involving continuous examination and improvement. Management can balance risk by implementing improvements in operations that can offset, at least to some extent, shortfalls in certain mitigation systems. An example from commercial practice is the fire watch, where meeting up-to-date fire protection standards would be impossible. Of course, the balancing process is itself subject to management oversight, as reflected in the subcriteria below.

4A. Administrative controls are in place for continued safe operation.

4B. An appropriate hierarchy of effective and independent oversight organizations is defined and functioning.

4C. A safety-issues management system is in place for evaluating, prioritizing, planning, and dispositioning safety improvements on an ongoing basis.

4D. Most important of all, management at all levels sets clear lines of responsibility and authority, ensures that all levels of the organization are competent and have the necessary training and tools to carry out their responsibilities, infuses them with a desire to achieve higher standards of professionalism and excellence, and fosters a climate in which nuclear safety is never compromised for schedule.

II. Application of Criteria to Savannah River Production Reactors

This section summarizes the conclusions and findings of the various subcommittees, whose recommendations are stated along with summary justifications in Section III. The appendices contain the more detailed reports of the subcommittees. Table 2 provides a listing of the membership of the committee and its subcommittees, along with an index number used to identify the subcommittees in these two sections and in the appendices.

1. MECHANICAL SYSTEMS

The Mechanical Systems subcommittee reviewed the systems, structures, and operations that provide the means of shutdown and long-term cooling, as well as mitigation of postulated accidents. The review focused on the functional adequacy and reliability of systems to satisfy design bases, taking into account environmental factors and the reasonableness of expected operator actions.

Members of the subcommittee had the benefit of extensive discussion with SRP reactor systems and operations personnel, reviewed the pertinent procedures and standards, and walked down the equipment in three reactor areas. In addition, this group consulted with the subcommittees reviewing PRA; electrical, instrumentation, and control systems; seismic; and safety analysis in forming its evaluation.

When compared with commercial power reactors, the mechanical systems of low-pressure HWRs are relatively simple. Their operating history has been essentially trouble free, and the various SRP reviews and walkdowns undertaken during the past year provide additional confidence in their continued good performance. However, the review identified several aspects of protection against the consequences of low-probability events that adversely affect the reliability of certain safety functions. These concerns are summarized below. Corrective measures involving procedural as well as physical improvements are recommended in Section III.

Table 2. Westinghouse Independent Safety Review Listing of Committee and Subcommittee Members.

Number and title of group chairman or sponsor		Members
WISR	WESTINGHOUSE INDEPENDENT SAFETY REVIEW Howard Arnold, Chairman	Howard Arnold, Dan Call, Hans Fauske, Bill Leggett, Nick Liparulo, John McAdoo, Bill McShane, Lee Strawbridge, George Toto, Dennis Richardson (Secretary)
1	MECHANICAL SYSTEMS John McAdoo, Sponsor	Mart Young, Larry Conway, Bob Magee
2	STRUCTURES, SEISMIC, AND MATERIALS Bill McShane, Sponsor	Bill Lapay, Don Griffin, Jim Anderson, Tom Mager, George Bohm
3	ELECTRICAL, INSTRUMENTATION, AND CONTROL Bill McShane, Sponsor	Mike Boger, Don Vochinsky, Jim Easter, Pete Morris
4	FIRE PROTECTION Bill McShane, Sponsor	John Bell, Bob Lichfield
5	CORE DESIGN Bill Leggett, Sponsor	Allan McFarlane, Dick Doncals, Hans Toffer, Ron Coffield
6	CONDUCT OF OPERATIONS George Toto, Sponsor	Dan Swaim, Keith Bonser, Dick Coulthard, Lee Legowik
7	PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENTS Nick Liparulo, Sponsor	Mike Hitchler, Bob Lutz, Mike Zentner, Jerry André, Bev Cassidy
8	SAFETY ANALYSIS REVIEW John McAdoo, Sponsor	Toby Burnett, Tim Andreychek, Steve Love, Bob Steitler
9	POWER LIMIT AND ACCIDENT PROPAGATION Hans Fauske and Lee Strawbridge, Sponsors	George Clare, Mike Epstein, Bob Henry

Operating Procedures--In the event of a large-area rupture of either a process water system (PWS) pipe (large loss-of-cooling accident) or one of the main cooling-water headers inside the 105 Building, procedures call for the operator to make decisions and take action to ensure successful mitigation. Before taking action, he must perform certain checks, as an incorrect response might exacerbate the event. The time available for accomplishing the checks is shorter than would be allowable in commercial reactor practice; and, in the reviewers' opinion, the challenge is made more difficult by the quality of information likely to be available to the operator.

In the large loss-of-cooling accident (LOCA), initiation of the emergency cooling system (ECS) is automatic when a low D₂O level in the reactor tank is detected. However, the operator is required both to throttle ECS flow to match water removal capacity and to locate and isolate the break by closing valves in the affected process water loop. To accomplish these actions, the operator must diagnose the event and then monitor at least four process variables to avoid (a) overthrottling and/or isolating the wrong loop, starving the core, and (b) under-throttling, thereby allowing flooding of the sump pump motors.

In the large break of a cooling-water header inside the 105 Building, the operator must manually initiate ECS quickly to offset loss of reactor circulation from flooding of the Bingham pumps. The time available for manual action can be on the order of 5 min, and, as improper actuation could have severe plant consequences, a number of checks must be made prior to taking action.

Both of the operator-response requirements outlined above exceed the industry standard for expectation of high reliability, even with well-qualified control-room personnel (criteria 2B, 2D).

Surveillance and Maintenance--The review found that certain key valves either are excluded from currently required surveillances or are subject only to functional testing. Considering the age of these valves and the fact that internal degradation of a kind that would escape detection in functional testing could result in flow blockage, the reliability of pathways containing these valves for essential water flow following an accident is degraded (criterion 2C).

Test data have shown that mitigation-system pumps are subject to significant flow-performance degradation. The degree of this degradation is not routinely determined under existing surveillance programs (criterion 2C).

Performance Testing Related to Loss of Cooling and Loss of Pumping Accidents--Flow testing of the ECS function is now performed every two years to verify delivery assumptions for core-limit calculations. The review found that these tests and analyses contained some deficiencies in case selection and in the way results are verified, computer methods are controlled, and margins for uncertainty are applied (criterion 2B).

The two-year test does not simulate the delivery of flow to the process tubes in a LOCA, most of which is supplied by continued operation of the Bingham pumps. A test of this type is planned in the near future in L Reactor.

The subcommittee's review of this test plan identified some cases of interest, such as an operator's incorrectly isolating an intact loop, which were not to be included. Unfortunately, plenum-level and assembly-flow instrumentation available for this test will be less than ideal from the standpoint of supporting the development of improved LOCA evaluation models (criterion 2B).

Sump Capability--To ensure the proper functioning of the Bingham pumps during LOCA events and to improve their availability for postseismic recovery, SRP is now planning to increase sump pump capacity to at least match the flow from ECS and other sources that might reach the -40-ft level during these events. On the basis of this review, those efforts are being broadened to include the provision of features to prevent blockage of sumps by debris (criterion 2B).

2. STRUCTURES, SEISMIC, AND MATERIALS

This subcommittee conducted a review of the buildings, structures, and equipment related to safe shutdown of the reactor and the mitigation of potential-accident consequences. Structural integrity and system safety performance were the important measures related to the plant safety philosophy and restart criteria. The subcommittee considered defense in depth, accident prevention, and risk avoidance as important to the recommendations given. Four criteria have been given in Section I under the subsection "Safety Acceptance Criteria." The review concentrated on the first two criteria concerned with safe shutdown and mitigation. The last two criteria, associated with risk and safety management, were not within the subcommittee's scope.

The structures and systems at the Savannah River reactors have commendable attributes.

- The piping system material is tough and ductile.
- The material is in good condition, not showing any aging or corrosion/erosion except intergranular stress corrosion cracking (IGSCC), which is closely monitored.
- Stresses in the piping and components are generally low because of the loading and temperature conditions, so there is ample reserve strength.
- The system designs are easily accessible, and visual inspections for leaks and deterioration can easily be accomplished.
- The system and structural designs are being upgraded to be consistent with 'current-day seismic criteria.'
- An extensive reactor material program has been carried out for the PWS that clearly demonstrates leak before break.
- The building and structural designs have reserve strength.
- The safety and safety-related structural systems have been designed and constructed to good commercial standards.

The restart criteria being used to qualify seismically the systems and structures are good ones because their emphasis is on reasonable assurance that the reactor can be shut down and cooled. Walkdown qualification procedures are acceptable and avoid extra cost and time that may be required to perform detailed analyses. Further, it is not necessary to perform analyses specifically to Regulatory Guide 1.60 and 1.61 seismic requirements (NRC 1973a, 1973b), but only to show seismic qualification to be comparable to these requirements.

The issues identified were discussed at length and recommendations provided. Actions that are considered to require completion prior to reactor restart were grouped in the short-term program recommendations. Those that are important but do not affect reactor restart are given in the long-term program.

Structures--The reactor gas plenum can be overpressurized upon actuation of ECS when the system is water solid. Although the consequences are probably not catastrophic, a more complete analysis should be provided (criterion 1).

The review of the fuel and thermal shield structural design did not reveal any potential problems; however, there is no structural-analysis documentation to demonstrate adequacy (criterion 2).

Inspection of the supports and anchors that are part of the safety systems is important, as demonstrated by the Seismic Qualification Utility Group (SQUG) walkdowns, which identified several supports and anchors that were either inadequate for seismic loading or improperly maintained (criteria 1, 2).

Materials--As noted above, the materials used in the plant are reasonably well chosen for their application. However, the subcommittee has identified issues relative to in-service inspection (ISI) and qualification of cooling water system (CWS) piping at low temperatures (criterion 1).

Because the vessel has been analyzed structurally, because no leaks have occurred in vessels of the same design, and because the radiation damage level remains acceptable and the potential leakage from a 360° crack is less than that from a piping double-ended guillotine break (DEGB), the subcommittee concluded that vessel ultrasonic testing (UT) examination should be included in the longer term PWS ISI program. A UT examination prior to startup is not required.

Seismic--Since a number of fluid systems are not being seismically qualified prior to restart, and because even qualified systems might experience leakage at seals and flanges, there is a risk that the PWS pumps will be flooded, resulting in a loss of decay heat-removal capability. It is necessary to remove this leakage. The contaminated-water removal and storage system (CWRSS) and the emergency power system provide for water removal but they are not seismically qualified (criterion 1).

The seismic improvements being made to the plant are to ensure that the reactor can be shut down and cooled. However, defense in depth to mitigate events that might occur following a seismic event is lacking. For example, the

ECS and the various confinement fluid systems are not qualified. A review of systems containing large inventories of radioactivity that may fail as a result of seismic events has not been systematically conducted. These systems include fuel-handling equipment and the PWS distillation system (criterion 2).

The subcommittee had some concerns about techniques used for the dynamic analyses, particularly the spectrum model techniques (criteria 1, 2).

3. ELECTRICAL, INSTRUMENTATION, AND CONTROL

The Electrical, Instrumentation, and Control subcommittee examined instrumentation, control, and electrical power systems associated with safety functions for the Savannah River reactors. Safety acceptance criteria are stated in Section I of this report. The focus of this subcommittee's evaluation is on criteria 1 and 2. A rigorous review in terms of criteria 3 and 4 was not performed, but concerns regarding these criteria were discovered in the course of evaluation.

Five safety functions were judged to be critical: subcriticality, core cooling, heat sink, confinement, and PWS inventory. Each of these has both monitoring and execution aspects. Under all conditions postulated for the reactor plant, methods of monitoring must be available so that the condition of the safety function can be assessed. Should it be determined that the safety function is threatened, methods must be available to return the function to an acceptable status. Separation of circuits and equipment, redundancy, diversity, testability, seismic and environmental qualification, and maintenance practices are issues considered in assessing the systems' susceptibility to single and common-mode failures.

The subcommittee was favorably impressed by the professional caliber of the personnel contacted at the SRP. An awareness of nuclear industry standards and a desire for continuing improvement of system design and performance were evident. Many of the systems include redundant, diverse, or fail-safe design features, and some separation of redundant components exists because of plant configuration. The DOE K Reactor restart strategy (DOE 1988) and many of the SRP responses to that plan alleviate much of the concern over vulnerabilities to failures from fire or seismic events.

The subcommittee found many strengths in the design of the systems, along with several vulnerabilities. A summary of observations is presented below. The five critical safety functions are discussed as well as several general issues.

Subcriticality--Three methods are provided for negative reactivity insertion: control rods, safety rods, and the supplementary shutdown system (SSS), i.e., injection of concentrated gadolinium nitrate solution (Ink). These can be actuated by the primary shutdown system (PSS), safety computers, or manually.

An automatic seismic trip is planned for the SSS. Only the SSS has been seismically qualified and will meet separation criteria. An existing seismic trip at 0.02g is not itself seismically qualified but would probably function at such a low seismic level. Existing methods for monitoring reactor subcriticality are not seismically qualified and are potentially vulnerable to a fire in the control room. Subcriticality is not monitored by the remote emergency monitoring and control system (REMACS) (criterion 1).

Core Cooling--Essential parameters for monitoring core cooling by the PWS are suggested as being the reactor tank level, pump operation, and the level of the 105 Building sump. Sump level is suggested since flooding in the pump or motor rooms threatens the core-cooling function. Existing methods and modification efforts currently under way at SRP partially satisfy the monitoring requirement but may be susceptible to single failures or fires. Spurious actuation of PWS valves from fire or a seismic event is possible and threatens core cooling. Spurious actuation of ECS is also possible and is undesirable because of the tritium released and the possibility of overpressurization (criteria 1, 2).

Heat Sink--Existing methods for monitoring and executing this function, together with modifications planned before restart, were found to be acceptable. Many of the requirements are satisfied by visual observation or manual operation (criteria 1, 2).

Confinement--The set of design-basis events for which the airborne activity confinement system (AACS) must operate is limited; for instance, it is not required to perform after a seismic event. Great emphasis is placed on the subcriticality and core-cooling functions to ensure that no event occurs requiring the AACS. Existing methods of monitoring and control appear to be adequate in the short term (criterion 2).

Process Water System Inventory--Qualification of the moderator recovery system (MRS), including electrical power, instrumentation, and controls, is already planned. Redundant methods of monitoring tank level should be provided as previously discussed for core cooling (criteria 1, 2).

General Design Criteria--Because of the vintage of the design, separation and qualification criteria comparable to current design standards have not been systematically applied to safety systems. Some safety functions are vulnerable, therefore, to external occurrences such as fire and seismic events (criteria 1, 2, 4).

Human Interfaces--Lack of separation and seismic and environmental qualification shifts the burden of defense in depth to the operator. His/her understanding of plant condition and potential threats to critical safety functions is essential to his/her following alternative paths available for event mitigation.

Status trees showing critical safety-function and symptom-based procedures are a proven method of aiding the operator in his/her actions (criteria 1, 2, 3).

Support Systems--The SRP site electrical power generation and transmission system is designed with sufficient redundancy and diversity to supply power to the reactor plant with reliability comparable to or better than that afforded commercial nuclear power plants. If power to the plant is lost, many systems and components normally used for safe shutdown will depend on emergency generators that are not seismically qualified. The maintenance program for safety-related batteries has not included the industry standard performance tests and intercell resistance checks (criteria 1, 2, 4).

Configuration Control--Drawings and other design documents reviewed by the subcommittee do not identify the overall scope or boundaries of the safety systems. Identification of safety circuits and equipment on top-level drawings is essential to safe conduct of operations and effective design-configuration control (criterion 4).

4. FIRE PROTECTION

The fire-protection safety assessment consisted of an extensive walkdown of the K Reactor, review of operating procedures and design-basis documentation, and safety reviews performed by others. The subcommittee conducted the review considering the Westinghouse Independent Safety Review (WISR) criteria in Section I above.

Fundamental to this entire review is the defense-in-depth concept. This concept as it applies to reactor-plant fire protection has three objectives.

- Prevent fires from starting.
- Detect rapidly, control, and extinguish promptly those fires that do occur.
- Provide protection for structures, systems, and components important to safety so that a fire not promptly extinguished by the fire-suppression activities will not prevent safe shutdown of the plant.

The fire-protection record at the SRP has been outstanding because combustibles are limited in most areas and procedures are in place to control combustibles carefully during maintenance.

The K Reactor restart criteria prepared by DOE, Du Pont, and Westinghouse in November 1988 (DOE 1988) have led to a number of actions with which the subcommittee is in agreement. These include plant changes to install a standpipe and a new water source for fire fighting and the installation of fire-detection equipment in areas not normally accessible. There are also plans to improve procedures governing fire-prevention inspections, fire watches, care

of fire-protection equipment, emergencies, control of transient combustibles, and fire fighting.

The principal safety findings, as a result of the subcommittee review, are the following.

- Fire-hazard analyses are incomplete for critical areas of the reactor facility (criterion 1). The major concerns are as follows.

- The control room could become uninhabitable and the REMACS inoperable. Therefore, there would be no opportunity to read the necessary postshutdown instrumentation.

- A fire might result in the inadvertent activation of PWS and ECS valves and ECS pump operation.

- Emergency response procedures do not address fire recovery (criterion 1). The principal concerns center on placing the reactor in a safe shutdown condition and monitoring plant conditions during and after a fire.

- Life-safety provisions may be insufficient to accommodate required emergency actions (criterion 3).

- Adequate water supplies are not available for fire fighting (criterion 2). Some actions are already under way to improve this situation prior to startup.

- There is no formalized fire-protection overview program in place (criterion 4).

- All three objectives of the defense-in-depth concept need to be supplemented.

- There are no fire-protection surveillance requirements (criterion 1).

- Automatic rapid-detection and suppression systems are lacking in most areas of the plant (criterion 2).

- Passive fire-protection features for critical safety functions are not provided in the event of failure or ineffective automatic and manual fire-suppression efforts (criterion 2).

5. CORE DESIGN

The primary considerations are the ability to identify abnormal occurrences that challenge design bases and the ability to predict core performance under these abnormal conditions. The design bases in nearly every instance are to avoid fuel damage and to ensure that the reactor can be made and maintained subcritical. For exceptionally rare events, the design basis may be to ensure that the fuel remains coolable. The core is unique among plant components because it is regularly changed (at SRP, sometimes several times per year), so the process by which core safety is ensured -- the reanalysis, incorporation of changes, accounting for deviations from nominal in the specific fuel charge, and

communications to plant operators -- is as important a consideration as the safety of a particular core.

The Core Design subcommittee examined three major aspects of core design:*

- The criteria--general design criteria (GDC) and delineation of abnormal occurrences
- Core parameters--accuracy and conservatism in reactivity coefficients, power distribution, etc.
- The core design process--organizational responsibilities and completeness.

General Design Criteria--Criteria 10 to 13 and 25 to 29 of the NRC's general design criteria in 10 CFR 50, App A (NRC 1988b) deal with core design and reactivity control. The subcommittee's review turned up no serious shortfall of K Reactor with respect to these criteria. The subcommittee believes that the transient resulting from a dropped part length rod should be analyzed and endorses the ongoing severe-accident analysis, which should address the potential reactivity addition in the event of fuel redistribution. Since accident analyses are not complete and the power level is yet to be set, the subcommittee's conclusions are based in part on the extrapolation of Du Pont work currently under way. Further details are provided in Appendix B.5.

It is worth noting that the K Reactor goes beyond what would be required by the GDC in some instances; the extensive instrumentation on each fuel assembly and the rapidly acting SSS are cases in point.

Core Parameters--Core parameters, which are used in safety analyses, have generally been calculated by Du Pont on a best-estimate rather than on a conservative basis. The subcommittee conducted independent calculations of the temperature coefficients and concluded that Savannah River should reevaluate its predictions, both for positive coefficient during heatup and for negative coefficient during cooldown, to ensure that appropriately conservative coefficients are used. The subcommittee believes that actual power distributions should be calculated for abnormal operation rather than using adverse power distributions selected from normal operation. During the subcommittee's investigation, the rate of negative reactivity insertion by safety rods following a scram was found by Du Pont to be significantly less than previously thought. This finding points out the need for regular tests, typically during startup, to ensure that safety analyses are valid and to provide a basis for steady improvement in analytical

* Specific issues such as acceptable power level vis-à-vis ECS performance following LOCA, core seismic response, and fission-product release in the event of a severe accident, were addressed by other subcommittees.

methods. The subcommittee also believes that all safety analyses should be reexamined to ensure an appropriate degree of conservatism.

One aspect of conservative core analysis requires recognition that fuel and core components (targets) will generally differ to some extent from their nominal dimensions and composition. The assembly exit thermocouples should prevent a safety problem from variation in assembly average parameters; but radial, azimuthal, or axial variations within the assembly (e.g. ratio of inner and outer fuel tube powers) will not be detected in the core. Du Pont has begun to develop a statistical treatment of these 'non-idealities;' manufacturing variations need to be reexamined for each charge, and safety analyses should recognize the potential for fuel and targets to be outside of specification. Recent changes in the manufacturing process (the shift from 80 wt% ^{235}U to 60 wt% ^{235}U in nuclear test-gauge usage) should be evaluated for their potential impact on core parameters.

Core Design Process--The high level of competence among the Du Pont personnel interviewed during the core design investigation, the successful operation of the reactors for more than 30 years under conditions representative of the expected future operation, and the intent to limit power on the basis of an extremely improbable accident all give confidence that large safety margins will exist during normal operations and during anticipated operational occurrences. To be effective, the core-design process needs a well-defined context in which changes are evaluated. In commercial practice this context is provided by the final safety analysis report (FSAR) or, better still, by a delineation of all the core parameters that had an important role in reaching the safety conclusions reported in the FSAR. The recommendations of the Core Design subcommittee on completing an SRP safety analysis report (SAR) have been incorporated with those of the Safety Analysis subcommittee.

The core-design process and that of ensuring safety in general are improved by a clearly defined responsibility for the safety evaluations and by the need to defend safety conclusions before an independent review group. Probably as a consequence of a long period of problem-free performance, the core-design process at SRP is highly automated. The responsibility for updating the automated methods -- computer codes -- and performing safety analyses was placed with the Savannah River Laboratory organization (SRL), and the Reactor Technology Department (RTD) had the job of running the codes and passing results to Operations. The subcommittee believes that the responsibility to determine that safety analyses are complete and to defend those safety analyses should be clearly stated as belonging to RTD. The labs will continue to do the bulk of methods development and SAR analysis, but the group closest to operations must understand the methods, concur in them, and be prepared to defend them as being appropriate and complete.

6. CONDUCT OF OPERATIONS

The Conduct of Operations subcommittee reviewed plant training materials and courses, operating and administrative procedures, engineering drawing control, and maintenance (work control) practices. The subcommittee interviewed a cross section of personnel and made workplace observations in addition to document reviews. Interviews were conducted in two ways: one-on-one discussions, and group interviews in which several subcommittee members met with operating units consisting of senior shift supervisor, shift supervisor, senior reactor operator, and reactor operator. The group discussions were such that anyone could contribute, add, or correct any information presented by any of the operating staff. On some occasions the sessions were attended by area supervisors. The review focused on K Reactor, and in-plant walkthroughs were conducted only at K Reactor. The subcommittee members believe that the issues identified are generic to the P, L, and K Reactors and germane to restart efforts, but concur with the philosophy of a phased restart, concentrating on K. The subcommittee was well aware that the K Reactor organization is in a state of flux and that conditions in existence at this writing do not reflect the organizational structure and operating methods that will exist at the completion of the restart actions now in progress.

The performance of the plant staff is a key element in safe reactor operation and encompasses each of the four criteria in Section I; however, the subcommittee believes that no amount of analysis, design, or overview can ensure safety in the conduct of operations without knowledgeable operators and effective line management. This statement of philosophy translates into the equally concise criterion 4 for the acceptability of the conduct of operations: a strong and continually improving safety-management system must be in place and functioning (i.e., evident in the workplace culture). Thus criterion 4 was the primary criterion used by the subcommittee. The Conduct of Operations subcommittee made a broad examination of the existing organization and the restart plans. The team then applied its collective judgment, based on current practices and the team's perception of planned improvements, as to the acceptability of restart.

Personnel contacted at SRP, and particularly at K, were helpful and candid with the subcommittee. Without exception, each person was looking forward to restart and seemed eager to do his/her part to bring restart closer.

The DOE restart strategy (i.e., the 'Charlotte Criteria') (DOE 1988) provides an excellent basis for the necessary organizational changes at the SRP reactors. The restart criteria are broad and comprehensive, and identify many tenets of modern nuclear power plant management. While endorsing the DOE restart strategy, the subcommittee offers a number of recommendations presented in Section III.

Configuration Control--Up-to-date procedures, specifications and diagrams must be on hand and used to control plant evolutions. As-configured drawings showing component locations, function, nomenclature, and other information necessary for complete and unambiguous operation and alignment are essential in plant control. No work or operation on the plant should be allowed unless it is known that reactor safety and personnel safety are preserved (criterion 4A). A review of the configuration control system used at K Reactor was made, and the methods used to control work and design changes were evaluated.

The control room does not have as-configured piping and instrumentation diagrams (P&ID) or electrical single-line drawings of strategic systems on hand. The K Reactor does not have a controlled drawing print file of P&ID, single-line electrical and logic diagrams, and design changes necessary for K Reactor restart in the control room; therefore, no system exists to ensure that such drawings and design changes are updated when a revised drawing is issued and that audits are scheduled and conducted on controlled drawing files (criterion 4A).

The SRP does not have a system that ensures that all types of K Reactor modifications, either direct or indirect, that result in a physical change to the plant operational configuration are made available to the Operations Procedure Development group, Training, and other operations support groups (criterion 4A).

A work-control system for a nuclear power plant should provide for problem identification, problem resolution and evaluation, identification of the type of work to be done (i.e., maintenance, corrective maintenance, or modifications), detailed work instruction for the performing organization, testing and retesting of completed work, documentation of test results, training, updating of spare parts inventories, turnover to operation, revision of or development of operating procedures, revision of affected drawings and design documents, and approval of the work to be done by Engineering, Operations, Quality, and Safety. The current work-control system possesses some of the elements listed; however, the level of rigor and detail is not consistent with management practices at nuclear power plants (criteria 4A and 4D). The DOE restart strategy (DOE 1988) identifies the minimum necessary actions in the work control area to conduct a safe restart of the K Reactor.

Training--Training programs were reviewed. The overall program seems well conceived, as was concluded by the Reactor Safety Advisory Committee in their review of January 31, 1989. The focus of the subcommittee's review was to evaluate present knowledge of personnel assigned to support a K Reactor startup and the quality of training, as measured by the retention of the trainees. The review covered training for reactor operations, power operations, component handling, chemistry technician, radiation-protection technician, maintenance, and emergency preparedness. Classroom, simulator, and in-plant observations were made. Document reviews and personnel interviews were also conducted.

The restart training being presented covers many subjects and is given at such a rapid rate that retention is diminished. The knowledge level of operators

is lower than found at other sites for similar functions. The qualification requirements are below industry standards (criterion 4D).

The Du Pont methodology of reactor operation was based on operators' responding and operating in accordance with written procedures. Knowledge of the underlying reasons for the actions required by the procedures was not considered necessary for the operator to execute operating actions successfully. This methodology is inconsistent with that of the power reactor industry and does not reflect the benefits of lessons learned from the Three Mile Island experience. In addition to following procedures, nuclear power plant operators are required to have a broad base of knowledge in fundamentals as well as detailed knowledge of their plant. The new programs in place reflect these new requirements, but have not had sufficient time to be absorbed.

The subcommittee finds that the DOE restart strategy (DOE 1988) delineates a minimum set of technical knowledge upgrades to allow safe restart of the K Reactor. The new management team will be challenged to establish rising standards of adequacy that bridge the gap from 'safe' to 'excellent' operation (criteria 4 and 4D).

Plant Operations--The DOE restart strategy (DOE 1988) establishes a vision of an effective plant organization. Great change from the current practices is required, in spite of the fact that several months have elapsed since the restart criteria were established. Some personnel working on administrative systems (e.g., tagouts) may not have had industry experience except at SRP. Therefore, changing the systems to meet nuclear industry or INPO standards may be difficult. The restart criteria do not establish a requirement for line management to assess the adequacy and effectiveness of the restart actions with regard to plant operations personnel and administrative systems (criteria 4A and 4D).

The K Area management team is an operations management team but is not yet an effective plant management team. The key disciplines (operations, maintenance, engineering, reactor engineering, and training) do not report to a plant manager who is held fully accountable for all aspects of plant operation (criterion 4).

Personnel/Morale--The P Reactor startup attempt and the more recent K Reactor water hammer event have had a negative impact on morale in the Operations Department even though personnel are eager to restart K. Those being asked to make many changes are not yet fully aware of the reasons for the philosophy underlying the changes. It was not evident that the DOE restart strategy or criteria have been shared with the first-line workers or supervisors. Not understanding the basic philosophy makes it doubly difficult to assimilate the myriad changes occurring.

In spite of these concerns, the subcommittee found the K Reactor staff members proud of their past accomplishments and willing, even eager, to show that they can meet new standards.

7. PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENTS

This subcommittee investigated the capability of the reactor design and operation to prevent or mitigate a severe accident. The investigation included the frequency of initiating events that could lead to a severe accident, the reliability and availability of systems to prevent those initiating events from propagating to a severe accident, and the actions of the plant operating staff in responding to such an accident. The subcommittee also investigated the capability of plant systems, confinement, and the plant operations staff to mitigate the consequences of a severe accident, should such an event occur.

The subcommittee focused on the following four major areas:

- Component reliability
- Systems reliability
- Accident sequence analysis
- Safety goal and confinement assessment
- Title 10, CFR, Part 100 (NRC 1988d).

The criteria applicable to the subcommittee's study included 2C and 3 of Section I, which concern the reliability of the mitigation systems, the ability of the mitigation systems to respond to accidents, and the level of threat posed by accidents beyond the design basis. In addition, DOE is in the process of establishing PRA-based safety goals for its production facilities (see Attachment 3 to the Nuclear Safety Policy, 2/15/89 draft). These draft goals provided a useful benchmark against which the subcommittee could measure severe-accident and risk perspective. Measurement against these goals requires the use of PRA. Du Pont has had a PRA under way for several years and, while it is not yet complete, much of the internal event information was available to the subcommittee. Du Pont personnel have been very agreeable in providing this information and extremely helpful in providing information and explanations on system/plant configuration and operation. In addition, the subcommittee has performed an independent assessment of the risk from internal events. (It should be recognized that the subcommittee's independent assessment was a 'best effort' over several weeks to do what normally requires two or more years for the detailed assessment.) This independent assessment also provided insights into SRP reactors. The following discussion provides the subcommittee's assessment in terms of the appropriate criteria.

Criterion 2C -- Component and System Reliability--The systems reviewed in this assessment were those considered important to plant safety. Two general conclusions are noted. The reliability of the normally operating systems used in accident mitigation are judged to be acceptable; that is, these systems will not dominate accident mitigation failure. The reliability of the standby systems could be improved by decreasing the technical specifications

type of surveillance testing intervals. Given these improvements, the reliability and availability would be adequate.

The normally operating systems evaluated included the PWS, CWS, and AACS (note that the AACS assessment does not include failure of the filters, which is addressed in the level 2 assessment, and it is assumed that the fans are designed to operate in a severe-accident type of environment). The standby systems include the ECS, CWRSS, confinement heat removal system (CHRS), automatic incident actuation system (AIAS), reactor shutdown system (RSS) and PWS valves required for break isolation and once-through cooling alignment. Testing for the majority of these systems is now performed on a semiannual or annual basis. The probable availabilities of the ECS, CWRSS, and CHRS will improve significantly with surveillance frequency increases. The CWRSS reliability could also be improved by providing better screening and filtering of flow to the pumps; the pumps are currently vulnerable to debris, as was noted by the Mechanical Systems subcommittee. The reliability of the CHRS is limited by the operator action required for actuation. The reliability of the RSS is judged to be adequate. The reliability of the AIAS is judged to be adequate with respect to the systems it actuates (ECS in particular), provided that restrictions on the number of channels out of service at one time are implemented.

In addition, it was noted that a program to identify component root cause failures and to provide feedback to plant maintenance does not exist.

Accident Sequence Analysis--The events considered in detail in this assessment include LOCAs and loss-of-pumping accidents (LOPAs). The decision to consider these two types of events was based on the greater challenge these events present to the safety systems than do other events. In general, it is concluded that the operator actions required to mitigate the events dominate event mitigation failure. The ECS is the mitigation system of primary importance while the CWRSS system is important when long mission times are considered. The LOPA event will dominate the core damage frequency. Operator actions of greatest importance are ECS initiation following a cooling-water pipe break that leads to loss of process water flow, break isolation following a LOCA, and ECS throttling following a large LOCA (to reduce the risk of flooding the CWRSS and PWS pumps).

Confinement and Release Assessment--Evaluations and scoping analyses performed to date for the SRP response to severe accidents show that the predicted offsite severe-accident risk will be within the DOE safety goals (DOE 1989). The scoping analyses also show that the confinement and associated safety systems are effective in mitigating the consequences of severe accidents; no offsite fatalities are expected for severe-accident sequences in which the confinement performs its intended function.

From a structural standpoint, no severe-accident phenomena have been identified that would result in failure of the confinement. Thus, any fission-product releases from the core during a severe accident would be retained initially in

the confinement for treatment by the confinement safety systems. From a functional standpoint, the AACS is designed to mitigate the releases from a core-melt accident. Operation of the AACS is dependent on reliable long-term operation of the CHRS; operator termination of the CWRSS and initiation of the confinement heat removal system prior to core melt; and reliable short-term operation of the reactor room spray system (RRSS). The capability of the AACS to perform its intended function is also dependent on timely renewal of the filter units and reliable operation of the EP-903 fans in severe-accident environments.

In addition to its own and DOE's criteria, the subcommittee was asked to review the SRP reactors relative to the NRC's Title 10, CFR, Part 100 siting criteria (NRC 1988d). The subcommittee found that it could not meet the NRC criteria using the standard nonmechanistic, prescriptive methodology, which assumes full core melt, however improbable. The available analyses indicate that the whole-body dose criterion (25 rem in two hours) is exceeded by a factor of approximately 9 and the thyroid-dose criterion (300 rem in two hours) is exceeded by a factor of greater than 3. Independent analyses have confirmed that these numbers are approximately correct. These analyses also indicate that compliance with the thyroid-dose limits can be shown, using assumptions and models at the limits of those currently acceptable. However, compliance with the whole-body dose criterion cannot be shown using any combination of assumptions and models within the intent of Title 10, CFR, Part 100 (NRC 1988d). A factor of approximately 5 still remains between the acceptable exposures and the lowest values calculated because of the inability of the confinement to retain noble gases.

Thus, it is the subcommittee's finding that SRP will not be able to show compliance with the Title 10, CFR, Part 100 criteria using models and assumptions currently defined as acceptable practice in the commercial LWR field. However, since the Part-100 methodology is based on a very conservative and nonmechanistic methodology, the capability to show compliance with the DOE safety goals (DOE 1989) should replace the need to show compliance with Title 10, CFR, Part 100. If the subcommittee's recommendations are implemented, it should be possible to show compliance with these DOE safety goals.

Summary--Based on the Du Pont PRA and the independent assessment, and assuming the completion of the many safety improvements already planned and those recommended by the committee, the committee reached the following conclusions.

- The DOE safety goals (DOE 1989) for minimum added risk to the public in the vicinity of SRP should be met.
- The SRP plant's expected frequency of core damage resulting from internal events should be less than the DOE goal.
- Plant safety-system reliabilities will be adequate to be consistent with the DOE safety goals (DOE 1989).

- The ability of the plant to respond to severe accidents, and the level of threat posed by these accidents, have been assessed and are judged to be consistent with the DOE safety goals (DOE 1989).
- The PRA can be used to prioritize and evaluate plant changes.

The subcommittee believes that pursuit of improvements in safety should be continuous and that technology to prevent and mitigate radioactive releases at SRP is by no means exhausted. In this regard, we further recommend that the full level 3 PRA be completed on an expedited schedule, but not necessarily prior to restart.

8. SAFETY ANALYSIS

The Safety Analysis subcommittee reviewed analyses performed by SRP to ensure an adequate margin of safety during normal and anticipated transient conditions and to show that engineered safety features will mitigate the consequences of postulated accidents. Excellent cooperation was received from the Du Pont personnel contacted in the course of the review. The scope of the review was essentially that of a SAR chapter 15, except that the LOCA analysis, which is currently being upgraded, could not be reviewed in final form.

The SRP procedures require for each core charge a systematic analysis of a set of transients and accidents that could challenge fuel design limits. Other analyses are routinely made on a generic basis to verify aspects of the design less sensitive to fuel parameter changes. Results of these analyses are used to set operating limits in the form of operator guidance and trip points.

The subcommittee concluded that in general such analyses are made by qualified people and are independently reviewed before release. It found, however, that some aspects of SRP's current practice could be deemed non-conservative or could otherwise be improved to provide greater assurance of safety. It also noted that safety analysis source documentation was sometimes difficult to retrieve. The subcommittee's findings in relation to the review criteria are summarized below. Recommended corrective measures are presented in Section III.

Loss-of-Cooling Accident Analysis--The LOCA analysis methodology is being upgraded by SRP at this time. A program of experiments is under way to determine an appropriate basis for setting limits to prevent damage from early flow instability (FI) following a large-area pipe break. Other tests and analyses are addressing limits to ensure adequate ECS flow to all fuel channels during the recovery phase. Close coordination between the engineering and development organizations should ensure that the results obtained are fully relevant to the SRP core materials and geometries and will support a suitably conservative analysis model. The concerns relative to development of such a model are discussed in Section II.9.

Non-Loss-of-Cooling Accidents--The present K Reactor restart program calls for a joint Du Pont-Westinghouse review of startup accident scenarios for comparison with commercial industry practice. Other non-LOCA accidents are not included in the scope of that review. The subcommittee did not find assurance that all such accidents are bounded by the presently documented set. For example, the rapid drop of a part length control rod because of the mechanical failure of its drive mechanism could cause a change in reactivity larger than those analyzed (criterion 2B).

Current analyses of the LOPA do not consider the buoyancy effects which might cause deviation from the circulation patterns predicted under low ECS-injection flow conditions. If this effect were to result in upward flow in some channels, the recovery procedures based on this analysis could be misleading (criteria 2D, 4).

Because simulation models that are realistic or 'best-estimate' in character are used, it is necessary to be sure that nonconservatisms when discovered are compensated for with specific allowances. In contrast to this principle, it was noted that some non-LOCA events are analyzed for flow instability using an uncertainty allowance less conservative than that recently adopted for the LOCA. Also, the basis for the burnout risk (BOR) limit in current use was developed for an earlier and different fuel design. It is appropriate that such assumptions and models be verified for use, even though events other than those in question are known to control the operating limits for the charge (criterion 2B).

Overpressure Transients--The subcommittee was unable to find that limits to prevent over-pressure in the tank (creating a lifting force on the inlet plenum) have been conservatively evaluated. A similar observation was made by another subcommittee (see Section II.2). It is noted here that events that might challenge the design of the relief paths and the plenum-anchoring system also include steam generation in the process tubes as a result of power-flow mismatch (criterion 2A).

Documentation--Descriptions of the analyses that support operating limits for the production reactors are contained in internal reports rather than in the SAR. Some limits are supported by generic analyses and others by charge-specific calculations. This practice, at best, complicates the task of management oversight and independent review, and thus could detract from the processes aimed at sustaining a high level of safety assurance.

The preliminary version of an SAR that meets NRC's format and content requirements has been completed as a first step in improving this practice. New technical specifications meeting the latest industry standards are being written. The review found, however, that there is no formal system to trace the applicable generic and specific analyses upon which the safety limits are founded (criterion 4).

9. POWER LIMIT AND ACCIDENT PROPAGATION

Loss-of-Cooling Accident and Leak Before Break--The operating power level must be established on the basis of the most limiting design-basis event. In establishing this level, a spectrum of flow and reactivity transients must be considered.

Historically, the DEGB has been a design-basis accident for the SRP reactors. It was established as such in the early years of reactor development, prior to the development and application of leak-before-break (LBB) technology. Leak before break means that if system components were to develop a crack, crack growth, rather than propagating rapidly to the point of gross failure, would be slow and would result in penetration of the coolant boundary, producing a slow leak. The slow leak would be detectable and provide adequate warning for an orderly reactor shutdown, to be followed by repair or replacement.

Increased knowledge of reactor materials and failure mechanisms and the development of sensitive leak-detection and warning systems have made the DEGB a decreasingly plausible event, even for high-energy cooling systems such as those of PWRs. The NRC has approved LBB as a basis for eliminating jet-impingement barriers and pipe-whip restraints in 39 LWRs.

In the case of the Clinch River Breeder Reactor Plant (CRBRP), a case pertinent to the SRP reactors, the NRC, in accepting LBB as a basis for establishing the design-basis leak for the primary coolant system, accepted a pressure of about 200 lbf/in² (gage) and a coolant temperature below saturation (even at atmospheric pressure), thus classifying the primary coolant system as a moderate energy system. The material was stainless steel, and a sensitive leak-detection system was available for early identification of leaks. The CRBRP satisfied all requirements for its construction permit, and the NRC had issued a safety evaluation report, NUREG-0968 (NRC 1983), prior to project cancellation. Based on piping integrity, fracture-mechanics material behavior, preservice and in-service inspections, and a sensitive leak-detection system, CRBRP was not required to analyze a DEGB as a design-basis accident.

The Savannah River conditions pertinent to LBB are very similar to the CRBRP conditions. The primary coolant system is a low-to-moderate energy system. Its material is ductile and tough and subject to low stresses and considerably lower temperatures than CRBRP. There is a low thermal- and mechanical-fatigue duty. Highly sensitive leak-monitoring systems are available based on the detection of tritium in the heavy water. A thorough inspection program is being implemented prior to restart and an ISI program has been defined. One significant difference is that the Savannah River reactors are subject to IGSCC. However, an evaluation of the impact of IGSCC on LBB shows that while it increases the probability of a leak, it does not invalidate the basic principle of LBB that a small leak will develop and be detected long before a crack could propagate to the point of gross failure. On the positive side, the

Savannah River reactors have demonstrated LBB during the course of their operation, including demonstration of a highly sensitive leak-detection system.

The subcommittee finds the arguments for LBB in the Savannah River reactors to be persuasive, and concludes that a smaller leak than the DEGB is appropriate as the design-basis leak. The limiting failure of a bellows, resulting in a large leak from a 55-in² opening, appears to be a rational choice. This leak should be analyzed using conservative assumptions typical of design-basis accident analyses.

Power Limit--The consideration of LBB and the selection of a 55-in² opening for the design-basis leak results in a very low probability of a leak larger than the design-basis leak. Nevertheless, the spectrum of leaks up to the DEGB should be considered and analyzed in the context of the PRA. These analyses should use realistic data and modeling. Such leaks beyond the design basis normally would not be considered in establishing operating constraints. However, it is recognized that the LBB position is still under review. Until the LBB position has been accepted, it is considered prudent to establish a power level such that core coolability would be expected even for a DEGB, based on analyses using realistic data and modeling.

It was not the intent of the subcommittee to define an operating power level. However, reviews of previous and ongoing work, along with some independent assessment (described below), lead the subcommittee to believe that a practical power level on the order of 50% is achievable as a minimum.

The evaluation on very large leaks, up to and including the DEGB, requires consideration of two critical times during the event:

- Power-to-flow mismatch during early depressurization, referred to as the FI phase
- The ECS equilibrium phase.

During the first few seconds of a leak, a mismatch in power-to-flow can occur, depending on the assumed coolant-pipe break location, leading to bulk boiling, flow reversal, fuel dryout, and overheating (generally referred to as FI). Until flow recovery can be demonstrated, the early power-to-flow mismatch concern can be eliminated altogether by limiting the power to 50% of the nominal power rating on the basis that the flow falls to 60% of nominal full flow. This power level will not lead to bulk-boiling conditions, a prerequisite for the onset of FI.

During the equilibrium ECS phase of the accident, the downward flow in the process assemblies is largely dominated by gravity and is complicated by possible gas entrainment. Furthermore, flow distribution among assemblies as well as among channels and subchannels within each assembly can vary substantially. Available information indicates that the assembly flow during the ECS phase will be at least 20 gal/min and will be split almost evenly among the three principal coolant channels.

Fortunately, a technically defensible power limit of practical interest can be established by recognizing that the controlling mechanism and associated power limit are closely tied to the highly conductive fuel material; i.e., a detailed knowledge of the flow distribution within a coolant annulus is not required. Even in the worst-case coolant distribution among subchannels, the maximum temperature in the fuel at full power remains below the fuel melting temperature. The maximum fuel temperature remains at about 350°C; i.e., well below the fuel-failure threshold, which we assume to be in the vicinity of 450°C and, based on fission-product retention, well below the melting point of ca. 630°C.

In summary, the subcommittee is optimistic that a practical power level of 50% or more can be established using current data and analytic capabilities. The assessment for both LOCA and non-LOCA events is as follows:

Event	Evaluation basis	Expectation on allowable power
Design-basis leak	Conservative	Near 100%
Leak beyond design basis	Realistic	>50%
Non-LOCA flow and reactivity transients	Conservative	60% to 80%

Forthcoming prototypic experiments are reasonably likely to demonstrate the acceptability of higher powers, even approaching 100%.

Accident Propagation--The possibility of a local fault, such as an inlet blockage of a process assembly and subsequent fuel meltdown leading to a whole-core accident, is of fundamental importance to the overall safety assessment of SRP reactors. A sudden and relatively large inlet blockage is believed to be a credible event only during startup of the reactor, while a slowly developing blockage could conceivably occur during normal operation. Since both flow and temperature are monitored in each process assembly, such an occurrence would lead to reactor shutdown. In the case of a complete inlet blockage, decay heat alone would be capable of voiding the assembly, an occurrence that would be followed by overheating, fuel meltdown, and fuel relocation.

An examination of the behavior of the metal fuel material within the assembly, following the postulated flow blockage in the inlet region of the assembly, emphasizes the important role played by fission gas in metal fuel dynamics. Fuel overheating would lead to rapid evolution of matrix fission gas once the fuel melting point was exceeded, resulting in radial expansion of the fuel melt. The concentric-ring design of the Mark 22 fuel assembly (Mk22) would cause the expanding fuel to accumulate on the inner and outer surfaces of the outer and inner target material rings, respectively.

The fuel would freeze rapidly because of the relatively cold target, then remelt, meeting the target material and mixing with it while draining to the

bottom of the assembly. Consideration of these processes suggests that substantial mixing of the fuel and the target material will take place as a result of swelling or foaming of the fuel upon melting; i.e., the fuel would not separate from the target material as the fuel meltdown process takes place. Consequently, any significant reactivity addition or the occurrence of recriticality in connection with fuel meltdown and relocation can probably be ruled out.

The potential for fuel relocation within the incident assembly as well as outside the assembly in the moderator space depends largely on the power level. At decay power levels, the refreezing of the draining fuel/target material would prevent this material from advancing very far below the melting zone and, since refreezing would occur in considerably less time than fuel heating and subsequent fuel melting, frozen fuel/target buildup would occur. That is, the draining rate of melted fuel/target material at decay power would be so slow compared to the rate at which it would refreeze that the potential for a completely refrozen fuel/target blockage of the assembly channels would be high. Moreover, owing to the high thermal conductivity of the fuel/target material, the frozen block of fuel/target material subject to decay heating would be coolable inside the process tube by the surrounding heavy-water moderator. It follows that whole-core involvement would not occur as a result of the inlet flow blockage and subsequent meltdown process.

However, if the power level is assumed to remain near full power during the meltdown process, sustained fuel/target draining would seem inevitable and would result in the relocation of most of the assembly fuel/target material to the bottom of the reactor tank, where it would undergo thermal interactions, breakup, and quenching. While the potential would exist for transferring the fuel/target material to the active moderator region, thereby possibly adding reactivity, the time scale for such a postulated scenario would be well beyond the anticipated reactor scram time. Since the negative reactivity associated with reactor shutdown would be more than enough to counteract the most pessimistic configuration associated with fuel relocation (even assuming separation between fuel and target during meltdown), the subcommittee concludes that a whole-core event can be ruled out.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

III. Recommended Action Items

The recommendations in this section, with the exception of the final two, stem from the subcommittee activities. However, all have been reviewed by the whole committee and represent its consensus. They are listed in Table 3 in order of the subcommittee responsible, according to the numerical code given at the beginning of Section II. The YES identifies those recommended for implementation prior to startup of the first reactor. All others are to be implemented as part of an aggressive overall reactor safety improvement program and before a substantial portion of the remaining operational lifetime has elapsed.

Table 3. Westinghouse Independent Safety Review
Summary Listing of Recommendations. (sheet 1 of 3)

Recommendation number	Subcommittee responsible	Prior to startup	Summary description
1	1	YES	ECS Actuation Following LOPA
2	1	YES	ECS Actuation Procedures
3	1		ECS Performance Testing
4	1	YES	LOCA Performance Testing
5	1	YES	Moderator Recovery System
6	1	YES	Pump Degradation
7	1	YES	Sump Water Removal Capability
8	1	YES	Valve Inspection
9	2		CWS Fracture Mechanics
10	2		Dynamic Analysis
11	2		Fuel and Tank Assembly Analysis
12	2		Fuel Handling
13	2		Gas Plenum Over Pressurization
14	2		Long-term Seismic
15	2		Process System Inspections
16	2		PWS Distillation System
17	2		Shutdown After Seismic Event

**Table 3. Westinghouse Independent Safety Review
Summary Listing of Recommendations. (sheet 2 of 3)**

Recommendation number	Subcommittee responsible	Prior to startup	Summary description
18	3	YES	Batteries and UPS
19	3	YES	Essential Core Monitoring
20	3		REMACS Displays
21	3	YES	Spurious Controls Operation
22	4		Fire Protection Program
23	5	YES	Core Evaluation Responsibility
24	5	YES	Fuel/Target Manufacturing
25	5		Refueling Operations
26	5	YES	Safety Margin Evaluation
27	5	YES	Startup Core Testing
28	6		Configuration Control
29	6	YES	Control Room Information
30	6		Event-Reporting Criteria
31	6	YES	Operational Assessment
32	6		Operator Knowledge Requirement
33	6	YES	Plant Site Organization
34	7		Confinement Performance
35	7	YES	Confinement Exhaust Fan Design Review
36	7		Improved Reactor Room Spray
37	7	YES	Improved Training and Procedures
38	7	YES	LOPA Event Frequency
39	7	YES	Procedural Guidance
40	7		Root Cause Analysis
41	8		Application of FI to Non-LOCA
42	8		Basis for Dryout Calculation
43	8		Core Charge Calculations

**Table 3. Westinghouse Independent Safety Review
Summary Listing of Recommendations. (sheet 3 of 3)**

Recommendation number	Subcommittee responsible	Prior to startup	Summary description
44	8		LOPA ECS Flow Requirement
45	8	YES	Part Length Rod Drop
46	8		Safety Documentation
47	9	YES	Basis for Power Level
48	9		LOCA Experimental Program
49	WISR	YES	Assimilation of Massive Change
50	WISR		Striving for Excellence

1. Recommended prior to startup

ECS Actuation Following LOPA

Investigate automatic actuation of ECS following a LOPA. Any implementation should preclude spurious ECS injection and should include evaluation of whether procedural changes in the short term will suffice while design and implementation proceeds on the hardware. Consideration may also be given to tripping the circulation pumps, which would considerably slow down the flooding rate.

Justification

ECS Actuation Following LOPA

A large break in the cooling water system can flood out the main alternating current (AC) motors in the 105 Building in 1.1 min, with the loss of the direct current (DC) motors in a further 1.6 min. Core melt would not occur for another few minutes, but the operator must identify the event and initiate incident action (single switch) in a very short period, thus bringing on ECS. He/she is instructed to do so only after confirming the following alarms: (1) reactor scram; (2) high motor room sump level; (3) high pump room sump level; and either (4a) reactor plenum low pressure or (4b) loss of circulation. Furthermore, if ECS is actuated while the AC motors are not running, there will be a spill of valuable D₂O and a release of the tritium contained in it (see recommendation Gas Plenum Overpressurization). The committee felt that the operator is asked to evaluate many things in a short time during a very stressful period, with potentially serious consequences from misjudgment.

2. Recommended prior to startup

ECS Actuation Procedures

Prioritize the limits that the operator is instructed to monitor while throttling ECS. These include assembly maximum temperature, ECS minimum and maximum flow rates, and sump level. Verify the acceptability of existing throttling limits. Instruct the operator not to isolate a loop until such action on an intact loop is acceptable and recoverable, or provide qualified instrumentation to ensure his/her ability to make the right choice.

Justification

ECS Actuation Procedures

Once ECS is placed in operation, the operator is asked to throttle it to avoid flooding of the DC or sump pump motors to the point where they become inoperable. Existing procedures ask that he/she protect three limits while throttling: (1) assembly effluent temperature; (2) ECS minimum and maximum flow; and (3) sump level. It is possible that under some circumstances the limits could be mutually exclusive, and some conflicting information was found on recommended flow rates for ECS. The operator is also asked to identify and isolate the broken loop to avoid aggravation of the sump flooding. Available information includes sump conditions, closed-circuit television (CCTV) monitors, and field inspection. This is limited information and could result in the isolation of an unbroken loop, which would in turn exacerbate the problem of cooling the reactor core.

3. Recommended long term

ECS Performance Testing

The analysis code used to convert test data to performance input employed in LOCA and LOPA safety analyses should be reviewed and agreed upon between the operations and support functions at SRP to achieve an independent verification. Once verified, the code should be kept under formal configuration control. The analysis techniques should take into account all relevant test measurement uncertainties, pump-developed head margins, and CWS header pressure margin. An expansion of the cases tested should include flow through the individual valves to ensure that both open fully.

Justification

ECS Performance Testing

Complete end-to-end testing of flow delivery by the ECS is not feasible because of the economic loss of diluting the heavy-water moderator. The system is tested about every two years through a diverter temporarily installed downstream of the individual line isolation and check valves, the flow going to the CWS effluent header. The analytical techniques, treatment of uncertainties and measurement errors, and combination of conditions chosen for testing all merit reexamination, as the results are used in the LOCA and LOPA safety analyses. These analyses are in turn reflected

directly in the plant operating limits. The analytical codes are self-developed and not benchmarked to industry standards, nor is it clear that all relevant errors and uncertainties are included.

4. Recommended prior to startup

LOCA Performance Testing

In the upcoming L Reactor test series, two additional configurations are recommended to simulate certain bounding cases needed in the safety analyses: four of six Bingham pumps operating, with one ECS loop spilling back to the tank and one isolated; and four of six pumps operating, with two lines spilling back to the tank.

Justification

LOCA Performance Testing

The bulk of the cooling flow following a LOCA is due to continued circulation by the main PWS Bingham pumps. Actual delivery to the fuel elements depends on a number of variables, some of which are determined in actual testing in a reactor system temporarily dedicated to the purpose. An upcoming test series in the L Reactor provides an opportunity to cover some additional combinations of assumptions relevant to certain assumed cases used in accident analyses.

5. Recommended prior to startup

Moderator Recovery System

The MRS should have the capacity to handle the maximum PWS leakage that would be expected following an earthquake. Sufficient power and a water source in the event of flow bypass will also be required.

Justification

Moderator Recovery System

This system has a role in mitigation because the ECS is not fully qualified seismically. Also, some PWS leaks may not flow to the sumps, so that a means of providing water other than the sump inventory is needed.

6. Recommended prior to startup

Pump Degradation

The ECS, CWS, and sump pumps should be monitored and/or tested periodically for flow degradation; minimum acceptance criteria should be established and the pumps overhauled if necessary.

Justification

Pump Degradation

The L Reactor booster pump has degraded over time by more than 10%, without a readily available explanation.

7. Recommended prior to startup

Sump Water Removal Capability

Provide sump pump capacity at least equal to that portion of the unthrottled ECS flow that spills to the -40-ft level during a LOCA, considering credible break sizes. Provide seismically survivable CWRSS capacity to a level consistent with expected flooding rates from the earthquake effects, and demonstrate survival of the discharge piping. Some means of ensuring sufficient power will also be needed. Reduce vulnerability to blockage through the provision of trash screens, and verify that sufficient dam louver flow capability exists to prevent early motor room flood-up. For the long term, increase capacity to accommodate single failures without operator action. Replace sump pumps to improve reliability.

Justification

Sump Water Removal Capability

The ability to remove water from the -40 ft level of the 105 Building is critical to LOCA and seismic events. The committee concurs with the ongoing efforts to ensure survivable sump pump capacity greater than the ECS flow to the sump during a LOCA. For the purposes of this recommendation, the assumed break size could be that identified as credible from PWS inspections and mechanical analyses (e.g., LBB). The evaluation need not include single-failure capability in the CWRSS, as ECS throttling is a potential backup action in the short term. Some portion of the CWRSS capability should be qualified seismically as well. There also appears to be a vulnerability to debris blockage, and there is concern over the possibility of differential flooding.

8. Recommended prior to startup

Valve Inspection

A minimum list of valves that should be inspected physically has been provided to K Reactor operations; a program should be put into place to identify others that might be key to safety as well.

Justification

Valve Inspection

The surveillance and test programs are selective and prescribe functional testing only for certain components. Valve maintenance and visual inspection of internals are generally not performed, and many valves in key lines have not been inspected since installation. A comprehensive inspection program should be put into place in the longer term to confirm the structural and functional capability of key valves. The valves covered are to be chosen for the importance of their function to safety or the consequences of their failure.

9. Recommended long term

CWS Fracture Mechanics

Perform fracture mechanics analysis of CWS and ECS considering operation with circulating water near 40°F. An alternative would be to find an operating mode that precludes such conditions, such as recirculation via pumps.

Justification

CWS Fracture Mechanics

The CWS and ECS fracture toughness at 40°F [nil-ductility transition temperature (NDTT) of the material] is available from the SRP test program and, as reported in terms of J_{Ic} , is relatively high. However, there is no formal documentation of the material's adequacy giving its toughness and the pipe loads.

10. Recommended long term

Dynamic Analysis

Identify systems for which dynamic methods have been used for seismic analysis of safety systems, and reassess for conservatism. First attention should be paid to the process water, cooling water, supplementary shut-down, and moderator makeup systems. Then all safety systems should be re-reviewed.

Justification

Dynamic Analysis

There is a concern that the methods used for spectrum modal analysis are potentially nonconservative.

11. Recommended long term

Fuel and Tank Assembly Analysis

Perform seismic and structural analyses of the process assemblies, thermal shield, and reactor tank. A tank fracture mechanics analysis should be performed using the latest fracture toughness data.

Justification

Fuel and Tank Assembly Analysis

A satisfactory stress analysis was not found for the process assemblies and tank assembly, including the thermal shield. This analysis should include combinations of seismic loads, thermal stresses, fatigues, and operating loads, and should consider other effects such as that of irradiation on the fracture toughness of the tank.

12. Recommended long term

Fuel Handling

Identify consequences of seismic events during fuel handling or on fuel-handling equipment, and evaluate for necessary action. The analysis should

include consideration of the forest above the reactor and possible damage in the disassembly area.

Justification

Fuel Handling

This concern has to do with releases or consequential effects of seismic events while handling fuel or when the fuel-handling equipment is in a vulnerable position.

13. Recommended long term

Gas Plenum Overpressurization

Determine the effects of overpressurization of the gas plenum from full ECS injection when the gas plenum becomes solid with water. Failure of the roll anchors is a particular concern. Determine uplift of the plenum and stress in the plenum inlet nozzles. Determine whether the plenum seal will rupture from overpressure and plenum uplift.

Justification

Gas Plenum Overpressurization

ECS injection when the PWS is full and the AC pump motors are not running, as might occur following a LOCA when the broken line is isolated, would cause an overpressurization of the gas plenum and an upward force on the top shield and D₂O plenum. The upward force is transmitted through the plenum inlet nozzles to the roll anchors, which serve to react the upward force on the plenum. If the roll anchors fail, the plenum would lift and stretch the plenum seal. Vertical motion of the plenum is limited to about 0.5 in. by the holddown beams. This motion would probably not cause the plenum seal to rupture, but should the seal rupture, it would provide additional pressure relief to protect other components. The roll anchors (K Reactor), plenum inlet nozzles, and plenum seal have apparently not been analyzed for overpressure of the gas plenum. However, preliminary analysis indicates that the roll anchor bolts and plenum seal are adequate for the anticipated lifting pressure. Other possible cases should be considered as well, such as LOPA events similar to the above or more severe accident cases in which the source of overpressure is steaming. (These might be set up as hypothetical reactivity accidents or as an aggravated LOPA with a degraded ECS.)

14. Recommended long term

Long-Term Seismic

Review and seismically qualify the emergency cooling and confinement systems. Modify maintenance and surveillance practices as indicated by this review. Check and qualify all safety system supports.

Justification

Long-Term Seismic

Seismic qualification and review of maintenance and surveillance practices of the emergency cooling and confinement systems will improve defense in depth.

15. Recommended long term

Process System Inspections

Develop indication acceptance criteria using American Society of Mechanical Engineers (ASME) Section XI (ASME 1986) as a guide. Develop in-service inspection plans for any portions of the CWS, ECS, CWRSS, SSS, and PWS (including the tank) that have not already been considered. Identify sensitized areas in PWS, ECS, and CWRSS. Identify and monitor sensitized areas such as weldments and flame-washed areas. Review adequacy of current ISI program related to supports. Check supports and anchors associated with automatic backup shutdown, reactor room spray (RRS), blanket gas, supplementary relief, and pressure and vacuum relief systems.

Justification

Process System Inspection

These recommendations provide enhancements to the current nondestructive examination (NDE) program, as well as additional assurance that the supports are installed as intended.

16. Recommended long term

PWS Distillation System

Develop emergency procedures for plant evacuation and post-shutdown instrument monitoring for seismic events impacting this system.

Justification

PWS Distillation System

The distillation system outside confinement is not seismically qualified and contains a substantial tritium inventory.

17. Recommended long term

Shutdown After Seismic Event

Ensure that enough safety rods can be inserted after a seismic event to maintain the plant in a safe-shutdown condition. Show that the control rod action following an earthquake below the threshold for SSS triggering is satisfactory from an accident analysis standpoint.

Justification

Shutdown After Seismic Event

Although the SSS (Ink) will shut the reactor down after a design-basis seismic event, greater assurance of long-term shutdown would be provided

by an ability to insert some or all of the safety rods. This insertion need not be rapid, as in the case of a scram. Thus the requirement will be that the permanent distortions and displacements not entirely preclude such insertions. For seismic events below the triggering threshold of the SSS, rods will be needed with acceptable scram delay times. The analyses should take into account the low structural damping and relatively high elevation of the forest.

18. Recommended prior to startup

Batteries and UPS

Complete performance tests and intercell resistance checks per Institute of Electrical and Electronics Engineers (IEEE) Standard 450 (IEEE 1987) for the following:

- 108 Building 125v station battery
- 105 Building control rod equipment room battery
- General Motors (GM) diesel generator (DG) start battery
- REMACS batteries and uninterruptible power supply (UPS)
- Confinement exhaust fan emergency generator start and control batteries.

In the longer term, review and upgrade maintenance procedures for all lead acid, nickel-cadmium, and nonstandard batteries.

Justification

Batteries and UPS

Procedures for inspection and maintenance of batteries and UPS systems do not meet current industry standards. A failed battery might escape notice.

19. Recommended prior to startup

Essential Core Monitoring

Provide redundant seismically and environmentally qualified methods of monitoring certain essential parameters. A suggested list includes neutron flux or alternative means of verifying shutdown; reactor tank level; process water pump motor speed or alternative means of verifying circulation; and sump water level. Evidence that the reactor is subcritical and that decay-heat removal is continuing must be available following any credible fire or flooding event. Procedures for reading the instruments should be incorporated into operator training and into site emergency planning.

Justification

Essential Core Monitoring

Seismic damage or fire in the control room or along cable runs has the potential to destroy the capability to monitor the condition of the core. Such capability is essential to ensure maintenance of core cooling.

20. Recommended long term

REMACS Displays

Add to the REMACS software the ability to provide six additional cathode ray tube (CRT) displays. This will provide the following:

- Summary of state or condition of the critical safety functions
- Display for each showing the appropriate systems and equipment available to the operator to restore the function.

Justification

REMACS Displays

The interface for control of the plant using REMACS is significantly different from the control board to which the operators are normally accustomed. Under the stressful conditions expected should its use be necessary, improvement in user friendliness is desirable.

21. Recommended prior to startup

Spurious Controls Operation

Show that spurious operation of PWS valves will not occur from a seismic event or credible fire, or show that such a condition is tolerable or recoverable. Include consideration of relay chatter. In the longer term, show that ECS will not be actuated by a fire or seismic event, or show that a safe recovery can be accomplished.

Justification

Spurious Controls Operation

Spurious operation of ECS or PWS valves because of relay chatter during a seismic event or a fire could lead to conditions not now considered in documentation available to the committee.

22. Recommended long term

Fire Protection Program

Prepare fire protection surveillance and operational requirements, perform a formalized fire protection overview program (including area hazards analyses and fire design-basis studies), and install rapid detection and suppression systems where appropriate. The current plan to install a standpipe and a new water source prior to startup is an excellent move. Use of the stairwells for required emergency access should also be reviewed.

Justification

Fire Protection Program

The prevention record at SRP has been excellent because of Du Pont management attention to control of combustibles and employee awareness training. However, there are some inherent problems because of the vintage of building designs and the unavoidable presence of materials such as lubrication oils and cable insulation.

23. Recommended prior to startup

Core Evaluation Responsibility

The responsibility to conclude that core safety evaluations are complete and reflect current plant conditions, and to defend these evaluations, should reside with Reactor Operations. The necessary interface agreements should be put into place with the laboratory support group.

Justification

Core Evaluation Responsibility

Reliance on another organization to understand and defend the analyses that set operating limits will contribute to a lack of responsibility in the analytical group closest to operations. The laboratory is a valuable resource for methods development and computations and can provide career growth opportunities for its personnel. However, the responsibility to understand and defend the core charge analyses should reside in the Reactor Operations organization.

24. Recommended prior to startup

Fuel/Target Manufacturing

Manufacturing deviations from nominal should be accounted for in the core charge safety analyses and reflected in the operating limits. The factors used to account for these deviations must recognize the potential for fuel and/or targets to have undetected characteristics outside of specified ranges.

Justification

Fuel/Target Manufacturing

The long successful history of production using the Mk22 fuel assembly could be upset by variations in manufacturing. Allowance for deviations needs to be reexamined with each charge, and the applicable safety analyses should recognize the potential for fuel and targets to be outside specifications. The recent changes in ^{235}U enrichment, in feed material source, and in testing should be thoroughly evaluated for their potential impact on core parameters.

25. Recommended long term

Refueling Operations

Install an annunciator or other means of allowing the crane operator to receive immediate indication that a refueling step has violated a criticality safety criterion.

Justification

Refueling Operations

The refueling procedures present a possible challenge to safe shutdown of the reactor: the shutdown margin is 3%, there is no interlock between cranes and flux detectors, the crane operator does not have access to flux monitoring information, and successive communication links are involved between

the crane operator, the control room operator, and manual scram using the SSS.

26. Recommended prior to startup

Safety Margin Evaluation

Non-LOCA as well as LOCA analyses need to be examined for conservatism and factors applied to the resulting limits as appropriate.

Justification

Safety Margin Evaluation

The core operational limits are set from accident and transient analyses using best-estimate input in some cases, rather than allowing for tolerances, actual equipment performance, and methods uncertainties. Pending the long-term update of the entire analysis system (see Safety Documentation recommendation), an interim procedure is required.

27. Recommended prior to startup

Startup Core Testing

Prepare and execute a plan for reactor restart that includes tests for parameters such as power distributions, scram shutdown rates, and temperature coefficients.

Justification

Startup Core Testing

The experimental basis for a number of the core parameters used in the limit-setting analyses could be improved relatively easily by performing certain tests during the reactor startup program.

28. Recommended long term

Configuration Control

Identify essential drawings. Essential drawings are those required for the safe operation of the reactor. Put them under configuration control, along with design analyses, calculations, computer codes, and other information supporting the process of setting operating limits and technical specifications and standards. Provide a system for the control of the location of essential drawings, the incorporation of changes in a timely fashion, retrieval, and integration into operating procedures. Develop a work control system that links the plant configuration with the drawing system and its change control procedures. Institute the necessary Quality Assurance (QA) system to meet the requirements of NQA-1 (ANSI/ASME 1986).

Justification

Configuration Control

There is insufficient assurance that the plant configuration is correctly represented in the information available to the operations, maintenance, engineering, and other personnel who need this information to perform their

duties safely. The process of controlling changes to plant configuration and its associated paper does not meet current DOE or NRC standards.

29. Recommended prior to startup

Control Room Information

Controlled, as-configured, P&ID, and electrical single-line diagrams should be placed and used in the control room. Logic diagrams are also desirable in the longer term. There also needs to be a formal method of maintaining current status between drawing revisions. Identify safety-related electrical, instrumentation, and control circuits on these drawings. The following systems at least should be covered: process water, cooling water, emergency cooling, contaminated water removal and storage, safety rods, control rods, supplementary safety, leak detection, shutdown monitoring instrumentation, emergency power, primary reactor shutdown, radiation protection instrumentation, and automatic backup shutdown. Develop a set of critical safety-function status trees to link plant instrumentation with symptom-based procedures for the most critical safety functions. The following should be included: subcriticality, core cooling, heat sink, confinement, and PWS inventory. In the longer term, link the status trees to symptom-based procedures and identify by tagging or marking the safety-related electrical, instrumentation, and control components, including sensors and transmitters, in the reactor plant.

Justification

Control Room Information

The committee's review concluded that information available to the operators and supervisors in the control room is insufficient if they are to understand the evolution of off-normal occurrences and use their understanding to guide actions rather than simply follow procedures. Lack of separation and seismic and environmental qualification shifts the burden of defense in depth to the control room staff. Their understanding of plant condition and potential threats to safety functions is essential to following alternative paths available for event mitigation. Critical safety-function status trees and symptom-based procedures are a proven method for aiding the operator in choosing his/her actions. The SRP operations history leads the committee to believe that inappropriate operator interaction in plant abnormalities can be a significant contributor to risk.

30. Recommended long term

Event-Reporting Criteria

Threshold criteria for reporting of abnormal events to DOE need to be better defined to the operations staff. Negotiate with DOE for a time period longer than the 15 min now allowed before making the decision to report an event.

Justification

Event-Reporting Criteria

The current instructions are so general that the only correct course of action, in the view of the operators, may be to report anything that occurs, no matter how trivial. Such a procedure leads to overload and gridlock, resulting in ignoring or glossing over the items that really do warrant reporting. The NRC regulations (10 CFR 50.72 [NRC 1988a]) allow up to one hour to review and determine the reportability of an event, which would be more appropriate than the 15 min specified by DOE.

31. Recommended prior to startup

Operational Assessment

The operations management should perform an operational assessment, including drills, prior to restart. This assessment involves personal verification of the state of readiness of the operating staff and is in addition to the formal readiness review checkoff.

Justification

Operational Assessment

The current operations staff-upgrading efforts are a major step in the right direction. It is recommended that the operations management perform an effectiveness assessment prior to startup. The questions to be addressed include the following:

- Adequacy of readiness review
- Whether operations staff have sufficient understanding of the reasons underlying necessary actions
- Whether forced draft additional training recently undergone has been retained
- Whether individuals are capable of operating in the new environment.

32. Recommended long term

Operator Knowledge Requirement

Establish definitive goals for level and depth of operator knowledge. Improve emergency preparedness training and drill for radiological events. Establish entry-level requirements for operations trainees to meet American Nuclear Society (ANS), medical, and psychological screening standards. Require a two-year scientific degree or proven success in a rigorous program such as naval or NRC-licensed reactors. On-shift and operations management should interview and select candidates. Establish separate job progressions, titles, and pay scales for reactor operations commensurate with the level of responsibility. Consider the establishment of a centralized training group for all functions in support of reactor operations that will be a part of the accreditation effort. Modify the senior reactor operator certification program to permit hands-on training, including reactivity changes.

Justification

Operator Knowledge Requirement

The entry-level operations position requires only a high school diploma at SRP. The operators' job grades are low on the overall scale, and the positions are not highly regarded compared to crafts positions. This situation, combined with the current status of training programs, results in not meeting DOE or ANS standards. The selection of personnel appears to be left up to Human Resources. High attrition may occur, so that the recommendations made here may be looked upon as an opportunity to perform a considerable upgrade.

33. Recommended prior to startup

Plant Site Organization

The key functions necessary for reactor operations should either report directly to the Reactor Site Operations Manager, or be tied closely enough that he/she can control their allegiance, daily schedule, and assignment to his/her organization. These functions include training, maintenance, power operators, diesel engine maintenance, reactor technology, cognizant engineers, and work control in addition to his/her own plant operating staff.

Justification

Plant Site Organization

The Reactor Site Operations Manager (or operations management directly responsible for the reactors) must have control of the resources necessary for operations and have clear lines of authority over those resources. This control/authority is required by his/her total responsibility for operations. Such an organization does not preclude people also having an administrative home in parent organizations that can look to peer review and career growth issues. Representatives of the necessary oversight organizations will, of course, remain independent of reactor operations.

34. Recommended long term

Confinement Performance

Demonstrate by analysis that there is a high degree of confidence that the confinement will provide sufficient holdup and removal of radioactivity so that the plant can be shown to meet the overall DOE safety goals. These evaluations must rely on realistic, mechanistic calculations and test data and include the relevant systems [AACS, RRS, CHRS, and magazine index assembler (MIA)].

Justification

Confinement Performance

The confinement system must perform its function in mitigating accident consequences to meet the overall DOE draft safety goals (DOE 1989) for risk to the general public and to the work force at SRP.

35. Recommended prior to startup

Confinement Exhaust Fan Design Review

Review the design of the AACS exhaust fans and demonstrate their operability in a postulated severe-accident environment.

Justification

Confinement Exhaust Fan Design Review

Proper operation of the AACS exhaust fans is critical to maintaining the filter temperatures at appropriate levels. Failure of fan cooling could lead to filter failure and significant release from confinement. Since the operating environment of the fans following an accident is expected to be more severe than the normal operating environment, the fan design should be reviewed to demonstrate that the fans will continue to operate in severe circumstances.

36. Recommended long term

Improved Reactor Room Spray

Reevaluate the need for this upgrade.

Justification

Improved Reactor Room Spray

The committee's opinion is that this upgrade may be ineffective in reducing severe accident releases. Analyses show that the present RRSS is capable of keeping the air/stream mixture in the inlet to the AACS at acceptable temperatures. Furthermore increased flow will not affect the noble gases, and reductions in iodine are expected to be limited by the high turnover rate of the air. The CHRSS also plays a long-term role in maintaining the viability of the filters.

37. Recommended prior to startup

Improved Training and Procedures

Provide updated procedures, and train the operators accordingly, for break isolation, manual ECS initiation, rotovalve closure in the LOPA case, CHRSS and RRS actuation, and CWRSS termination at the appropriate time in a severe accident.

Justification

Improved Training and Procedures

The preliminary PRA has shown that the plant response to hypothetical severe accidents is highly dependent on operator actions. The probabilities assigned to successful outcomes can be improved considerably through improvements in procedures and assurance that the operators can perform successfully.

38. Recommended prior to startup

LOPA Event Frequency

Institute a visual inspection and surveillance program to ensure the integrity of the CWS piping. The piping of concern is that which could lead to the process water pumps' flooding and subsequent failure to provide circulation.

Justification

LOPA Event Frequency

The preliminary PRA results indicate that plant safety, as measured by core-damage frequency, is highly dependent on the frequency assigned to LOPA. A LOPA results from simultaneous failure of all PWS Bingham pumps, a common-mode event. The primary cause of such a failure has been identified as a large break of the CWS with subsequent flooding and failure of the process water pumps. The PRA considered a range of frequencies for this event from $1 \text{ E-}03$ to $1 \text{ E-}04$ with results indicating that over 70% of the core damage frequency is related to the LOPA event when using the frequency at the high end of the range. The judgment, based on comparisons with comparable PWR systems, is that the frequency at the low end of the range is correct. To ensure the correctness of this judgement, it is recommended that a cooling water pipe inspection and surveillance program be instituted to ensure the integrity of the cooling water pipes located where such a leak could lead to a PWS pump flooding event.

39. Recommended prior to startup

Procedural Guidance

Provide increased surveillance testing at quarterly intervals where possible for the CWRSS, ECS injection lines, and the automatic incident actuation (AIA) relays and breakers. Reexamine allowable out-of-service times for AIA, CHRS, RRSS, CWRSS, and MIA. The Level 1 PRA effort under way at SRP and subcontracting organizations should be pursued vigorously to bring to light other recommendations of this type. In the long term, it should be completed through full-scope and the associated severe-accident analyses and supporting experiments. The onsite emergency plan should be reviewed to ensure adequate protection for SRP personnel in the event of a severe accident.

Justification

Procedural Guidance

The PRA analysis has identified a number of areas where overall risk can be reduced through increased surveillance testing, changes in out-of-service time allowances, and clarification of operating procedures. In the longer term, a full-scope PRA and supporting severe-accident information will allow assessment of the efficacy of accident consequence mitigation systems and of the achievement of the overall DOE safety goals.

40. Recommended long term

Root Cause Analysis

Institute a formalized system that performs an engineering analysis searching for root causes of individual failures and trends in failure types. Feedback to plant maintenance would be required. Closeout would require that recommendations to avoid similar instances in the future be made, tracked, and completed.

Justification

Root Cause Analysis

High reliability of safety-related systems is critical to plant safety. Component failures in safety systems lead to system degradation and failure, and compromise plant safety. Therefore, as components fail, the root causes of failure should be determined to identify potential component design deficiencies and/or related procedural deficiencies, to identify potential common-cause failure modes, and to alert appropriate personnel to these vulnerabilities. This information should be used in a program to sensitize plant maintenance to such vulnerabilities and also to modify procedures and/or designs to resolve the problems. This program would reduce repeat failure modes in like components and also reduce system vulnerability to common-cause failures.

41. Recommended long term

Application of FI to Non-LOCA

Upgrade non-LOCA analyses where necessary to incorporate the current LOCA technology in the FI regime.

Justification

Application of FI to Non-LOCA

Recent developments in LOCA analysis have shown that the FI limit predicated on simple channel models may be nonconservative for the Mk22 fuel assembly. Since this phenomenon applies to some non-LOCA cases, these cases should be reexamined in light of this information.

42. Recommended long term

Basis for Dryout Calculation

Assess the dryout correlation used to derive the BOR core limit and verify its applicability to current fuel, or confirm that the FI limit is always bounding.

Justification

Basis for Dryout Calculation

The BOR limit, which is used to ensure avoidance of dryout during various design transients, is based on a correlation developed for an older, different fuel design. The committee is concerned that it may be inappropriate. Also, it may be superseded by the FI limit.

43. Recommended long term

Core Charge Calculations

Require that a formal checklist be prepared by those responsible for the generic analysis to document the applicability of generic analyses not performed specifically for that charge. The responsible operations group will then perform the charge-specific analysis.

Justification

Core Charge Calculations

Generic design and safety analyses are performed by SRL and referenced by the charge designer, Reactor Technology (RT), in establishing the operational and safety limits for that charge. Routine charge designs are documented internally and reviewed, but applicability is difficult to trace. The committee is concerned that this documentation practice may not support independent review and audit.

44. Recommended long term

LOPA ECS Flow Requirement

The SRP should provide an analysis that ensures that fuel assembly flow stagnation or boiling will not occur during the LOPA once-through cooling mode.

Justification

LOPA ECS Flow Requirement

Following a loss of all PWS circulation, the fuel is cooled in a once-through mode by ECS flow to the plenum, through the fuel, and exiting the reactor vessel vent paths. The ECS flow can range from 10,000 to 15,000 gal/min depending on the assumed single failure and can be reduced to 4,500 to 8,000 gal/min by operator action. Also, backflow paths through the main loop piping could significantly diminish fuel assembly flow. At these low flow rates, it appears that the buoyancy of heated water in a fuel assembly may be comparable to the driving head developed for forced downward flow through the assembly. This situation could result in flow stagnation, boiling, or upflow through some assemblies.

45. Recommended prior to startup

Part Length Rod Drop

Provide an analysis of the reactor transient resulting from the rapid drop of a part length rod from the highest worth position.

Justification

Part Length Rod Drop

The rapid drop of a part length control rod appears to be credible from a mechanical standpoint and is not an accident analyzed for a core charged with Mk22 elements.

46. Recommended long term

Safety Documentation

The preparation of a SAR and accompanying technical specifications meeting current commercial reactor standards should be committed to and pursued vigorously. The completion plan and commitment of resources are needed in the short term, although the completion of this effort will be long term. New technical specifications will require a major effort to revise the operating procedures. These specifications should include mechanisms for procedure revision, waiver, and periodic review and update. Events selected as evaluation bases should be categorized according to their expected frequency of occurrence.

Justification

Safety Documentation

Current nuclear industry standards requiring a SAR based on analyses of record and using benchmarked methods under a quality controlled system are not in place, nor are the operating limits or technical specifications based on a SAR. Efforts to date to prepare such a SAR and technical specifications have identified the magnitude of the task involved.

47. Recommended prior to startup

Basis for Power Level

A design-basis leak should be established on the basis of LBB technology and used with appropriate conservatism to establish a short-term operating power limit. Until the LBB review has been completed and accepted, this allowed power level should also be established in such a way that avoiding the meltdown of a major fraction of the core would be expected even for the hypothetical DEGB, based on analyses using best-estimate data and modeling. The power level specification should also be consistent with a conservative evaluation of the design-basis leak and non-LOCA flow and reactivity transients.

Justification

Basis for Power Level

The LBB is applicable to the PWS because of the ductile and tough material of its boundary, the low energy available to expand openings, and the sensitive leak-detection capability. A conservative design-basis leak is a bellows failure, resulting in a 55-in² opening. Larger leaks are highly improbable and should be addressed in the context of the PRA, using best-estimate data and models.

48. Recommended long term

LOCA Experimental Program

Following a large-break LOCA, there would be early depressurization and a power-to-flow mismatch. The safe power level should be determined on the basis of two-phase cooling during this flow transient and should not be

limited to onset of significant voiding (OSV) consideration alone. The analytical and experimental program should emphasize the flow excursion and subsequent ability of the two-phase flow to remove heat, in addition to just addressing its onset. In the following ECS "equilibrium" phase, the success criteria should allow for significant local overheating (up to 430°C while requiring enough assembly flow to ensure a reasonable channel flow and removal of heat as sensible heat only. Near-term as well as future experiments and analyses addressing the ECS equilibrium phase should be examined to ensure proper prototypicality and reflect actual experience with postdischarge cooling of Mark 18 (Mk18) assemblies.

Justification

LOCA Experimental Program

Prior to being shut down in August 1988, the operating power level of the SRP reactors had been reduced in stages from 100% to about 50% as a result of concerns about ensuring reactor coolability following a postulated large-break LOCA in the PWS. These reductions were based largely on a success criterion of avoiding the onset of significant boiling and FI. The sudden large-break LOCA has a low probability of occurrence because of the toughness and ductility of the system boundary material, the low system pressure available to expand openings, and the enhanced leak detection capability enabled by the tritium levels in the coolant. Thus this approach appears overly conservative, because the success criterion is also quite conservative. The program of experiment and analysis that is needed to allow a proper understanding of the phenomena should allow for the two-phase heat removal capability following the flow excursion, including the possibility of stable dryout and fuel overheating. The beneficial effect of the high thermal conductivity should also be included.

49. Recommended prior to startup

Assimilation of Massive Change

Top DOE and contractor management must make sure that the massive changes being incorporated currently in hardware, in standards for conduct of operations, and in DOE and the contractor organization are assimilated and understood by the organization and fully reflected in the procedures, training, and performance of the operations staff, so that the excellent overall safety record is not jeopardized.

Justification

Assimilation of Massive Change

For many years the operations at SRP have been successful from a production standpoint, and the overall safety record is excellent. Nonetheless, the standards for design and operations that were valid at the time of startup have been surpassed in naval and commercial reactor practice. The organization has set about a massive upgrading of standards with a generous

measure of goodwill and determination, but many of its members remain to be convinced of the necessity for all the change. The loss of Du Pont is also felt keenly by many of the people. While the contractor transition is being accomplished along with the upgrading of standards for hardware and conduct of operations, it is essential to convince the organization that it is headed in the right direction and to generate in its people enthusiastic participation in the process. Furthermore, it is vital that the changes in hardware and software be correctly reflected in the procedures and that the staff be thoroughly trained in these new procedures after the change process has settled down. Otherwise the changes could become counterproductive and the operations more prone to error than before.

50. Recommended long term

Striving for Excellence

The reactor operations organization, and others at SRP who support it, must share with DOE and contractor management a clearly articulated commitment to a continuous striving for greater excellence in nuclear safety, accompanied by a rising standard of professionalism in operations.

Justification

Striving for Excellence

Following on the related recommendation, Assimilation of Massive Change, the SRP reactor operations and supporting functions must share with DOE and contractor management a strong desire to achieve excellence in nuclear safety through continuous striving for improvement. Among the elements involved in addition to hardware upgrades are infusion of personal desire to become better trained and more professional; management visibility, discipline, and support; and constant searching for ways to do things better. This process will be a long-term one, and will never, in fact, be completed. That it is being achieved will be evidenced in a record of accomplishment; in the attitude of the people as they express themselves to reviewers, visitors, and each other; and through peer reviews by other organizations, such as INPO.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

APPENDIX A: Westinghouse Independent Safety Review Committee Charter and Meetings

The WISR was commissioned by Mr. James S. Moore, President, Westinghouse Savannah River Company (WSRC), on November 1, 1988, in response to a request from the DOE. A similar review (WHC 1987) had been performed by Westinghouse personnel on the Hanford N Reactor prior to Westinghouse's assumption of responsibility at the DOE's Hanford Site. Dr. W. Howard Arnold, who had been a member of the N Reactor review team, was asked to chair the WISR committee. As in the case of the N Reactor review, Westinghouse was asked by DOE to draw heavily on people experienced with a broad range of reactors, particularly commercial power reactors. Special emphasis was to be placed on familiarity with current practice in codes, standards, and conduct of operations. This review was to be performed under the transition contract, DE-AC09-88SR18035.

Dr. Arnold met with Mr. Moore and several members of his senior management at Savannah River on November 2 to choose the committee members, agree on a charter and scope of review, and schedule the activities. The committee members are listed on the title page of this report, with biographical information included in this appendix. The charter is stated below. The schedule was intended to parallel the transition of the Savannah River operations contract from Du Pont to Westinghouse so that committee conclusions would be due April 1, 1989. It was recognized that the recommendations would be available only in summary form on that date, to allow for review and publication time for the final committee report. Since the reactor startup date was not known at the time, the committee was asked to review on the basis either of recommending continuation of operations on April 1, or of reviewing readiness for operation if the reactors were not actually in operation. The final report was specifically requested by DOE to have concurrence and endorsement by the Westinghouse Executive Vice President, Utility Systems, Mr. Theodore Stern.

The first full committee meeting was held at SRP November 15-17, 1988. All members were present, along with Mr. Dennis Richardson who has been secretary and coordinator, and Mr. Thomas Gorrell of Du Pont who has acted as liaison with the Du Pont organization. At that meeting a number of subcommittees were formed whose membership and summary reports are contained in the other nine appendices. In addition, a number of status presentations were provided by Du Pont personnel.

Subsequent full committee meetings were held as follows: December 6-9 at SRP, December 20-22 at the Westinghouse Energy Center in Pittsburgh, January 10-12 (SRP), January 24-26 (Pittsburgh), February 7-9 (SRP), February 21-23 (Pittsburgh), and March 7-9 (SRP). At the final committee meeting in Pittsburgh on March 21, the findings and conclusions were presented to Mr. Stern. In addition, individual committee members and subcommittees and their members have had numerous meetings, visits, and briefings at both sites.

The following statement of objectives was agreed upon with DOE at the time of formation of the committee:

"Westinghouse Electric Corporation proposes to perform an independent nuclear safety review and assessment of the SRP reactors as a basis for, and condition of, the operating management contract changeover to its wholly owned subsidiary, the Westinghouse Savannah River Company, on April 1, 1989.

"The purpose of this review and assessment is to determine and make recommendations to DOE-SR:

- Whether and which of the three SRP reactors (PKL) are sufficiently safe for immediate continued operation.
- Or, lacking such determination, what specific remedial actions are necessary as a condition of continued safe operation.
- And, in either case, what further specific actions are appropriate for the near future, but concurrent with continued safe operations."

A further scope statement was also provided as follows:

"The Westinghouse independent review and assessment will consider SRP reactors status and safety adequacy with regard to [the following]:

- Findings and recommendations of the NAS Defense Production Reactors Safety Review dated October 1, 1987.
- Findings and recommendations of the DOE SRP Reactors Technical Safety Review dated August 1986.
- Findings and recommendations arising from the SRP integrated Safety Evaluations and SAR and Technical Specification Upgrade programs.
- Additional issues or concerns referred by DOE-SR for consideration, and
- Any other issues or concerns which may arise during the course of the review insofar as these findings, issues, concerns, or recommendations relate to either a design or operations capability to:
 - Shut down the reactor and maintain it in a safe shutdown condition, or
 - Prevent or mitigate the consequences of accidents which could result in potential off-site exposures comparable to those referred to in 10CFR100.11[sic]."

BIOGRAPHICAL INFORMATION

W. H. ARNOLD, CHAIRMAN

Dr. Arnold is Vice President, Engineering and Development Divisions, Westinghouse Hanford Company. Included in his management responsibilities are operation of the Fast Flux Test Facility (FFTF) reactor and direction of engineering and projects for the Hanford Site. Prior to this assignment, he had been General Manager of the Westinghouse Advanced Energy Systems Division since 1981, where he was responsible for Westinghouse efforts in advanced reactor design and development and production reactor support efforts for DOE. In the 1970s, he was responsible for engineering design, safety analysis, project implementation, and international support of the Westinghouse PWR business (1970-72, Engineering Manager, PWR Systems Division; 1972-79, General Manager, PWR Systems Division; 1979-80, President, Westinghouse Nuclear International). He joined Westinghouse in 1955 after receiving his AB from Cornell University and his PhD in physics from Princeton University. He worked for his first six years with Westinghouse on core physics and safety analysis of commercial power reactors, including Yankee Rowe, BR-3, SAXTON, SELNI, SENA, and CVTR, and the associated critical experiments. He spent another six years with the NERVA nuclear rocket program including responsibility for reactor testing at the Nevada Test Site and two years in the Westinghouse Underseas Division before rejoining the PWR business as Engineering Manager in 1970. He is a fellow of the American Nuclear Society and the American Association for the Advancement of Science and a registered professional engineer in Pennsylvania. He was elected to the National Academy of Engineering in 1974.

D. W. CALL

Mr. Call is Manager, Safety Department, WSRC, responsible for site-wide independent oversight of Savannah River safety practices and activities. He is a physics graduate from the Carnegie Institute of Technology, now Carnegie-Mellon University, and has 30 years of direct nuclear safety experience including National Aeronautics and Space Administration (NASA), commercial nuclear power, and DOE production reactor projects, programs, and services. He joined Westinghouse in 1959 at Westinghouse Astronuclear Laboratory as part of the successful proposal effort for the NERVA nuclear rocket project. He worked on that project for 12 years, primarily in the areas of shielding and core design, nuclear excursion, and radiological and hazards analysis. He then transferred to the Westinghouse Pressurized Water Reactor Systems Division in 1971 and spent 17 years in virtually all aspects of commercial nuclear power safety and licensing activities. In 1988 he was on a special assignment to the Westinghouse Hanford Company with responsibility for safety analyses, SAR, and technical specifications activities associated with the N Reactor restart effort.

H. K. FAUSKE

Dr. Fauske is President, Fauske & Associates, Inc., a wholly owned subsidiary of Westinghouse Electric Corporation. Since leaving Argonne National Laboratory in 1980, where he served as the first director of the Fast Reactor Safety Technology Management Center and was responsible for the planning and management of the DOE program, he has been involved in projects involving a wide range of safety issues. He served as a senior consultant to the Industry Degraded Core Rulemaking program (IDCOR), sponsored by the Atomic Industrial Forum and as a senior technical advisor to the CRBRP, and provided overall technical direction of the American Institute of Chemical Engineers Design Institute for Emergency Relief Systems. He also participated in DOE design review teams for the Hanford N Reactor (1986), Savannah River Reactors (1987), and the Westinghouse Independent Safety Assessment of N Reactor (1987), and is currently a member of the Westinghouse Safety and Environmental Oversight Committee. Dr. Fauske is a Fellow of the American Nuclear Society and the American Institute of Chemical Engineers. In 1975 he became the first person in the field of reactor technology to receive the University of Chicago Medal for Distinguished Performance at Argonne National Laboratory, and in 1982 he became the third recipient of the "Tommy" Thompson Award, the highest honor the American Nuclear Society gives in the field of reactor safety. He received his DSc from the Norwegian Institute of Technology in 1963.

W. D. LEGGETT

Dr. Leggett is manager of Nuclear Engineering at the Westinghouse Hanford Company. His management responsibilities include reactor physics and core safety analysis for the FFTF and N Reactor, PRA, and thermal hydraulic analyses of Hanford facilities. Prior to this assignment, he had been Systems Engineering manager for the Basalt Waste Isolation Project and manager of Nuclear Engineering in the Westinghouse Nuclear Fuel Division. Dr. Leggett joined Westinghouse in 1963 and shortly thereafter received his PhD in nuclear engineering from North Carolina State University. From 1983 to 1986, Dr. Leggett was a director of the American Nuclear Society.

N. J. LIPARULO

Mr. Liparulo is manager of Risk Management and Operations Improvement in the Westinghouse Nuclear and Advanced Technology Division of the Energy Systems Business Unit. He joined Westinghouse in September 1972 as an engineer in the Safety Analysis group and worked for over 16 years in the nuclear safety analysis and licensing areas. In 1981 Mr. Liparulo became manager of the Severe Accident Analysis group where he directed all aspects of the analysis of degraded-core accidents. In 1985, after a one-year assignment as manager of Programmed Regulatory Compliance, he assumed his present position as manager of the Risk Management and Operations Improvement section

(formerly Risk Assessment Technology). In his current position, he is responsible for all the risk management, system analysis, severe-accident analysis, containment analysis, boiling-water reactor (BWR) transient analysis, and severe accident testing efforts in the Energy Systems Business Unit. Mr. Liparulo's duties include developing technology and supporting all commercial applications, both nuclear and non-nuclear, of risk assessment technology. Mr. Liparulo received a BS in 1971 and an MS in 1974, both in chemical engineering, from the University of Pittsburgh.

J. D. McADOO

Mr. McAdoo is Assistant Manager, Nuclear Safety Department, Nuclear and Advanced Technology Division of Westinghouse. In this capacity he is responsible for development and control of software to support safety-related design and analysis for commercial nuclear projects. He also directs and coordinates strategic programs for the nuclear safety product lines. In the 1970s, he held positions of management responsibility for fluid systems engineering, safety, licensing, and QA functions during which time he was influential in developing and gaining regulatory acceptance of standardized safety system designs for PWRs. He received a BS in chemical engineering from Carnegie Institute of Technology in 1951. He joined Westinghouse's Commercial Atomic Power Division after spending five years with Vitro Corporation in nuclear process development.

W. J. McSHANE

Mr. McShane recently retired as manager of the Engineering Department, Westinghouse Hanford Company. His department was responsible for a number of engineering functions site wide, including drafting, stress analysis, and configuration management. He also furnished specialized engineering services to all of the divisions and departments of the company. He joined Westinghouse in 1948 after graduating from Carnegie Institute of Technology and started his nuclear career at the Bettis Atomic Power Laboratory in 1949. He held a number of management positions including chief test engineer at Portsmouth Naval Shipyard and manager of Submarine Plant Engineering. He was active in development of the FFTF from 1968. He was the engineering manager of that facility during construction and throughout the acceptance test program. He assumed his position as Engineering Manager in 1981.

L. E. STRAWBRIDGE

Mr. Strawbridge is Deputy Manager, New Production Reactor Programs at Westinghouse Advanced Energy Systems, a department of the Nuclear and Advanced Technology Division. Prior to this assignment, he was Manager, Defense Materials and Liquid Metal Reactor Programs, with responsibility for development and support of production reactors at Savannah River and the

Hanford Site and the design and development of liquid-metal reactors for commercial utility applications. Since graduating from MIT with an MS in nuclear engineering in 1959, he has had 30 years of experience in the design and development of nuclear reactors, including PWRs, HWRs, and several advanced reactor concepts. He was manager of Nuclear Design for FFTF and manager of Safety and Licensing for the CRBRP. This experience included extensive interactions with the NRC and the Advisory Committee on Reactor Safeguards and participation in public hearings as an expert witness. He is a member of the Westinghouse Nuclear Safety Review Committee, a consultant to the University of Chicago, and a member of the Safety Subcommittee of the Technical Review Committee for the Integral Fast Reactor. He participated in the Westinghouse independent review of the N Reactor. He is a professional engineer, registered in the Commonwealth of Pennsylvania.

G. TOTO

Mr. Toto, staff assistant to the Senior Nuclear Vice President, Tennessee Valley Authority, is a Westinghouse manager loaned to the TVA to help in the recovery and restart of its nuclear program. In 1986, Mr. Toto was selected by Admiral Steve White, Tennessee Valley Authority manager of Nuclear Power, to be the site director of Watts Bar Nuclear Station. He led the effort to resolve technical and personnel issues, helping to establish employee trust in management so that the station could meet required standards. Mr. Toto played a key role in the startup of the Sequoyah Nuclear Station. He served as a key member of a special eight-person team reporting to Admiral White on the readiness of the plant and personnel to restart and operate the plant safely, efficiently, and properly. Prior to his selection as site director, Mr. Toto was responsible for field efforts both as a product line manager and as an engineering manager for the repair and servicing of reactor plants. Mr. Toto was the Westinghouse Project Manager for the C Tank characterization and repair effort at SRP. He came to the Westinghouse Water Reactor Divisions in 1979, after 23 years of technical and management experience at Bettis Atomic Power Laboratory, where he had been responsible for Bettis Naval Reactor efforts in nuclear shipyards. These responsibilities included selecting and training personnel to provide technical direction to shipyard management in the design, testing, operation, refueling, and maintenance of more than 150 reactors. Mr. Toto began his nuclear career at Bettis in the design and analysis of the Nautilus Power Plant after graduation from the University of Pennsylvania with a BS in electrical engineering in 1953. He is a registered professional engineer in Ohio and Pennsylvania.

D. C. RICHARDSON, SECRETARY

Mr. Richardson is manager of the Safety Analysis and Risk Management Department in the Westinghouse Savannah River Company. In this capacity he is responsible for managing the risk and safety analysis of all facilities, including reactors, at the SRP. Prior to this assignment, he had managed the Risk

Assessment Technology Organization in the Nuclear and Advanced Technology Division of Westinghouse, Pittsburgh. In the 1970s, he held positions of management responsibility in Reactor Protection Analysis and PRA. He also spent 10 years in control and protection system design for high-temperature gas-cooled and PWR commercial plant designs. He received a BS and MS in Aerospace Engineering from Pennsylvania State University (1963/1965), an MS in mathematics from San Diego State University in 1970, and an MBA from the University of Pittsburgh in 1980. He joined Westinghouse in 1972 after nine years with General Dynamics Corporation.

APPENDIX B: Subcommittee Reports

APPENDIX B.1: MECHANICAL SYSTEMS

Marshall W. Young, Manager, Fluid Systems Department,
Westinghouse Hanford Company

Larry E. Conway, Engineer, System Engineering Department,
Westinghouse Nuclear and Advanced Technology Division

Robert D. Magee, Engineer, System Engineering Department,
Westinghouse Nuclear and Advanced Technology Division

B.1.1 SCOPE

We assessed the functional adequacy of those systems and operations that are relied on to provide safe shutdown and long-term cooling following normal and anticipated operating occurrences and to mitigate postulated accidents (criteria 1, 2). The review included design documentation and procedures for operation and maintenance, as well as control and distribution of this information. The adequacy of power supply and instrumentation for monitoring and control of the systems was reviewed by a separate task group (see Appendix B.3), as was the performance of systems under severe-accident conditions exceeding the intended design capability (see Appendix B.7).

The mechanical systems were reviewed against the four criteria in Section I. In several respects, we found insufficient assurance that the mitigation systems would meet the criterion of reliability. Several of our recommendations based on this finding are included in Section III. The subcommittee feels that implementation of these recommendations and completion of already planned restart tasks would support a favorable assessment of safety.

The design and operating procedures for the ECS rely on operators to assess correctly events that may require intervention (e.g., to initiate ECS manually or to isolate a cooling loop from the reactor tank). By contrast, commercial nuclear plant philosophy tends to avoid the necessity of similar intervention, particularly under unusual or stressful situations and where the risk attending either a mistaken intervention or a failure to intervene is substantial. We find this contrast to be troublesome when viewed together with the control room issues (see Appendix B.6) (i.e., training and qualification of supervisory personnel, access to information, and the clarity and symptom orientation of procedures).

Specific comments and recommendations are included below at points where we believe further analysis, training, or procedure changes are justified to reduce the risk of an operator error. This general concern should be addressed as an integral element of an ongoing safety management upgrade.

B.1.2 OPERATOR RESPONSE FOLLOWING A LOSS-OF-PUMPING ACCIDENT

Maintaining current limits of the existing design requires prompt operator action to prevent loss of circulation to the reactor following a design-basis LOPA. This event assumes a large break in the CWS resulting in rapid flooding of the 105 Building. Once the water level reaches 18 in., the Bingham Pump AC motors flood, and at 35 in. the DC motors flood. Accident mitigation requires the operator to initiate emergency cooling prior to flooding of the DC motors. Existing calculations estimate the AC and DC motors flooding at 1.1 and 2.7 min, respectively. Therefore, the operator must identify the event and then initiate incident action (single switch) within 2.7 min. This manual action results in ECS injection and ensures cooling flow to the assemblies.

The operator is instructed to implement incident action only after confirming the following alarms: (1) reactor scram, (2) high motor room sump level, (3) high pump room sump level, and either (4a) reactor plenum low pressure or (4b) loss of circulation. Adding to the delay of diagnosing the event is the fact that, depending on break location, the alarms for "Reactor Scram" and "Reactor Plenum Low Pressure" might not occur until flooding of the AC motors. As such, the necessary combination of alarms required to initiate incident action might not be satisfied until after the AC motors are flooded. Such a situation leaves a relatively short period of time (1.6 min) between loss of the AC motors and loss of the DC motors during which the operator must confirm that the combination of alarms exists and actuate the ECS.

It is noted that although ECS is required to prevent fuel damage following a LOPA, its actuation would result in loss of D₂O inventory and may result in excessive plenum lifting forces (see Appendix B.2). Although ECS actuation is necessary, we note that its actuation will likely have long-term implications. This possibility could cause an operator to second-guess his action or delay incident action as long as possible in hopes of isolating the leak before the DC motors fail.

B.1.2.1 Findings

It is likely that the operator will be asked to evaluate multiple sources of information during a very stressful period, and in a very short time, to make a decision with long-term implications. It is the opinion of this subcommittee that the available time to perform this action is too short to ensure a high probability of success (see Appendix B.7).

B.1.2.2 Recommendation

We therefore recommend that, to ensure timely actuation of the ECS following a design-basis LOPA, an automatic system be studied. This system must be designed to preclude spurious ECS injection whenever the AC motors

are tripped. Prior to startup, this issue could perhaps be addressed in another fashion (e.g., tripping the CWS pumps or procedural changes) (see recommendation ECS Actuation Following LOPA).

B.1.3 PROCEDURES

Our review of several key reactor incident procedures identified concerns about ECS throttling, isolation of process water leaks, and general format.

B.1.3.1 Emergency Cooling System Throttling

To prevent flooding of the sump pumps and DC motors, the ECS, after being actuated, may have to be throttled to match the water-removal capacity. Procedures identify three limits that should be protected while throttling: (1) assembly effluent temperature, (2) ECS minimum and maximum flow, and (3) sump level. However, it is possible that these three limits could be mutually exclusive, and the procedures provide no priority. A second concern associated with throttling is the flow limits identified. In one place, the procedure requires that total ECS flow be throttled to 8,000 to 9,000 gal/min. In another, it specifies that total ECS flow be throttled down to 4,500 to 5,000 gal/min. Our review was unable to identify a basis for these limits. These flow rates should be verified to provide adequate cooling.

B.1.3.2 Process Water Leak Isolation

To avoid flooding the DC motors following a process system break, procedures instruct the operator to attempt to locate and isolate the break. Isolation is also desirable to minimize transfer of water to the disposal basin. Information available for evaluating leak location includes sump conditions, CCTVs, and field inspection.

In general these diagnostic techniques are limited. The risk is that the operator could isolate the wrong process loop, which would result in a further reduction in assembly flow. No analysis evaluating the impact of one loop spilling and one line being isolated was identified.

In summary, the operator has inadequate information and guidance to identify leak location with a high degree of accuracy. We feel that it is not prudent to chance isolating the wrong loop, which would, in turn, further degrade the plant condition.

B.1.3.3 Findings

In the opinion of the subcommittee, significant benefits would be gained from a comprehensive review and rewrite of existing procedures. The procedures reviewed were difficult and time-consuming to follow and lacked adequate

contingency planning. In addition, the basis for several of the limits could not be located (e.g., ECS flow-throttling limits).

B.1.3.4 Recommendations

The following short-term recommendations (see recommendation ECS Actuation Procedures) are provided to correct issues associated with the existing procedures:

- Prioritize the various limits that the operator is instructed to monitor while throttling ECS. These include assembly maximum temperature, ECS minimum and maximum flow rate, and sump level. Operators should have available adequate guidance in case these limits conflict.
- Verify the acceptability of existing throttling limits.
- Instruct the operator not to isolate until isolation of an intact loop is acceptable and recoverable, or provide qualified instrumentation that will ensure his/her ability to identify the location of a process water break and ensure isolation of the correct loop.

B.1.4 SURVEILLANCE/MAINTENANCE PROGRAM

The plant currently has implemented a surveillance and test program. In general, component testing included in the program is selective, particularly for functional testing.

B.1.4.1 Findings

Valve maintenance, which includes visual inspection of the internals, generally is not performed. Some valves located in key lines have not been inspected since installation. In addition, even functional tests that are performed may not necessarily attest to the structural integrity of the component (primarily the valve internals).

B.1.4.2 Recommendations

This subcommittee believes that the age of the plants warrants a comprehensive inspection program to confirm the structural and functional capability of key components (see recommendation Valve Inspection), whose selection should be based on their importance to safety and on previous testing or maintenance. Importance to safety considers the consequences of a valve that is failing to perform its safety function and the extent to which a failure within its internals could impact the safety function of the system. For example, a given valve may not perform any safety function; however, if its disk corroded and dislodged, flow blockage might result. It is possible that such a situation might go undetected

until the time when the system might be called upon to perform its safety function. We have provided to SRP a list of the valves that we believe should be inspected.

B.1.4.3 Finding

A second surveillance testing issue involves observed degradation in the L Reactor booster pump head flow curve. Available data indicated that this pump has degraded in excess of 10% over recent time. An analysis should be performed to evaluate the cause of this degradation and determine the acceptability of the flow.

B.1.4.4 Recommendation

A surveillance program should be implemented to monitor all ECS, cooling water, and sump pumps for flow degradation. If similar degradation is noted in K Reactor, the pump should be overhauled prior to startup (see recommendation Pump Degradation).

B.1.5 EMERGENCY COOLING SYSTEM PERFORMANCE TESTING

B.1.5.1 Findings

A flow test of the ECS function is performed approximately every two years. This test includes full system flow through the individual injection line valves but does not inject light water into the PWS. The test is accomplished by disconnecting a piping elbow downstream of the valves in each injection line and connecting each elbow to a test line connected to the cooling-water effluent header. System performance is measured for a full spectrum of ECS supply sources (i.e., 1, 2, 3, or 4 lines injecting). Pressure and flow measurements are made to characterize the overall system resistance.

The RTD uses the raw test data to calculate, for most of the ECS source and injecting line combinations, the ECS flow that would actually be delivered to the reactor plenum under accident conditions. This information is then used as the basis for fuel limit calculations for about the next two years until the system is retested. This information is also available to SRL for LOCA and LOPA analyses.

B.1.5.2 Recommendations

The subcommittee's concerns and recommendations relative to the ECS performance tests and use of the data are as follows (see recommendation ECS Performance Testing).

- The conversion of test data into expected ECS-delivered flow is currently performed by a single RTD person using a self-developed computer code. The SRL is independently developing its own analysis code but the RTD was not aware of SRL's analysis methods or results to date. Whichever analysis is finally used, SRL and the RTD should perform an independent review and verification of the test data and resulting calculated ECS delivery. Once verified, the data analysis code should be controlled to prevent code modifications that have not undergone independent review, verification, and sign-off.

- The calculation of ECS flow delivery should include consideration of all test measurement error, pump-developed head margin, and cooling water header pressure margin. Minimum and maximum ECS deliveries should be specified for both LOCA and LOPA mitigation.

- It was stated by the RTD that no evaluation of ECS delivery to the plenum with all five ECS sources currently exists. The RTD, while producing the raw data, did not perform the calculation. This fact was most evident in discussions concerning vessel pressure caused by ECS delivery and venting following a LOPA. The RTD's evaluation of plenum anchor forces was based on the assumption that the maximum ECS flow (maximum vent back pressure) was 1.2 x booster pump delivery. No evidence that this assumption is conservative was provided by the RTD. A single group should be responsible for determining the ECS flow capability. It appears that this group should be the RTD since it performs the system tests and is aware of the specific test instrumentation and instrumentation location. The RTD could then provide SRL with the required ECS flow information needed for fuel operating limits, LOCA, and LOPA analyses.

- The two-year flow test should specifically include a case to measure flow through the individual valves to ensure that both are open fully. (This procedure was done during the last K Area test.)

- A minimally acceptable ECS pump- and booster pump-developed head should be specified. This minimum head (at a specified flow value or a limited flow range) would be used as an acceptance requirement during periodic pump start tests, which are performed on a more frequent basis than the two-year flow test.

B.1.6 LOSS-OF-COOLING-ACCIDENT PERFORMANCE TESTING

Unlike commercial plant designs in which the safety system provides all the core cooling following a large LOCA, the majority of core cooling flow in

the SRP reactors is provided by continued operation of the PWS Bingham pumps taking suction from the reactor vessel. Several tests have been performed to develop a correlation between the water level in the vessel versus flow from the Bingham pumps to the plenum. Another test of this type is to be performed in the near future at L Reactor. We offer comments concerning the upcoming test based on a review of the test authorization (see recommendation LOCA Performance Testing).

A clear objective of this test should be to simulate limiting LOCA conditions and identify limiting fuel assembly flows. We would include the following test conditions for a postulated DEGB.

- Reactor vessel level versus Bingham pump flow should be established with all six pumps in operation. This arrangement would simulate five intact loops in operation with a single loop pumping to the break (already included in the current SRP test plan).

- Minimum plenum levels versus delivered flow and plenum-spill flow versus plenum level are then determined with five of six Bingham pumps in operation with one PWS loop in backflow from the plenum to the reactor vessel. Calculations should ensure that the elevation head from the plenum to the reduced vessel water level is sufficient to provide the anticipated accident plenum-spill flow. Accurate backflow measurement is needed (the current SRP test plan includes this operating mode).

With this information and a correlation of plenum level versus fuel assembly flow, the fuel assembly flows and equilibrium vessel levels versus ECS flow rate can be determined (the SRP test plan will include rotovalve adjustment to simulate loops with and without ECS delivery). If this procedure proves too difficult, Bingham pump flow can be increased to simulate ECS flow with a small increase in reactor vessel (RV) level. However, the simulated ECS flow would be equally distributed in all five injecting loops.

- Another test case that should be demonstrated would have only four of six Bingham pumps operating with one loop spilling back to the reactor vessel and one loop isolated. This case would correspond to the incorrect isolation of an intact loop by the operator or failure of a Bingham pump in loops 2 or 5 with successful automatic closure of the rotovalves (note that five of six Bingham pump flows versus reactor vessel level are needed).

- Also, four of six Bingham pumps operating with two lines spilling back to the reactor vessel should be demonstrated. This case corresponds to the failure of a Bingham pump in loops 1, 3, 4, or 6 where there is not auto-isolation by the rotovalves.

For these two tests, various break/backflow/ECS injection loop orientations would need to be tested to demonstrate areas of minimum plenum level and/or maximum spill and backflow.

In addition, the currently specified test appears to lack sufficient plenum level and fuel assembly flow instrumentation. The instrumentation plan should be reviewed thoroughly.

B.1.7 LOSS-OF-COOLING-ACCIDENT EMERGENCY COOLING SYSTEM FLOW REQUIREMENT

Following a loss of all PWS circulation, the fuel is cooled in a once-through fashion by ECS flowing to the plenum, through the fuel, and exiting the reactor vessel vent paths. For this cooling mode, ECS flow can range from 15,000 to 10,000 gal/min, depending on the assumed single failure, and can be reduced to 8,000 or 4,500 gal/min by operator action. Also, backflow paths through the main loop piping could significantly diminish fuel assembly flow. At these low flow rates, it appears that the buoyancy of heated water in a fuel assembly may be comparable to the driving head developed for forced downward flow through the assembly, which could result in flow stagnation, boiling, and/or up-flow through some assemblies.

Reactor technology personnel interviewed had not analyzed this situation, and our review team did not have the opportunity to discuss this scenario with SRL personnel. It is recommended that SRP provide an analysis to ensure that fuel assembly flow stagnation/boiling cannot occur during the LOPA once-through cooling mode (see recommendation LOPA Flow Requirement).

B.1.8 SUMP CAPABILITY

The ability to remove water from the -40-ft level of 105 Building is critical to respond to a number of design-basis events (e.g., LOCA and seismic). The subcommittee concurs with the ongoing efforts to increase survivable sump pump capacity to at least the ECS flow expected to reach the -40-ft level during a credible LOCA. We believe that this change should be accomplished prior to startup but that it need not include the capability to accommodate single failure in the CWRSS since ECS throttling would be available as a backup in this event. Some portion of the CWRSS capability or some alternate water removal capability should be seismically qualified (see the Appendix B.2 on seismic qualification).

For the long term, the CWRSS should be modified to increase its capability to accommodate a failure of one sump pump. This modification would eliminate the need for the operator to throttle the ECS. The sump pumps should be replaced to improve pump reliability to a level equal to that of industry.

In addition to the above, the subcommittee noted during several plant walkdowns at both P and K Areas that sump removal capability is vulnerable to debris blockage. We recommend the following (see recommendation Sump Water Removal Capability).

- Install 'trash rack' protection for all sump pumps (including MRS) and for the louvers in the dams between pump and motor rooms.
- Show by test or analysis that sufficient dam louver flow capability exists to prevent early motor room flood-up.

B.1.9 SUBCOMMITTEE ACTIVITIES

We visited the SRP sites a number of times to walk down the systems and components included in the review scope and to interview SRP personnel. These activities are summarized below:

Reactor walkdowns:

K Reactor - 12/15/88, 1/18/89, 3/3/89

P Reactor - 2/3/89

L Reactor - 3/6/89

Discussions with SRP Personnel:

Reactor Technology

L. DeWitt - 12/14/88, 2/3/89

J. Hinton - 12/14/88, 1/15/89

T. Monahan - 1/18/89, 2/2/89, 3/6/89

R. Taylor - 1/11/89, 1/13/89, 2/2/89, 3/6/89

Laboratory

J. Church - 1/12/89

J. Smith - 1/12/89

H. Baker - 2/2/89

J. Price - 2/2/89

K. Okula - 2/2/89

Operations

H. Allen - 2/2/89

F. Pulley - 2/1/89.

B.1.10 BIOGRAPHICAL INFORMATION

M. W. YOUNG

Mr. Young, who is manager of Fluid Systems, has been with Westinghouse Hanford Company since April 1972. During this time he has managed a wide variety of engineering organizations at both the section and subdivision levels. These assignments have included not only analysis and design, but procurement, fabrication, installation, construction, and test verification responsibilities as well. His accomplishments include the technical

management of design, development, and fabrication activities on all engineered equipment subcontracts for FFTF, valued at about 90 million dollars. Prior to joining Westinghouse Hanford Company, he was with Aerojet General Corporation for 14 years, where he was manager of Turbopump Design and Development Engineering for nuclear rocket engines. He has a BS in mechanical engineering from the University of California.

L. E. CONWAY

Mr. Conway is a senior engineer with 17 years of experience in fluid systems and nuclear plant design. He graduated from the University of Pittsburgh in 1969 with a BS in chemical engineering. He is currently working in the Nuclear Plant Development Programs group, Nuclear Plant Programs department, located at the Westinghouse Energy Center in Monroeville, PA. For the past seven years, he has been responsible for the design of safety systems for the Westinghouse advanced PWR project. He designed and patented the 'passive' safety system plant concept that formed the basis for the 10-megawatt electric small military power plant, the AP600, and, most recently, the SPWR plant design efforts. He is currently on the AP600 and SPWR design teams with particular responsibility for the development of the passive containment cooling system and safety system feasibility and demonstration testing. He also participated in the recent Westinghouse Independent Safety Review of the Hanford N Reactor.

R. D. MAGEE

Mr. Magee joined Westinghouse in 1980 at the Energy Center in Monroeville, PA. Since then he has held various positions within Fluid Systems Design in the Nuclear and Advanced Technology Division. His most recent position is that of senior engineer in the Safeguards Engineering group. This position includes involvement in a wide variety of fluid systems engineering activities. He is responsible for the design, application, and field support of Westinghouse-supplied systems. These include systems associated with residual heat removal, emergency cooling, primary cooling, containment spray, component cooling, chemical control, and other auxiliary systems. He is a graduate of Michigan State University with a BS in mechanical engineering. In addition, he holds an MS in business administration from the University of Pittsburgh.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

APPENDIX B.2 STRUCTURES, SEISMIC, AND MATERIALS

William S. Lapay, Advisory Engineer, Westinghouse Nuclear and
Advanced Technology Division

Donald S. Griffin, Manager, Energy Systems Engineering, Westinghouse
Nuclear and Advanced Technology Division

Matthew J. Anderson, Manager, Engineering Analysis, Westinghouse
Hanford Company

George S. Bohm, Consulting Engineer, Westinghouse Nuclear and
Advanced Technology Division

Tom R. Mager, Consulting Engineer, Westinghouse Nuclear and
Advanced Technology Division

B.2.1 SCOPE

We reviewed the structures, buildings, equipment, and piping systems considered necessary for safe shutdown of the reactors and for mitigation of potential accident consequences. We emphasized structural integrity and system performance (operability). Our review has focused on the K Reactor; however, the recommendations are applicable to the other reactor sites. Because of the nature of our subcommittee, the review concentrated on design and not on the two major areas of safety influence defined by operations and management. We recognized the as-built condition and not just the design requirements. Recommendations provided are consistent with the safety philosophy and restart criteria of Section I. Defense in depth was used as a measure of safety along with accident prevention and risk avoidance. The key issues identified by the subcommittee stem from criteria 1 or 2, which concern safe shutdown and mitigation systems, respectively.

The objectives of this subcommittee were the following.

- Determine which systems are essential to satisfy the minimum criteria from a structural standpoint.
- Determine the structural condition of the safety systems necessary to permit startup or continued operation.

B.2.2 GENERAL ISSUES

Five systems were identified as key for achieving and maintaining safe shutdown and mitigating the consequences of an accident. They are the PWS, CWS, SSS, REMACS, and CWRSS. It is important to note that three of these have already been considered important to safety and included in the SRP SQUG

seismic walkdown program. This subcommittee considers the CWRSS also to be important to the defense-in-depth philosophy. It is necessary to provide a means of removing within 72 hours, as per SQUG methodology assumptions, water from flooding, to avoid the loss of the sump pumps. Although the subcommittee considers the ECS important, it is not a key system. Therefore, a seismically qualified ECS is considered desirable in the long term. Various confinement systems are also considered important if not key to meeting criteria 1 and 2.

The subcommittee does not consider a large LOCA of the PWS a credible event because the temperature and pressure are low. There is not enough energy to cause a pipe break that would result in a large LOCA. The SRL has completed a program justifying the conclusion that the pipe will leak before it breaks. Therefore, we believe that a seismic event will not cause a LOCA as long as the PWS is itself qualified.

Issues identified by the subcommittee that are already being addressed by the November 1987 K Reactor restart criteria (DOE 1988) are not included in the recommendations. However, it is assumed that those commitments as understood by the subcommittee will be completed and implemented. Those items include the following.

- Resolve the overstress condition of the building structure under the stack. Adequate margin against loss of systems important to safe shutdown must be demonstrated prior to restart, or design modifications must be made. We understand that this position is shared by Du Pont and DOE.

- Resolve with DOE the adequacy of the dynamic model used to generate response spectra and seismic loads for the reactor building, and develop supplementary spectra as needed.

- Meet, as agreed to with DOE, the restart seismic criteria for the K Reactor (considered acceptable by the subcommittee) that define "on an interim basis a means of assuring a level of seismic resistance comparable to that resulting from the application of Regulatory Guides 1.60 and 1.61 (NRC 1973a, 1973b) for structures, pipe, and equipment associated with the Savannah River Plant reactors."

- Ensure that the seismic analyses agreed to with DOE as part of the restart requirements (see item above) are completed.

- Ensure that the modifications identified as needed from the SQUG walkdowns are implemented (e.g., missing bolts replaced, bracing added, damaged items repaired).

- Implement items identified under the PWS Reactor Materials Program.

B.2.3 SPECIFIC SAFETY ISSUES

This section addresses the specific issues identified by the subcommittee in three areas: materials, seismic criteria, and the adequacy of safety systems and structures.

B.2.3.1 Materials

B.2.3.1.1 Inspection. Is the inspection procedure for the PWS adequate?

Du Pont originally procured the austenitic stainless steel to a specification that required solution heat treatment and water quenching. Approximately 6% of the 1,400 circumferential welds in the PWS piping that have been inspected using UT methodology have been found to contain IGSCC indications. This situation is consistent with inspection experience for commercial nuclear power plants in which 5% to 6% of the sensitized welds that have been inspected contain IGSCC indications. Approximately 90% of the indications were less than 50% through the wall with the largest crack depth/pipe thickness ratio being 0.8. Over the life of the SRP reactors to date, only 12 leaking cracks have been reported. The majority of these were discovered in the early to mid-1960s. The SRP established a pipe replacement criterion for IGSCC determined by UT inspection as follows: a pipe segment will be replaced if (1) the IGSCC indications exceed a depth of 50% of the wall or (2) the IGSCC is more than 20% of the circumference. To date, 23 piping segments have been replaced in the PWS. They are replaced with piping fabricated from 304L-grade stainless steel.

The PWS piping system is grade-304 austenitic stainless steel with unspecified carbon content. Weldments in the PWS piping system are likely to be "sensitized." Because oxygen (1 to 2 p/m) is added to the PWS coolant, IGSCC is and will continue to be present. Ultrasonic inspection of the circumferential welds in the PWS piping over the past five years demonstrates that the IGSCC is readily detected and sizes are indicated. However, there are 24 welds (four per loop) deemed inaccessible by current UT methods. Further, each segment of piping in the PWS contains a longitudinal seam. However, only selected areas of the longitudinal welds were polished for in-service inspection. The areas polished were approximately 12 in. on either side of the circumferential welds. Approximately 130 lin ft of longitudinal welds in the L and K Reactors were ultrasonically inspected, and no indications were recorded. The longitudinal seams have not been completely inspected because of a belief that the piping was procured to a specification calling for solution heat treatment followed by water quenching. Evidence suggests that Du Pont waived this requirement at some stage of construction. However, a number of essential performance requirement measurements performed on longitudinal weld seams did not reveal any evidence of sensitization.

Some presence of IGSCC in the PWS piping is considered acceptable. The IGSCC generally grows through the wall (depth) without greatly increasing in length. This phenomenon reduces the probability of rupture prior to a leaking

crack, which should be readily detected. The probability of IGSCC for the SRP PWS is essentially the same as in high-temperature, high-pressure BWR piping systems. With lower temperature and pressure, the IGSCC growth rate should be considerably less than the 10^{-5} in./h used for BWR piping.

It was observed during a walkdown of the K Reactor that brackets were welded to the PWS piping, which resulted in a large number of flame-wash areas. During the past five years, the SRP PWS has undergone ISI. The inspectors have been certified by the Electric Power Research Institute (EPRI) NDE Center as qualified for detection of IGSCC.

We also considered whether it would be necessary to test ultrasonically the reactor vessel prior to startup. As noted in Section B.2.3.3.7, the vessel has been analyzed for structural loads including steady state and seismic. Furthermore, no leaks have occurred in reactor vessels of this design. Section B.2.3.1.3 shows that radiation damage to the vessel is being tracked and that there is adequate residual toughness. Finally, calculations made by the subcommittee indicate that the flow from a 360° through-wall crack in the vessel would be approximately 13,000 gal/min, which is less than the flow expected from a DEGB. Therefore, we concluded that the UT development program for the reactor vessels should be brought to a successful conclusion and made a part of the ISI program for the PWS, but that completion of the vessel inspection prior to startup is not required.

Finding. Since the startup of the SRP PWS, an ISI plan has been in operation. While the ISI did not include ultrasonic examination, nor was the procedure formalized in an approved document, the PWS was inspected after each shutdown. No IGSCC was detected. The procedures for ISI of the PWS are specified in internal SRP documentation.

Recommendation. Du Pont is generating an ISI plan for the SRP reactor PWS. The plan, which is to be in general conformance to ASME Section XI (ASME 1986c), is awaiting final approval. Based on the experience utilizing ASME Section XI methodology in commercial light water systems, the SRP ISI plan should be adequate to detect flaws in the PWS. All areas that have been sensitized should be identified and monitored in the ISI plan (see recommendation Process System Inspections).

B.2.3.1.2 Fracture Toughness of the Secondary Cooling Water and Emergency Cooling (past second valve) Systems. Are the carbon steel secondary cooling and emergency cooling piping sufficiently tough to permit operation at temperatures as low as 40°F?

The SRP secondary CWS provides water to cool the D₂O in the main heat exchangers, to provide for the emergency supply of cooling water (ECS), and for other area uses. The lower bound temperature is 40°F.

The CWS and ECS piping is fabricated from ASTM A285 (ASTM 1982) and ASTM A53 (ASTM 1987b) carbon steel plates. Thus the CWS piping contains longitudinal weld seams in addition to the circumferential ones. Eight

pieces of pipe material and five pieces of weldments from the CWS piping were used to characterize the fracture toughness of the A285 and A53 material.

The Charpy V-notch test results indicate that all the subject materials exhibit an NDTT near 40°F. Static fracture toughness J_{IC} tests at 40°F with the crack oriented in the circumferential direction were quite high, indicating a ductile mode of fracture. Charpy V results exhibited a much reduced shelf energy with the notch oriented in the axial direction indicating a lowering of J_{IC} in that direction. The corresponding J tests were not performed, however.

The integrity of the ECS must be maintained, because it is designed to remove decay heat following reactor shutdown when the normal decay heat removal system is not operable. Interestingly, the most credible mechanism for a LOPA is identified as being a large rupture of the CWS that floods the D2O circulating Bingham pump motors.

Finding. The fracture resistance of the CWS and ECS carbon steel piping may or may not be adequate in the presence of cracks under functional operating loads. The rupture of a large CWS pipe could lead to a loss of primary pumps. Satisfactory fracture mechanics evaluations of the carbon steel CWS and ECS systems are not in evidence.

Recommendation. The fracture toughness, J_{IC} , at 40°F of the CWS and ECS piping should be determined in the axial direction. Failure of the ECS function could lead to inadequate flow in the primary system while CWS pipe rupture could lead to loss of primary pumps by flooding (see recommendation CWS Fracture Mechanics).

B.2.3.1.3 Fracture Toughness with Irradiation. Does the PWS receive irradiation sufficient to product reduction in fracture toughness?

In commercial light water reactors, the fluence of interest for austenitic stainless steel reactor internals exceeds 10^{21} n/cm² (E > 0.1 MeV). The maximum fluence to date in the tank wall of the SRP production reactors is approximately 1×10^{21} (E > 0.1 MeV). It was recognized early in the life of the SRP that irradiation could be a concern. Studies have been performed on the effect of irradiation on the tensile properties of austenitic stainless steel from the tank wall material of a decommissioned tank. Several years ago the SRP embarked on a reactor materials program. The program included PWS tank surveillance capsule(s) that contained specimens from the weld metal, heat-affected zone, and base metal of austenitic stainless steel. The target fluence is 10^{22} n/cm² (E > 0.1 MeV), which should represent a higher level than end-of-life fluence. To date, the surveillance capsules have reached approximately 20% of the target fluence. In addition, specimens fabricated from the same austenitic stainless steel material were placed in the high-flux isotope reactor (HFIR). However, the HFIR test facility is not yet back in operation. Specimens from the austenitic stainless steel were also irradiated at the University of Buffalo test reactor. To date, testing of the irradiated specimens indicate that they have 30% to 40% residual toughness.

Finding. The SRP has an on-going materials radiation surveillance program for the PWR tanks. In addition, SRP has embarked on an accelerated test reactor program to obtain irradiation damage data on austenitic stainless steel similar to the PWS tank material. Available data to date indicate that degradation of the PWS tank material as a result of irradiation could be a problem.

Recommendation. Continue to monitor the PWS tank material for degradation from irradiation. Perform a fracture mechanics analysis based on the most recent fracture toughness data (see recommendation Fuel and Tank System Analysis.)

B.2.3.2 Seismic

B.2.3.2.1 Site Seismic Criteria. Are the seismic ground response spectrum and associated ground acceleration level consistent with today's licensing requirements?

The original seismic design for the buildings (ca. 1950-1953) was based on the Uniform Building Code using loading defined by 0.1(DL+0.5LL) (ICBO 1950). A restart criterion has been established for the K Reactor (DOE 1988) based on Regulatory Guides 1.60 and 1.61 (NRC 1973a, 1973b) through discussions with the DOE (Charlotte, North Carolina, meeting of 11/11/88; Washington, D.C., meeting of 11/17-18/88). Representatives at DOE had expressed concern with the potential for higher eastern seismicity based on the Charleston earthquake of 1886 and the desire to have seismic capability equal to that exhibited by commercial plants.

The commercial nuclear power plant site closest to SRP is the Vogtle Plant, directly across the river in Georgia. The design response spectra are in conformance with Regulatory Guide 1.60 (NRC 1973b). The horizontal and vertical seismic ground acceleration is 0.2g. The earthquake level at SRP is in agreement with the Vogtle seismic ground acceleration level with the exception that the vertical ground acceleration level is taken as two-thirds of the horizontal component (considered acceptable from the safety viewpoint by the subcommittee). Vogtle set the vertical ground acceleration equal to the horizontal ground level, per Regulatory Guide 1.60 requirements (NRC 1973b).

A preliminary safety analysis report (PSAR) for a defense waste processing facility located in the 200-S Area at SRP based its seismic criteria on Regulatory Guide 1.60 (NRC 1973b) with the horizontal and vertical seismic components equal to 0.26g and 0.17g (two-thirds of horizontal component), respectively.

Finding. The restart seismic criteria for the K Reactor are not as conservative as recommendations for new facilities located at SRP. The use of a 0.2g seismic ground acceleration level is considered adequate by the subcommittee to define the design-basis earthquake (DBE) event. The restart seismic criteria for the K Reactor are acceptable because they provide a level of seismic resistance

comparable to that exhibited by the Vogtle Plant and have been agreed to by DOE as the interim criteria.

B.2.3.2.2 Response Spectrum Analysis. Are the response spectrum modal analyses for equipment and piping systems being performed consistent with the NRC regulatory guides?

From discussions with analysts as well as a review of reports, it was determined that the methods employed are not always consistent with current practices.

- A modal combination by square root sum of squares is used, which is representative of early 1970 methodology. It will yield a lower response than the methodology in Regulatory Guide 1.92 (NRC 1976).
- Response from three orthogonal seismic components could be conservatively calculated using absolute sum instead of the accepted practice of root-mean-square combination.
- Modes less than 25 Hz only are used, ignoring the potentially significant effect of the higher modes on piping stresses and support loads. This practice is contrary to currently accepted practices and can be nonconservative.
- Support flexibility is not considered.

Finding. Response spectrum modal analyses performed using dynamic methods do not conform to current NRC requirements and have the potential of being nonconservative.

Recommendation. A review should identify the dynamic analyses that are used to demonstrate qualification of safety-related systems. An evaluation should be made of all these dynamic analyses to determine whether the support stiffness should be included and whether the modal cut-off frequency used ("missing mass" effect in the analysis) could significantly affect the result. Where significant, an evaluation or rerun should be made (see recommendation Dynamic Analysis).

B.2.3.2.3 Response Spectra Development. Are the response spectra developed for the reactor building conservative?

Response spectra using a stick model representative of 1967 technology have been developed. Discussions are being held with DOE concerning the adequacy of using this stick model on an interim basis. A review of this model and its analysis is being performed for Du Pont by members of the Westinghouse transition team. The findings from this review are being incorporated into the SRP upgrade program. A commitment has been made by Du Pont to DOE to revise this model in the long term using current technology.

Finding. Response spectra are developed using a dynamic model based on 1967 technology. Meetings are being held among DOE, Du Pont, and Westinghouse concerning the adequacy of the dynamic model for the interim. The subcommittee has been following the progress of these meetings and is in agreement with the actions being taken.

B.2.3.3 Adequacy of Safety Systems and Structures

B.2.3.3.1 Seismic Qualification Utility Group Criteria. Are the SQUG criteria adequate for seismic qualification of SRP systems and have all the necessary safety systems been seismically qualified?

The commercial nuclear industry formed the SQUG to gather experience data from facilities exposed to actual seismic events and to use these data to establish an explicit set of guidelines and acceptance criteria for evaluation of equipment in older nuclear plants. The SQUG prepared a generic implementation procedure (GIP) to define the walkdown procedures, the qualification of walkdown teams, and the generic equipment qualification procedures to be used.

The NRC issued a safety evaluation report endorsing the GIP in July 1988 (NRC 1988). The NRC approval of the entire SQUG methodology is also contained in NUREG 1211 (Chang and Anderson 1987).

Pipe systems are not specifically addressed by the GIP because very few pipe failures were observed in actual earthquakes. The basic SQUG position is that pipe built to ANSI Standard B31.1 requirements and attached to properly anchored equipment will not fail at acceleration levels common to DBEs in the continental United States. The SRP used a combination of analyses and walk-down procedures to qualify pipe systems. Civil structures and buried pipe systems are excluded from the SQUG methodology and require explicit analysis.

The SQUG walkdowns using SRP-specific procedures based on the GIP were conducted on K and L Reactors in September and October 1988. The SRP identified a minimum number of safety systems to be qualified to the GIP and NUREG 1211 requirements:

- The SSS, consisting of two redundant poison injection systems. Only the pressure boundary, manual activation system, and new seismic trigger system are to be qualified
- The PWS, including Caterpillar diesel generators and primary pumps and drives
- The CWS, including heat exchangers and gravity-feed pressure boundary
- Instrumentation and electrical as required for SSS, PWS, and CWS, and reactor monitoring and control.

The above systems were seismically qualified by SQUG procedures and analyses. Methodology included II/I interaction evaluations. The associated civil structures and buried pipe were qualified to withstand a 0.2g zero-point acceleration DBE by explicit analyses.

The pipe systems for these safety systems were also qualified by walk-down and explicit analyses. The systems were evaluated using equivalent static load methods to ensure that resulting pipe stresses are within ASME Code Case 1606 limits (ASME 1973) and that pipe support anchoring is adequate.

The results of the SQUG evaluations of the K and L Reactors were addressed at meetings of DOE-SRL, DOE/E&HS, Du Pont, and subcontractors in Charlotte, North Carolina, on November 11, 1988, and in Washington, D.C., on November 17-18, 1988. At these meetings, DOE expressed a concern with eastern seismicity based on the Charleston earthquake of 1886. Additional requirements were imposed on SRP that are now being addressed by Du Pont.

Based on the SQUG evaluations and DOE reviews, the following additional actions are required prior to restart.

- Complete the generation of new confinement building floor response spectra using both site-specific and Regulatory Guide 1.60 (NRC 1973b) generic spectra.
- Complete the evaluation of the confinement structure to Regulatory Guide 1.60 spectra.
- Complete the reevaluation of 107 Building sump pumps to Regulatory Guide 1.60 spectra.
- Complete the lead expansion anchor bolt test program to develop allowable loads.
- Complete the reevaluation of K and L Reactor anchorage and pipe systems using Regulatory Guide 1.60 and/or site-specific floor spectra and new lead anchor allowables.
- Implement mandatory fixes identified by SQUG evaluations.
- Add a seismically qualified MRS.

Finding. The SQUG criteria are an adequate basis for the seismic qualification of safety equipment in the SRP reactors. The procedures are acceptable to NRC for commercial nuclear plants.

Recommendation. A concern is whether the SRP staff has identified and qualified a sufficient number of safety systems to protect the public adequately in the event of a major DBE seismic event. It appears that they have met the minimum requirements as outlined in the SQUG GIP and NUREG 1211. However, improvement in defense in depth is desirable. Flooding may occur, causing loss of PWS pumps, if the CWRSS is not qualified. This system should be seismically qualified prior to restart, along with the necessary power supplies, at least to a capacity consistent with the consequences of the event (see recommendation Sump Water Removal Capability).

Of lesser concern, because of other systems that provide backup safety functions, is the ECS. The ECS should be qualified in the long term. The SQUG methodology should be used for these tasks (see recommendation Long-Term Seismic).

B.2.3.3.2 System Structural Integrity. Is the structural integrity of the safety systems adequate to ensure operability under normal and off-normal operating conditions?

Structural components of safety and safety-related systems were originally designed to chemical process industry and Du Pont standards. Fluid-containing systems were designed to ANSI standards B31.1 and B31.3 (ANSI 1986) for piping and the ASME Boiler and Pressure Vessel Code, Section VIII (ASME 1986a), for vessels and components. The design approach is based on the ability to inspect, detect structural deterioration, and make repairs as necessary. The structures were not initially designed for seismic loads, except for those implicit in the civil structural codes of the time (e.g., 0.1g static).

Over the years since 1953, the systems have been modified, components replaced, and new systems added. The systems were designed and evaluated to the then-current standards. Systems or portions thereof added recently have been evaluated generally to the nuclear standard for Class 2 components, ASME Section III-NC (ASME 1986b). These include the SSS and the MRS. Systems considered critical to safety have also been evaluated for a seismic 0.2g ground acceleration, some by SQUG walkdowns and some by analysis.

The habitability system has been qualified during the SQUG walkdown to a limited extent, addressing emergency lighting and items that could fall and affect identified safety class systems and the operators.

Finding. The safety and safety-related systems have been designed and constructed to good commercial standards. The systems considered most critical to safety have been evaluated for seismic loads and upgrades identified to meet current standards. The PWS has been evaluated extensively to current nuclear standards and is considered to provide the same level of safety as recently designed plants, based on implementation of enhanced inspection procedures and revised operating procedures. The SSS and the MRS have been designed and constructed essentially to nuclear standards for Class 2 components. Since neither the control rods nor the safety rods have been seismically qualified, the SSS is required to ensure safe shutdown. The CWS and REMACS are considered adequate based on SQUG walkdowns and implementation of defect corrections to those systems. The confinement structure is adequate based on analysis. The CWRSS, ECS, GM diesels, and emergency power systems (EPSs) have not been seismically qualified.

The SQUG walkdowns performed to date have identified a number of component supports and anchors that were either inadequate for seismic loading or improperly maintained.

Recommendation. From the defense-in-depth standpoint, additional systems should be qualified as part of the upgrade program after restart. It is recommended that the AACS and CHRS be seismically qualified in the long term. It is recognized that, based on the assumption that a large LOCA will not occur as a result of a seismic event, the confinement system will not be required during and immediately following a seismic event. However, these systems should be seismically qualified in the long term to improve defense in depth. All supports and anchors of all safety and safety-related systems should be checked and upgraded to accommodate seismic loading. The maintenance program

should be reviewed to ensure adequate inspection of supports and anchors (see recommendation Long-Term Seismic).

B.2.3.3.3 Process Water System Gas Plenum Overpressurization.

Are the roll anchors adequate to hold down the PWS reactor tank top shield and plenum when subjected to overpressurization of the gas plenum?

Full ECS injection when process water flow is interrupted (e.g., as a result of a LOPA) may cause overpressurization of the gas plenum and an upward force on the top shield and D₂O plenum. The upward force is transmitted through the plenum inlet nozzles to the roll anchors, which serve to react to the upward force on the plenum. If the roll anchors fail, the plenum would lift and stretch the plenum seal. This situation could overload the piping, inlet nozzles, and plenum seal. Failure of the piping or plenum inlet nozzles could cause a loss of cooling water.

Finding. The roll anchors have been modified to accommodate over-presurization of the gas plenum, but it is not known whether the modification is adequate for the K Reactor. Preliminary analysis indicates that the roll anchor bolts are adequate for the predicted overpressure. The lifting force on the top shield and D₂O plenum is displaced through the plenum inlet nozzles, which are already highly stressed under certain conditions, and the plenum inlet nozzles have apparently not been analyzed for this condition. The plenum seal is a thin-walled bellows type of stainless steel seal that has apparently not been analyzed for overpressurization. The plenum uplift and resulting seal deformation have also not been determined.

However, even if the roll anchors fail, it is not apparent that the damage would cause disruption of core-cooling capability. The maximum upward motion of the plenum, limited by the hold-down beams, is reported to be about 0.5 in. Rupture of the plenum seal would provide another path for water overflow and thus reduce plenum pressure. Preliminary analysis indicates that the plenum seal would not rupture from predicted overpressurization, but the effect of plenum uplift has not been evaluated.

Recommendation. The effect of overpressurization of the gas plenum from full ECS injection when the gas plenum becomes solid should be determined. This process should include evaluation of the roll anchor structure, plenum inlet nozzles, vertical motion of the plenum, and plenum seal deformation and stress (see recommendation Gas Plenum Overpressurization).

B.2.3.3.4 Fuel Transfer. Does the process assembly pose a III/I problem during fuel transfer?

The process assembly is hung on monorails. No analysis has been made of its impacting a safety-related piece of equipment as a III/I problem. It was noted by SRP that the fuel does not weigh much and that multiple failures would be necessary for the fuel to be released. That the fuel would be dropped is not considered credible by the RTD of the SRP. Further, the forest above the reactor

has not been evaluated when it is in the fully extended position during fuel transfer.

Finding. No evaluation has been made of the impact of the process assembly, handling equipment, or forest on a safety-related piece of equipment during transfer.

Recommendation. As a minimum, safety-related equipment that could be affected by dropping of the process assembly, its impacting in the disassembly pool areas, and failure of the forest should be identified, and an evaluation should be made. This issue is not related to restart (see recommendation Fuel Handling).

B.2.3.3.5 Safety-Related Buildings and Structures. Are the buildings and structures that are important to safety structurally adequate?

Six structures and buildings were identified that are important to safety. They are the reactor building (105 Building), reactor building exhaust stack, actuator towers, reactor cooling-water basin and effluent sump, confinement system filters compartment, and disassembly area.

The assembly area does not contain irradiated fuel. The only safety-related system that could potentially be lost by failure of the building is a 1-in. PWS line. However, the flow loss would be less than the makeup capability, and the line can be closed manually. Therefore, the structure is not considered critical.

The reactor building and stack and actuator towers have been evaluated for the 0.2g, Regulatory Guide 1.60 (NRC 1973b) seismic event. The basin and sump structures have been evaluated for the Blume spectra at the 0.2g seismic level. The disassembly basin, walls, and columns have been assessed for the defined 0.2g Housner seismic criteria in 1969 by Blume and Associates.

The reactor building, actuator towers, and exposed areas of the disassembly area are designed for an over-pressurization load of 1,000 lbf/ft². It is noted in the Blume report that: "Buildings shall be designed for static live load of 1000 lbs per square foot acting simultaneously on gross area of outside face of exterior walls and roof. Foundations and building anchorage to be checked for overturning produced by the 1000 lbs per square foot acting on one face only at one time." Care must be taken in extrapolating the blast loads to an equivalent seismic loading since only foundation and building anchorages were checked for overturning and not the internal stresses within the building structures. The reactor building and actuator towers have been evaluated for a tornado load of 280 mi/h with a 1.5 lbf/in² pressure drop. The only structure evaluated for tornado missiles [defined in Table 3-2 of the *Safety Analysis of Savannah River Production Reactor Operation* (Du Pont 1987)] is the disassembly area structure. The building exhaust stack has been evaluated for a 125 mi/h wind. The tornado event affecting unprotected structures and systems is discussed in the SAR referenced above: "... Damage to the 200 foot stack, confinement system filter compartments, and other parts of the building that are not resistant to tornadoes, would not cause, directly or indirectly, a reactor accident. The emergency power and cooling capabilities are sufficient to maintain the reactor in a safe shutdown

condition if outside power is lost during a severe weather disturbance. Hence, the filter compartments, which are not tornado resistant, are not needed under that circumstance."

It is important to note that during the review of the seismic building analyses by the Westinghouse transition team it was discovered that the structure under the stack had not been evaluated. For the stacks and their support structures, forces resulting from the earthquake ground motion have been computed, but a design check for dead, seismic, and other loads on the support members and foundations has not been performed. A preliminary assessment was made by R. S. Orr, of the Westinghouse transition team, of the building structure under the stack; he found that the building's structural columns are potentially over their ultimate moment capacity. This issue is known to Du Pont and DOE and is being addressed accordingly. An action plan is being developed with parallel programs considering further analysis and potential design modifications.

Finding. The building structure under the stack is potentially overstressed. This condition is known by Du Pont and the situation is being addressed. The subcommittee is in agreement with the approach being taken to resolve this issue and no program change is recommended.

B.2.3.3.6 Vessel Internals and Plenum. Can a sufficient number of control/safety rods be inserted after a design seismic event to maintain a safe-shutdown condition?

This part of the review includes the plenum and top and bottom shields with tubes. This evaluation includes component behavior under steady state, expected and unexpected transients, and accident conditions such as a seismic event. The plenum, connected pipes, sleeves, and process assemblies are supported vertically by the permanent sleeves in the top shield. No lateral restraint exists to absorb horizontal seismic loads and/or nozzle loads resulting from the piping. Friction between the connecting sleeves and the shear strength of the fuel assemblies will transfer the horizontal load to the top shield. The top shield is vertically supported by six I-beams with bearing pads. Permanent lateral displacements resulting from top shield movement or permanent deformation of the fuel assemblies could impair insertion of the control and safety rods. Seismic analysis is presently not available, but we judge that a detailed analysis could prove that the seismic response will remain below acceptable limits when the specific response spectra and realistic damping values are used. Allowable criteria and acceptable stresses, coefficient of friction, and differential displacement should be established. The lower shield should not have any problem from a seismic point of view. No stress analysis for normal operating and transient loads has been seen for these structures, but it is felt that this is not an issue because of many years of operation without a problem. The review was limited by the lack of specific analyses for these components. We feel that the risk of a failure under seismic loads is very small.

We recognize that under a seismic load from a design-basis earthquake the plant will be shut down with the SSS and that rods are not needed. The question does arise as to whether there will be a further need to insert rods if the plant remains in a shutdown situation for a prolonged period of time. For a seismic event below the DBE, rods will be needed when the system is not initiated; and even if the rods can be inserted, it should be shown that scram delay time is acceptable. Low seismic events could produce relatively high input resulting from lower concrete structures damping, damaging the upper structure (forest) integrity and operability.

Finding. Based on the premise that there is no need to insert the rods during an earthquake, scram time is not considered a problem, but attention should be given to the need to insert enough control or safety rods after the seismic event or in case the Ink system is not initiated to maintain the plant in a safe-shutdown condition.

Recommendation. Perform a seismic analysis after restart and show that enough control or safety rods can be inserted after a seismic event to maintain the plant in a safe-shutdown condition (see recommendation Shutdown After Seismic Event).

B.2.3.3.7 Vessel and Thermal Shield. Is the vessel and thermal shield structural integrity adequate for the design loading?

The vessel has been analyzed for steady-state operating and seismic loads. No seismic analysis was found for the thermal shield. The absence of problems during the operation period provides confidence of the acceptability of the design, but there are indications that material damage could exist due to radiation. The tank has been shown to be within acceptable levels according to Section VIII of the ASME Code (ASME 1986a). The fact that the reactors have been operating for so many years without major problems (other than leaks in C Reactor) is proof that the design is reliable for the operating conditions of interest, but the analysis should be updated. Fatigue (low-cycle fatigue) should be considered assuming that two full cycles (70°F to 212°F) will occur per month (i.e., 24 per year of operation). Certain transients not seen by the plant in the past, such as an earthquake, will need to be reviewed and qualified (particularly for the thermal shield). Also, material deterioration during the years of operation should be considered in the evaluation. No analyses for transients on the tank were made available to the reviewers, nor was a study determining that the thermal shield will not lean on a localized vessel wall segment.

Finding. No complete structural analysis of the tank and thermal shield was found.

Recommendation. Complete structural analysis should be performed. This issue is not related to restart (see recommendation Fuel and Tank Assembly Analysis).

B.2.3.3.8 Fuel Assemblies. Is the process assembly structural integrity and reliability adequate for the design loadings?

The fuel is inside the housing cylindrical tubes (universal sleeve housing), hanging from the top of the plenum and laterally supported at the top by the plenum wall and at the bottom by the guiding pins. During plant operation, these assemblies are subjected to flow-induced vibration resulting from the D₂O longitudinal flow inside the assembly (around 20 ft/s) and the much lower cross flow (around 1 ft/s). Through the years, the design has been optimized to minimize the effect of wear on the ribs. The universal sleeve housing is replaced when wear is noticed, after two to five years of use. To avoid excessive wear, fuel columns are laboratory tested, and the design is adjusted every time a new configuration is used. Some analyses have been performed for transportation transients (Crowley and Yau 1983). Consequently, we felt that, from the structural point of view, no short-term action is required.

For the long term, particularly for future designs, we suggest a joint effort among mechanical, hydraulic, and nuclear experts to consider the optimization of the design.

Regarding seismic qualification of the process assemblies, we found no credible analysis. These structures have a low natural frequency (0.3 Hz for the first natural frequency has been mentioned), and a seismic analysis should indicate the level of response. The complexity of the concentric structure will ensure that losses during vibration (damping) will be important in limiting the seismic response. A systematic and realistic combined test and analysis process will eventually show that the seismic event being postulated for the site will not produce unacceptable damage. Consequently, we felt that a seismic qualification process does not need to be performed before plant restart, but it will be prudent to have a seismically qualified process assembly in the not-too-distant future. The qualification should obtain information about structural properties of the fuel assemblies (modal stiffness and modal damping in water) and response amplitude. In addition, criteria for these assemblies should be established for allowable stresses under dynamic loads.

Finding. No evaluation exists to show structural integrity under seismic loads. No seismic criteria exist for the structural design of the process assemblies.

Recommendation. Seismic analysis should be performed. Criteria with allowable limits and load combinations should be prepared. This issue is not related to restart (see recommendation Fuel and Tank Assembly Analysis).

B.2.3.3.9 Process Water (System) Distillation System. In the event of failure of this system, are procedures in place to evacuate personnel and provide the ability to monitor necessary postshutdown instruments?

The PWS distillation system is located outside the confinement building. It contains a large inventory of tritium. The system is not seismically qualified. In the event of an earthquake it could fail, releasing heavy water and tritium.

Finding. We were not able to determine what the effect of this release would be on reactor personnel or others such as maintenance people. Furthermore, since the REMACS is not seismically qualified, it is not certain that postshutdown instruments could be monitored.

Recommendation. Develop emergency procedures for plant evacuation and postshutdown instrument monitoring for seismic events that may impact this system (see recommendation PWS Distillation System).

B.2.4 MEETINGS AND INFORMATION GATHERING

Five SRP site visits were made during the months of December 1988 and January and February 1989 by members of the subcommittee. Information was obtained primarily from discussions with Du Pont personnel, supplemented by reports, documents, and calculations. The supplementary information sources are referenced above as necessary. Individuals interviewed at the site included the following: Overview--Tom Gorrell; materials--Bill Awadalla, Bob Ondrejcin, R. E. Sprayberry, M. E. Du Pont, W. S. Ehrhart, E. J. Majzlic, M. H. Hilker, P. R. Vormelker, M. R. Louthan, R. L. Sindelar, J. Morrison, J. Stone; seismic/structures--D. R. Ketcham, T. M. Monahan, Dave Freeman; system qualification and seismic criteria--Bill Anderson; confinement system--Larry DeWitt; SSS qualification--Rich Salizzoni; CWS qualification--D. Ferguson; ECS qualification--Bob Taylor; Integrated Safety Evaluation Program--Bob Findley; vessel and internals--W. Yau, George Richardson, Vascoe Whatley, Elwyn Wingo; site tour--Al Mink, Ivan Lewis, Lee Gaston, George Rawls, Kevin Stoner, Tom French, Sam Formby.

B.2.5 BIOGRAPHICAL INFORMATION

W. S. LAPAY

Dr. Lapay joined Westinghouse in 1969 after completing a PhD in civil engineering at Case Western Reserve University. Prior to joining Westinghouse, he provided structural engineering services to architect/engineer (A/E) firms as well as to Bethlehem Steel Corporation. He has held the position of adjunct faculty member of the Department of Civil Engineering at the University of Pittsburgh. He has almost 20 years of experience in the nuclear power industry, during which time he has been actively involved in the field of qualification of nuclear power plant structures, piping systems, and equipment. Currently he holds the management position of advisory engineer responsible for providing technical assistance to the functional groups on complex technical issues related to structure and equipment design and analysis. He is recognized as a technical expert in the fields of dynamic and seismic response, civil and structural design, and nonlinear and inelastic structural behavior. He is a member of two American Society of Civil Engineers (ASCE) committees: (1) Nuclear Structures and Materials and (2) Nuclear Standards. He is the affiliate member representative for Westinghouse on the Building Seismic Safety Council. He also is a member of IEEE-344 Committee 2.5A responsible for establishing seismic qualification standards for Class IE electrical equipment. He received his BS and MS in civil

engineering from Case Institute of Technology and is a licensed professional engineer in Ohio, Pennsylvania, and California.

M. J. ANDERSON

M. J. Anderson graduated from Oregon State University in 1955 with a BS in civil engineering. He is a registered professional engineer in the state of Oregon. He has been a member of the Westinghouse Hanford Company staff since 1972 where he is presently manager of the Engineering Analysis Function. His assignments have included responsibility for preparation of ASME as-built stress reports, including seismic qualification, of FFTF high temperature pipe systems; seismic upgrade qualification of the N Reactor primary pipe system and control room building; and structural design and seismic qualification of the SP-100 ground engineering system sodium pipe systems and containment building. Mr. Anderson is a member of the ASME and has published 18 ASME technical papers related to seismic qualification and acceptance of nuclear pipe systems. He is also an active member of the Pressure Vessel Research Committee and participates on the Subcommittee on Elevated Temperature Design, the Task Force on Elevated Temperature Pipe, and the Technical Committee on Piping. Prior to joining Westinghouse, Mr. Anderson was a member of the technical staff of Rocketdyne Division of Rockwell International for 14 years, where he performed detailed structural analyses of rocket engine turbomachinery.

G. J. BOHM

George Bohm has over 39 years of experience including 28 years at Westinghouse. His expertise is in structural mechanics related to nuclear power plants as well as the development and implementation of methodology to qualify equipment. He has been a consulting engineer to the Engineering Manager and General Manager, Power Systems. He provided technical consultation to the engineering departments on all phases of structural analysis, dynamic behavior and testing of equipment, development of qualification methods, allowable criteria, and training and qualification of personnel in relation to analytical methods and problem solving. He provides advice on the development and adoption of structural codes, flow-induced vibration methodology, accident loads consideration, and computer-aided engineering technology. Mr. Bohm acts as a consultant for Westinghouse in Japan, Italy, Belgium, and Germany regarding the dynamic behavior of reactor components. He has pioneered the seismic technology presently in use, particularly on methodology and damping determination. Mr. Bohm is the author of more than 70 publications on nuclear power plant design and analysis. He is presently chairman of the ASME Task Force on Faulted Conditions, a member of the ASME Task Group on Dynamic Analysis, Vice Chairman of the ASME Subcommittee on Vibration Monitoring, and member of the ASME Committee on Equipment Qualification. He received his BS and MS in civil engineering from the University of Buenos Aires.

T. R. MAGER

Mr. Mager is Consulting Engineer, Plant Engineering Department, in the Westinghouse Nuclear and Advanced Technology Division. Included in his responsibilities are identifying major technical problems and providing consultation in the areas of fracture, reactor vessel integrity, radiation effects, and fracture mechanics. Prior to this assignment he was Manager, Metallurgical and NDE Analysis, Westinghouse Power Systems Division, responsible for the nondestructive examination, materials, and process support technology relating to the design, fabrication, construction, licensing, and operation of PWR plants. In 1975-1976 he was Manager, Materials Engineering, Westinghouse Nuclear Europe. He joined Westinghouse in 1953 in the Solid State Physics Department of the Westinghouse research laboratory and worked for 13 years primarily on the relationship of magnetic phenomena to metallurgical phenomena. During his 22 years in the Energy Systems Division, he has been concerned with the fracture mechanics approach to brittle fracture and irradiation effects. He received a BS in 1959 and an MS in 1962 from the University of Pittsburgh in metallurgical engineering. He is a member of the American Institute of Metallurgical Engineers, the American Society of Metals, and the American Society for Testing and Materials. In 1978 he was elected to the Technical Advisory Committee of the Metals Properties Council.

D. S. GRIFFIN

Dr. Griffin is Manager of Energy Systems Engineering in the Westinghouse Nuclear and Advanced Technology Division. He has 30 years of experience in the structural design, development, and evaluation of nuclear reactor systems. At Westinghouse he has developed computer-oriented methods of analyses, structural design criteria, and design procedures for naval, PWR, and fast breeder reactors. He has directed structural analyses of static and dynamic systems including effects of fatigue, fracture, thermal shock, seismic, fluid-solid interactions, and nonlinear response of materials. He is known as an expert in buckling and instability, inelastic analysis, and elevated-temperature structural design. Dr. Griffin received his BME from Cornell University, and his MS and PhD in engineering mechanics from Stanford University. He is a Fellow of the ASME, past Associate Editor (1973-1980) of the *Journal of Applied Mechanics*, past Chairman (1982-1983) of the ASME Pressure Vessel and Piping Division, and author of 26 publications in applied mechanics, computer methods, and elevated-temperature structural design.

APPENDIX B.3 ELECTRICAL, INSTRUMENTATION, AND CONTROL

R. Michael Boger, Principal Engineer, Westinghouse Hanford Company
James R. Easter, Fellow Engineer, Westinghouse Nuclear and Advanced
Technology Division

Peter J. Morris, Manager, Instrumentation and Control Systems
Licensing, Westinghouse Nuclear and Advanced
Technology Division

Donald J. Vochinsky, Senior Engineer, Westinghouse Nuclear and
Advanced Technology Division

B.3.1 SCOPE

Our subcommittee evaluated whether essential electrical, instrumentation, and control safety systems are adequate to support restart of the SRP reactors. We met with SRP personnel; inspected reactor facilities, primarily at the K Reactor; coordinated with other subcommittees; and participated in meetings of the full committee. Many individual contacts with SRP personnel supplemented these activities, as listed at the end of this appendix (section B.3.6).

Restart safety acceptance criteria are stated in Chapter I of the committee report. This subcommittee's evaluation focused on criteria 1 and 2. We did not perform a rigorous review in terms of criteria 3 and 4, but concerns related to them are noted. In performing our assessment, we used our best judgment according to the intent of current industry standards for the design of nuclear reactors. Interpretation of intent was based on the way standards are applied to nuclear plants of similar age, on significant design differences between Savannah River reactors and commercial nuclear reactors, on DOE policy statements concerning standards for reactor facilities, and on the combined experience of the subcommittee members.

Because of the scope that a detailed review of the electrical, instrumentation, and control systems related to safety would have entailed, we focused our evaluation on the adequacy of critical safety functions. This concept was developed and adopted in the commercial nuclear power industry through the efforts of EPRI and the NRC following the 1979 incident at Three Mile Island, Unit 2. The design of a commercial nuclear power plant includes three concentric barriers to prevent a release of radioactivity: the fuel clad, the reactor coolant

system boundary, and the containment. The functions that the operating staff can and must control to protect the integrity of the barriers in a commercial PWR are the following:

- Reactivity (subcriticality)
- Core cooling
- Reactor coolant system coolant inventory
- Heat sink
- Reactor coolant system pressure (this is sometimes called the RCS integrity function; it focuses on the problem of cold overpressurization)
 - Flow of radioactivity (this function focuses on ensuring that the containment is and remains sealed).

In adapting the concept to the design of the SRP reactor, the subcommittee chose five essential functions to monitor and control:

- Subcriticality
- Core cooling
- Heat sink
- Confinement
- Process water inventory.

A large portion of the subcommittee's evaluation and observations in this report is organized around these five functions.

The commercial nuclear power industry uses critical safety functions to address the issues critical to ensuring the health and safety of the public. We suggest that the same strategy be adopted for the SRP reactors in their continuing long-term improvement program.

B.3.2 GENERAL DESIGN ISSUES

B.3.2.1 Separation

By separation, we mean electrical and physical isolation between redundant channels of safety circuits and between safety circuits and nonsafety circuits. Proper separation of safety circuits ensures that an external event or a single failure within a redundant circuit will not cause loss of capability to trip the reactor or mitigate postulated design-basis accidents.

Defense in depth requires redundancy, and the requirement for separation is inherent in the requirement for redundancy. Lack of electrical separation increases the vulnerability of redundant circuits to single failures, while the lack of physical separation increases the vulnerability of redundant circuits to common-mode failures. Common-mode failure hazards include seismic events, fire, missiles, high-energy tanks and piping, and flooding.

It is the nature of instrumentation, control, and electrical circuits to be concentrated physically and thus subject to common-mode failures and the propagation of single failures. In addition, failure modes (shorts, hot shorts, and open circuits) and failure sequences are not predictable. Therefore, strict separation guidelines are applied as a means of protection against failures.

The primary concern over the lack of separation comes from fire. The November 11, 1988, DOE restart strategy issue DB-4 (DOE 1988) and the current SRP plans will implement procedures for prompt response to an indication of fire and prompt shutdown of the reactor during a fire. We endorse these as essential measures to be implemented prior to restart for reducing risk to critical safety functions.

The second concern related to separation is a seismic event. This concern is being addressed by restart strategy issue DB-2 (DOE 1988) and has resulted in the addition of seismic trips to the redundant SSS (Ink).

Another concern involves the ability to monitor maintenance of the reactor in a shutdown condition and core cooling during and following design-basis events. Lack of redundancy and separation could result in loss of the ability to monitor a critical parameter.

B.3.2.2 Seismic and Environmental Qualification

Equipment is qualified to reduce the potential for common-mode failures leading to the complete loss of important plant safety functions. Such common-mode failures could result either from natural phenomena (e.g., seismic) or from internal plant events such as accidents that might impose abnormal service conditions. Much of the equipment important to safety in the SRP reactors has not been qualified either seismically or environmentally. Humid and radioactive conditions could exist for some time following an accident. It has not been possible to determine that credible environments were properly considered in equipment specification and operation. We suggest that criteria be established for future plant changes to ensure that equipment will operate properly during service conditions for which its performance is required. This suggestion includes clearly defining a set of environmental qualification criteria for the confinement building and any other areas where important safety equipment could be exposed to adverse environmental conditions from events for which it must provide protection.

Commercial nuclear power plant practice has been to qualify all safety equipment for seismic conditions. This approach has not been followed at SRP, where only a limited set of the plant equipment, including instrumentation and control, has been so qualified. The safety systems at SRP are very dependent on the use of relays for actuating reactor scram and other safety systems. Relays have been shown to be subject to chatter or complete failure if seismic levels are sufficiently high. We suggest that a sample of relays be removed from the plant and tested seismically to ensure that chatter or other failure modes will not result

in the inability to operate necessary safety systems or lead to the spurious actuation of safety systems in a manner that could lead to unsafe plant conditions.

B.3.2.3 Defense in Depth

The principle of defense in depth is particularly important as applied to the electrical, instrumentation, and control areas. These systems are intimately involved in manual and automatic shutdown, maintenance in a safe shutdown condition, accident mitigation, accident monitoring, and remote monitoring and control. To ensure the success of accident prevention and mitigation, instrumentation and control and associated electrical systems are designed and operated to minimize the effects of both single and common-mode failures.

Our review attempted to determine how well the instrumentation, control, and electrical systems support defense in depth by minimizing the effects of single and common-mode failures through separation, redundancy, independence, seismic and environmental qualification, good human factors practices, maintenance, and operational practices.

B.3.2.4 Redundancy/Diversity

Redundancy and diversity are provided in safety systems designed to ensure that credible failures do not lead to failures of important functions. The single failure criterion, generally applicable to all safety systems, has guided the design of commercial nuclear power plants. The result has been to provide two or more redundant channels of instrumentation and actuation equipment to perform important safety functions. The SRP reactors do not provide simple redundancy of the type described above for some safety systems, relying instead on the diversity of actuation equipment or instrumentation to tolerate single failures while still ensuring that safety criteria are met. This situation is true in the scram actuation circuits. Several of these have only one instrument, so that failure would preclude a scram on that process measurement. The argument is made that other instruments are available in such cases to scram the reactor prior to the violation of safety limits. Verifying this assessment in every case was beyond the scope of our review.

B.3.2.5 Functional Performance

Functional performance, as used here, includes selection of the proper protective functions and evaluation of their accuracy and time response. Selection of proper protective functions (for safety system actuation) is directly related to knowledge of accident progression and accident acceptance criteria. We did not evaluate these choices. System accuracy is typically accounted for in the commercial nuclear power industry by ensuring that sufficient margin exists in the setpoints actually set into instrumentation systems to account for uncertainties

such as calibration, drift, environmental effects, etc. Terms such as 'safety analysis limit,' 'channel allowance,' and 'limiting safety system setting' have been developed to deal with the issue of accuracy and are reflected in current standard technical specifications. It was not demonstrated that instrumentation uncertainties, for either automatic actuation or operator information purposes, had been systematically evaluated in this manner for the SRP reactors. We suggest that such an evaluation be made, updated when any information affecting it changes, and used in choosing setpoints for automatic systems and operator actions.

Time response is normally accounted for by including appropriate response times in the safety analysis (typically modeled as a time delay or first-order filter, as appropriate). Time response issues should be fully incorporated in safety analyses for all instrument channel and other time delays.

B.3.2.6 Testability

Testing of safety systems ensures that equipment can be expected to perform properly if called upon to do so. The requirements for periodic testing (surveillance) are contained in the technical specifications for commercial nuclear power plants. One good testing practice performed at the SRP reactors is a bench-calibration and time-response test of all scram sensors (aside from the instruments monitoring fuel assembly parameters) yearly, a period that is generally defined as up to two tritium cycles or about 18 months. This procedure meets or exceeds the sensor testing practice used in commercial nuclear power plants today.

The testing of safety circuits takes place on two levels at SRP. The first is a test performed on each safety circuit at each refueling outage. This test checks the entire circuit including the sensors and the final actuation devices. The second is a functional test performed periodically during plant operation at intervals of between 7 and 60 days depending on the circuit. These tests also include the sensors and go through to the last component in the circuit that can be tested without causing a scram or other safety system actuation. One exception is that the input from the thermocouples and flow sensors to the safety computers is not checked periodically because of the difficulty in doing so and because of the long time interval during which the safety computers would be bypassed to check the large number of sensors involved. These tests are controlled by plant procedures and are equivalent to those performed at commercial power reactors.

B.3.3 MONITORING AND CONTROL OF CRITICAL SAFETY FUNCTIONS

For each of the critical safety functions, the subcommittee listed possible methods of monitoring and execution appropriate for the SRP reactor design and

postulated design-basis events (Table B.3-1). Depending on the event and the condition of the plant, different methods or combinations of methods may satisfy the requirement.

Table B.3-1. Critical Safety Functions.

Critical function	Subcriticality	Core cooling	Heat sink	Confinement	PWS inventory
Methods for monitoring	Flux	PWS core exit temperature	Pond level	Radiation flow-path monitoring	Reactor vessel level
	Rod position	Pump delta P	Valve lineup		Moderator recovery
	Ink concentration	Reactor vessel level 105 Building sump level	Flow out to sump		
Methods for execution	Drive control rods in	ECS pumps and DGs	Recirculate to pond from sump	Fans, dampers, spray	Moderator recovery
	Drop safety rods	105 Building sump pumps			ECS
	Inject ink		Gravity feed to heat exchangers		
	Stop moderator purification				

DG = Diesel generator,
ECS = Emergency cooling system,
I&C = Instrumentation and control,
PWS = Process water system.

For the majority of conditions and events, existing systems satisfy the needs for these safety functions well. The following paragraphs discuss each of the safety functions, including the vulnerabilities of the existing design, planned modifications, and ongoing evaluations by SRP. Human interfaces and support systems, which affect all of the safety functions, are also discussed.

B.3.3.1 Subcriticality

The shutdown systems stop the fission process and terminate heat generation in the core (with the exception of decay heat) when limiting conditions in the reactor system are reached. The PSS does this by use of the safety rods and, to a lesser extent, the control rods. The SSS injects a soluble neutron absorber into the reactor tank to shut down the reactor during certain conditions, including failure of the PSS and significant seismic events.

B.3.3.1.1 Reactor Shutdown Systems. There are 66 safety rods, each of which enters the reactor through an open standpipe on the upper plenum. They are driven by DC motors through a gear set, clutch, and drive cable. Normal outward movement of the rod is via a drive motor powered from a 480-V AC emergency bus. The safety rods are fully withdrawn during power operation; reactor criticality and power control are performed by an independent set of control rods. Scram is accomplished by deenergizing the clutch, at which time the rod falls by gravity.

The SSS injects, by nitrogen pressure, a gadolinium nitrate solution (Ink) through a number of distribution headers inside the reactor tank. The Ink can be injected (1) by either one of the safety computers' signaling an explosive valve; (2) by manual actuation of the explosive valves; and (3) manually by a pull-ring in the control room that mechanically punctures a diaphragm, thus venting air from the pneumatic valve diaphragm. A system functional test, performed when the system was first installed, included the actual injection of Ink to shut the reactor down. A system test is performed every two years, in which the Ink solution is replaced by heavy water that is actually injected into the reactor tank. The Ink system is required to be seismically qualified as a part of the seismic scram upgrade by DOE restart strategy issue DB-2.1 (DOE 1988).

B.3.3.1.2 Analog Scram Circuits. The analog circuits that actuate the PSS are generally simpler than those found in the protection systems of commercial power reactors. Most scram functions are actuated if any one of a set of redundant measurements reaches the scram setpoint, greatly simplifying logic design. A typical analog scram circuit might contain a pressure sensor, a pressure switch, and a scram relay. The analog circuits, which protect the reactor against events for which the process measurements used to provide protection either are located on the reactor itself or are associated with one of the six process water cooling loops. They remain essentially as designed when first built, and most of the hardware is original equipment. The analog circuits are not seismically qualified, but spurious operation is likely to result in scram rather than impairment of the scram function.

B.3.3.1.3 Safety Computers. The two safety computers are digital minicomputers installed in 1976 to protect against damage to individual fuel assemblies from flow or power anomalies. Redundancy is provided by separate flow (pressure) and temperature measurements for each fuel assembly. Each safety computer monitors the process water flow in one half of the fuel assemblies and the process water outlet temperature (as monitored by thermocouples) from the other half of the fuel assemblies. This system also provides some redundancy in protection to individual fuel assemblies. The safety computers also monitor the status of the analog scram circuits and actuate an "echo scram;" that is, they will scram the reactor independently if they detect a scram demand from any of the analog circuits. They will actuate the Ink system if the safety rods are

insufficiently inserted within a prescribed time, if a power runaway occurs, or if the reactor goes back to power after a scram involving the safety rods.

The safety computers are programmed in a combination of high-level and machine assembler languages. The use of assembler language tends to make the computers inscrutable to users or evaluators. They have never gone through a verification and validation program to the letter of current nuclear industry standards for computer systems used in real-time safety critical applications. However, we were told that efforts to ensure their reliability have incorporated many of the elements of such standards. Replacement of the safety computers is currently being planned. We suggest that a verification and validation program consistent with current industry and regulatory standards be performed as part of the replacement program.

Because of the large number of process-water flow and temperature measurements (up to 600 of each) that are input to the safety computers, it is fairly likely that a small number (fewer than 10 or so) of such measurements could be lost during an operating cycle. Individual computers also become inoperable at times. Such outages, coupled with the potential loss of a few monitoring instruments as discussed above, lead to the possibility of no monitoring at all of certain fuel assemblies at various times (called gaps) during a fuel cycle. We suggest that the safety computer replacement program give consideration to eliminating the need for operating with gaps.

B.3.3.1.4 Seismic Scram. An existing seismic monitor is set to alarm at 0.002g and to scram at 0.02g, but is not seismically qualified. We found no documentation of the ability of the existing seismic trip and the automatic scram circuits and scram rods to function for seismic events of any level. We judge that the initiation of a scram signal at these low seismic levels would very likely not be impaired; moreover, such a signal would more than likely be the result of spurious action. A new seismic scram has been developed to provide an alternative to the existing scram circuits and is required to be installed prior to restart by DOE restart strategy issue DB-2.2 (DOE 1988). The new scram uses the existing SSS. This new seismic scram is fully qualified and relies on simple circuitry of the type described above for the analog scram circuits. The PSS has not been qualified for operability up to the 0.05g setpoint of the new seismic scram, leaving a range of seismic events for which reactor shutdown has not been proved. Restart strategy issue DB-2.9 (DOE 1988) requires development of procedures and training for response to a seismic event, including the identification of instrument and equipment vulnerability to shaking. We endorse this criterion and expect that it should include an evaluation that the scram rods will function at these fairly low-level ground accelerations.

B.3.3.1.5 Subcriticality Monitoring. A number of instruments monitor the nuclear process in the core from subcriticality through full power. None of these is seismically or environmentally qualified for conditions in the confinement building. Information about subcriticality must be available to the reactor

operator whenever the core should be shut down. However, there are other ways to monitor shutdown status. Knowledge of the control and/or safety rod position or Ink concentration, if available, combined with a detailed burnup history of the core and information on how its reactivity changes with burnup, can be utilized to assess the degree of subcriticality. Core temperature measurements can be used to verify that significant power generation is not occurring. These measurements are indirect, however, and subject to their own uncertainties.

B.3.3.2 Core Cooling

B.3.3.2.1 Monitoring. The subcommittee chose three parameters as a minimum to monitor core cooling.

- The reactor vessel level tells whether the core is covered. In the event of a leak it would indicate whether the rate of makeup is satisfactory.
- Pump operability indicates whether the core is being cooled by forced circulation with the Bingham pumps in the PWS. Cooling by forced circulation with the PWS pumps is the first line of defense and the only method that is currently seismically qualified.
- Sump level is important because flooding in the pump or the motor rooms is a direct threat to cooling flow in the PWS. Numerous small leaks from the PWS or CWS, caused by a seismic event, could pose such a threat.

These parameters should be available for any circumstances including a credible fire or seismic event. Many of the existing methods for monitoring these parameters are not seismically qualified and may be inaccessible or failed because of a fire. The SRP is partially addressing this need in its response to issue DB-2 of the November 1988 DOE restart strategy (DOE 1988). This issue calls for seismically qualified instruments or the capability to monitor primary coolant temperature, tank level, and pump operability. Efforts are under way at SRP to provide this monitoring.

- Temperature. A separate battery-powered box will be mounted on the 'jack panel' in the control room to read a selected set of thermocouples. The entire route of the thermocouples and place for mounting the 'box' have been walked down using the SQUG process. The new equipment being added is being 'qualified' by the experience method. The thermocouple leads are run through the isothermal junction box along with other assembly thermocouples. Fire in the control room or in a space that communicates with the control room could affect operability or prevent access. The isothermal junction box must be verified as spray tight. Although it is very valuable information, the actual core-coolant temperature could be considered secondary in importance to the means of cooling, namely, reactor vessel level and pump operability.
- Pump operability. Procedures will call for visual and audible inspection of the drive system that is accessible from the motor room (motors and shaft).

Rotation and absence of abnormal noises or vibration are good indicators of acceptable pump operation on the DC motor. Additionally, pump delta P will be read using existing suction and discharge gauges located in the motor rooms. The gauges have been included recently in the SQUG program.

- Reactor vessel level. Redundant instruments will sense pressure at monitoring pins near the bottom of the reactor tank. These will be locally read pressure gauges mounted in each of the motor rooms. There is no control room readout.

- Sump level. The SRP assured us that the motor room is accessible, that overflow from the sump is visually observable through the pump observation window, and that the pump room overflows to the motor room across the dam before the pumps are threatened. The existing sump-level instruments are not seismically qualified.

B.3.3.2.2 Process Water System and Emergency Cooling System Operation. The six PWS pumps are the principal method of cooling the core. The ECS provides a backup for events in which the PWS cannot function. With on-line, seismically qualified independent diesel generator and motor drive trains, the PWS accomplishes the core-cooling function in nearly all scenarios. The operation of the PWS requires that the valves be maintained in a normal, open position. Spurious operation of PWS valves as a result of fire or relay chatter in a seismic event threatens the core-cooling function. Multiple valves would have to operate but all are subject to the same type of failure. The PWS valve control circuits have not been seismically qualified, and it is not clear that they are separated or otherwise protected from a fire.

The ECS can be initiated manually from the control room, automatically by the AIA panel, or remotely through the REMACS. In all three cases, actuation of ECS is accomplished through relays in the individual control circuits for the valves and pumps involved. Most of these require power from the emergency power system. In addition, power supplied from UPS or battery systems must be available to the REMACS and the AIA panel.

Automatic initiation is based on reactor tank level and time-delay logic in the AIA. In general, the AIA appears well designed against single failure and inputs to it are reasonably separated. However, the AIA, actuating relays, REMACS, and the power systems on which they depend have not been seismically qualified. There is no special separation or protection of the manual initiation circuits in the control room. The ECS circuits appear susceptible to common-mode failure from a seismic event or a fire. The ECS is not expected to be needed during these events; however, spurious actuation of ECS may have severe consequences. The chief concern is release of tritium from the displaced moderator.

A seismically qualified method of removing water from the 105 Building sumps is required to prevent flooding of the PWS pump motors. To do so will in turn require a seismically qualified power source and the associated instrumentation and controls.

B.3.3.3 Heat Sink

The heat sink is water pumped from the river, stored in a pond and pumped to the reactor building, and returned to the river via the sump. Upon loss of river water pumping, cooling water can be pumped from the sump back to the pond. Concern over potential loss of AC power to the recirculation pumps is resolved by the installation of diesel generators for the pumps and the availability of gravity-fed cooling for 8 h. Coolant flow can be controlled by manual valve operation and CWS status can be monitored visually.

B.3.3.4 Confinement

The confinement systems and their instruments and controls are not seismically qualified. For the startup phase, emphasis will be placed on shut-down and core-cooling functions to ensure that no event escalates to the point of requiring the AACS. In the longer term, however, the confinement systems, including their supporting electrical, instrumentation, and control systems, should be seismically qualified.

B.3.3.5 Process Water System Inventory

The PWS inventory will be effectively monitored by the reactor vessel level measurement discussed in the core-cooling function. The MRS is being seismically qualified to return the moderator so as to restore the PWS fluid lost from small leaks. Naturally, the electrical power, instrumentation, and control systems should be modified to be consistent with this purpose. The SRP intends to provide power from the planned DGs. If PWS inventory loss is too great, ECS is initiated. The SRP safety analyses do not assume a loss of PWS coolant coincident with a loss of normal and emergency power or a seismic event. Hence, the existing methods of initiating ECS are adequate.

B.3.3.6 Recommendations

- Provide redundant seismically and environmentally qualified methods of monitoring certain essential parameters to show subcriticality and decay heat removal. A suggested list of instruments includes monitors for neutron flux, reactor tank level, process water pump operation, and 105 Building sump water level. Evidence that the reactor is subcritical and that decay heat removal is continuing must be available for water flooding or any credible fire (see recommendation Essential Core Monitoring).
- For startup, show that spurious operation of the PWS valves will not occur from a fire or seismic event, including consideration of relay chatter. For the longer term, show that ECS will not be actuated by fire or a seismic event or

that spurious operation is recoverable without threat to core cooling (see recommendation Spurious Controls Operation).

B.3.4 HUMAN INTERFACES

B.3.4.1 Control Room Process Data Display

The SRP control room does not have a safety parameter display system. However, the computer/CRT display system that performs the diagnosis of multiple alarms (DMA) was designed to reduce, if not eliminate, alarm avalanching during major events. But the DMA analysis covers only those alarms related to the loss of process D₂O or secondary side cooling water. There is no centralized place for displaying the bypassed and inoperable status data [Nuclear Regulatory Guide 1.47 (NRC 1973c)] or for monitoring compliance with technical specifications.

B.3.4.2 Procedures

No operator action outside the strict interpretation of the letter of the procedure is tolerated and very little such behavior on the part of the control room senior reactor operator is deemed appropriate. A significant group of people continually evaluates and revises the procedures, based partly on difficulties that the operating crew encounters with the existing set of procedures. It is impossible to anticipate and proceduralize all possible operating circumstances. However, given that modern computer technology has not been applied, this mode of operation probably is a safe one. The procedures often do not provide for contingencies; i.e., if a result called for by a procedure does not happen or if a process parameter is not available, the procedure often provides no guidance as to what should be done. As one retired SRP employee has noted, this heavy reliance on procedures has resulted in abnormal events in which the operators were properly executing the procedure, but were solving the wrong problem. Very few abnormal events are the result of a crew's incorrectly executing the correct procedure. The SRP is presently engaged in writing a set of symptom-based procedures for K Reactor.

B.3.4.3 Crew Structure/Organization

The SRP plants are typically operated with a five-man crew. The crew roles are as follows:

- Equivalent senior reactor operator who acts as the control room commander
- Reactor operator
- Fluid systems or balance-of-plant operator

- Shift supervisor who also performs the functions of the site manager on the back shifts
- Floating operator who fills in as needed.

This structure is consistent with commercial practice.

B.3.4.4 Control Room Layout

The SRP control rooms contain four primary workstations.

- A desk type of workstation for the control room commander. He has no controls or instruments, but is located with a good view of the entire control room.
- A seated workstation for the reactor operator, with reactor controls and a close-up view of a large mimic board showing the X-Y geometry of the core with control rod locations and various core parameters.
- A stand-up workstation for the fluid systems operator in front of a very large and complete mimic of the plant's fluid systems. This mimic board contains readouts of component states and process variables as well as the controls for those components. The mimic lines are color coded to reflect different fluid systems and are easily followed.
- An office workstation, called the fish bowl because it has glass walls. It is in one corner of the control room, manned by the shift supervisor, and provides a full view of the control room and its activities.

In general, the control room and board layouts seem to be well thought out.

B.3.4.5 The Remote Shutdown Room

At SRP the remote shutdown room is the control room of either of the other two reactors or a room in the Remote Shutdown Building, all of which contain REMACSS. The core of the REMACS displays is plant P&IDs with process data distributed in the displays. There is also a set of summary displays. Several of these can be made easily into some of the critical safety function displays, though not all of the critical safety functions are addressed. For example, REMACS does not include nuclear instrumentation or rod position in its data base as a means of monitoring subcriticality. Control is effected through the use of the REMACS keyboard in connection with the active display on the screen. Therefore, the large control board mimics have been reduced to several individual displays that can only be viewed one at a time. We were unable to see the REMACS in operation so did not assess whether or not this significant reduction in viewability has hampered effectiveness.

B.3.4.6 Safety Systems Configuration Control

A safety-management system for evaluating, prioritizing, planning, and dispositioning safety improvements on an ongoing basis, and for effective management of operation, requires that safety equipment be identified as such. Also, operations, maintenance, and design personnel need to be aware of the safety importance of the equipment being operated, maintained, or modified. This condition is especially true for safety equipment sensitive to single and common-mode failures. The SRP drawings or working documents reviewed by our subcommittee do not identify the overall scope (except by title) or boundaries of the safety circuits. Some of the safety-related system documentation we examined did not agree with the actual plant configuration. Some components are tagged as 'SCRAM INST' but there appears to be no established method or requirement to mark safety instrumentation, control, and electrical components or cabling either in the plant or in design documents.

There did not appear to be a structured, effective method to ensure that appropriate seismic and environmental qualification criteria are consistently applied to all modifications to safety-related systems. Design baseline documents should include the environment in which safety-related equipment and systems must operate for postulated design-basis events. The design verification process must ensure that the criteria have been applied consistently to any new analyses or modifications.

B.3.4.7 Recommendations

B.3.4.7.1 Instrumentation and Control Configuration Information.

Identify safety-related electrical, instrumentation, and control circuits and equipment on top-level schematics, P&IDs, instrument loop diagrams, control logic diagrams, and electrical single-line diagrams for the following: PWS, CWS, ECS, CWRSS, safety rods, control rods, SSS, leak-detection, shutdown monitoring instrumentation, EPS, primary reactor scram, and automatic backup shutdown. Work in this direction should be undertaken for startup (see recommendation Control Room Information).

B.3.4.7.2 Instrumentation and Control Human Factors.

- Develop a set of critical safety function status trees to link plant instrumentation with existing procedures for the critical safety functions. Suggested functions include subcriticality, core cooling, heat sink, confinement, and PWS inventory (see recommendation Control Room Information).
- Complete the development of symptom-based procedures for the critical safety functions and link with the critical safety function status tree (see recommendation Control Room Information).
- Add to and modify REMACS CRT screen displays to show a summary of the state or condition of the suggested critical safety functions and a

display for each of the critical safety functions showing the appropriate systems and equipment available to the operator to restore the function (see recommendation REMACS Displays).

B.3.4.7.3 Configuration Control. Review the configuration control system to ensure that critical drawings and design documentation are up to date and reflect actual plant configuration. Ensure that the design verification process provides for consistent application of appropriate separation, seismic, and environmental qualification criteria for all design changes (see recommendations Control Room Information and Configuration Control).

B.3.4.7.4 Safety System Identification. Identify (by tagging or marking) safety electrical, instrumentation, and control components, including transmitters and sensors, in the reactor plant (see recommendation Control Room Information).

B.3.5 SUPPORT SYSTEMS

B.3.5.1 Overall Site Electrical Power

Electrical power is supplied through an SRP area generation, transmission, and distribution system. The system receives power from multiple connections to 115-kV and 230-kV utility sources. Additionally, multiple generating stations in the SRP system provide sufficient power to achieve safe shutdown of reactors in the event that the utility sources become unavailable. Since the SRP reactors do not supply power to the grid, an upset condition at the reactor does not cause a grid perturbation, in contrast to similar circumstances at a nuclear generating station. There is considerable redundancy in the capability to supply power to the main substations at the reactors.

Two concerns require long-term consideration. First, cables that supply power from the main substation at each reactor site to the transformer rooms in the reactor building are direct buried and over 30 years old. To date, there have been no in-service failures. However, the uniform advanced age of the cables and their importance to normal reactor operation dictate a periodic test program. Second, maintenance of batteries has not included recommended industry practices. The recommendations of IEEE Standard 450 (IEEE 1987) should be applied to the maintenance of batteries supplying control power for the operation of the substations.

B.3.5.2 Emergency Power

As defined here, the emergency power system is comprised of the 1,200-kW GM DGs, their support systems, and the associated electrical distribution equipment. In the case of loss of electrical supply from the grid, the

emergency generators supply power to a great variety of loads that allow normal operation of plant equipment involved in achieving and maintaining normal safe shutdown of the reactor plant. There are some circumstances in which both DGs are required to supply all the loads assumed to be needed. Many loads now served from the emergency buses could be and are planned to be moved to a nonemergency bus. The ability to perform recommended tests on the DGs is limited. The DGs, auxiliary systems, and electrical distribution of the emergency power system have not been seismically qualified.

Two site projects are designed to enhance the ability to test the DGs, remove many nonessential loads from emergency buses, and annunciate system lineup problems that might otherwise go undetected. The subcommittee agrees with SRP's plans to complete these projects on K Reactor at the first opportunity after restart. Further effort will be necessary to show that the system will function after a seismic event.

Ability to operate the numerous components and systems served by emergency power is crucial to responding successfully to design-basis events and to many abnormal plant conditions. The absence of AC electrical power would severely hamper the operator's ability to assess plant conditions, would limit his options for response, and could lead to errors in execution with further risk to maintaining safe shutdown. The SRP safety analyses assume that most design-basis events will not occur simultaneously with a total loss of offsite power. We are concerned, however, over some scenarios that we feel to be credible.

Specifically, a seismic event could cause failure of piping systems and other unqualified systems coincident with a loss of offsite power. The 105 Building sump pumps would then have to operate to prevent flooding of the PWS pump motors. Seismic qualification and capacity upgrade of these pumps is discussed in other subcommittee reports (see Appendices B.1 and B.2, and recommendation Sump Water Removal Capability). A seismically qualified emergency power source with suitable redundancy must be provided for the sump pumps. The existing emergency power system could be upgraded to supply this power; however, other alternatives may be preferable. Except for the need to provide a seismically qualified power source for the sump pumps, there is no specific requirement for qualifying the emergency power system. However, because it is important to recovery from abnormal plant conditions, seismic qualification of the system should be considered as part of continuing improvements after restart as an ingredient in defense in depth.

B.3.5.3 Emergency Lighting

Emergency lights throughout the facility are now supplied from the 125-V DC station batteries and the GM DGs. It is already a restart prerequisite to add seismically qualified lights with an 8-h battery backup at specified locations. The lights are intended to allow operator response for actions necessary to achieve and maintain safe shutdown.

B.3.5.4 Batteries and Uninterruptible Power Supply

Numerous large and small batteries and UPSs, at least 14, provide backup power to essential power, control, and monitoring functions. Over 30 incidents in SRP reactors in the last 15 years have involved batteries. Maintenance performed on the lead-acid batteries has not included periodic capacity tests or intercell connection resistance checks, which are strongly recommended by Standard 450 (IEEE 1987) as important measures of a battery's ability to perform as expected. Load profiles and required capacities are not well documented for some of the batteries. These deficiencies are well recognized by the cognizant SRP engineers, and proposals have been made to institute the recommended maintenance.

Batteries and associated systems regarded as having a safety function are the 108 Building 125-V DC station battery, 105 Building rod equipment room battery, GM DG start battery, REMACS batteries and the UPS, and the exhaust fan emergency DG start and control batteries. These systems have not been qualified seismically and would require modification or possibly replacement to achieve qualification. However, since the systems served are not required to function after a seismic event, qualification of the batteries is not strictly required. For example, the safety computers are not seismically qualified because it is assumed that the seismic trip of the SSS accomplishes reactor shutdown.

B.3.5.5 Recommendations

- **Batteries and UPS.** Prior to restart, we recommend complete performance tests and intercell resistance checks per Standard 450 (IEEE 1987) for the following: 108 Building 125-V station battery; 105 Building rod equipment battery; GM DG start battery; REMACS batteries; and exhaust fan emergency DG start and control batteries (see recommendation Batteries and UPS).

- **Battery maintenance.** Review maintenance practices for all lead-acid storage batteries in terms of the recommendations of Standard 450 (IEEE 1987) and institute appropriate changes. Ensure that load profiles for all batteries are documented and compared against their rating. Ensure that practices for nicad or other nonstandard batteries provide a similar level of confidence in required performance (see recommendation Batteries and UPS).

- **Emergency power.** Maintenance and testing practices for standby diesel generators used for safety functions such as sump pumps, exhaust fans, ECS booster pump, and EPS should be compared to current industry guidance and modified as necessary. The upgrading of the EPS should be completed at the earliest opportunity. Verify that monitoring for operability of the standby DGs is adequately covered in technical specification surveillance (see recommendation Long-Term Seismic).

B.3.6 SUBCOMMITTEE ACTIVITIES

B.3.6.1 Savannah River Project Personnel Contacted

T. C. Gorrell, Reactor Technology
R. J. Moore, Reactor Technology
R. A. Allen, Reactor Technology
S. M. Revolinski, Reactor Technology
M. E. Bacinoglu, Reactor Technology
R. L. Salizzoni, Reactor Technology
T. M. Monahan, Reactor Technology
C. M. Schaumann, Reactor Technology
J. Falin, Reactor Works Engineering
W. D. Croft, Reactor Technology
W. H. Hearn, Reactor Technology
J. H. Hinton, Reactor Technology
C. E. Apperson, Reactor Technology
R. Murphy, Reactor Works Engineering
Tony Sealy, Reactor Works Engineering
J. Hardin, Power Technology
G. Youell, Power Technology
J. Janes, Westinghouse Transition Team
H. Allen, Operations
C. Mastromonico, Reactor Technology
K. L. Gimmy, Reactor Technology (retired).

B.3.6.2 Subcommittee Meeting Schedule

December 6-8, 1988, Savannah River, meetings with SRP personnel
December 20-21, 1988, Pittsburgh, PA, support committee meeting
January 5-6, 1989, Pittsburgh, PA, subcommittee working meeting;
joint meeting with Structure, Seismic, Materials subcommittee
January 17-20, 1989, Savannah River, meetings with SRP
personnel, K Reactor plant inspection
January 24-26, 1989, Pittsburgh, PA, support committee meeting,
coordination with other subcommittee members, subcommittee
working meeting
February 7-9, 1989, Savannah River, support committee
meeting, meeting with SRP personnel
February 21-23, 1989, Pittsburgh, PA, subcommittee working session,
support committee meeting.

B.3.7 BIOGRAPHICAL INFORMATION

R. M. BOGER

Mr. Boger, who is a Principal Engineer at the Westinghouse Hanford Company, was the subcommittee leader. He has had 18 years of experience in design, operation, and maintenance of nuclear reactor plants. He served in the U.S. Navy in the nuclear submarine program for six years and was qualified to serve as Engineering Officer. Since joining Westinghouse in 1976, he has worked as engineer and manager on DOE reactor facilities including the FFTF, N Reactor, and SP-100 Ground Engineering System Test Site. He holds a BS in electrical engineering from the University of Notre Dame and an MBA from the University of Washington. He is currently a member of IEEE Working Group 3.4 on Nuclear Plant Life Extension.

J. R. EASTER

Mr. Easter is a Fellow Engineer in the Westinghouse Nuclear and Advanced Technology Division. He has been employed in the commercial nuclear power sector for 24 years. He began his career at Westinghouse Electric Company working on the nuclear core design of the Southern California Edison San Onofre Nuclear Generating Station and continued in core design for 10 years, involved with subsequent core designs and the development of methods for analyzing, controlling, and monitoring core power distribution measurement aspects of the Westinghouse digital integrated protection system. An interest in improving operator understanding of such a system led to his working on the development of a new digital advanced control room. Mr. Easter has spent the last 10 years developing an understanding of the role of the operator in the control room and the tasks that he/she must perform, and in developing appropriate computer-based interfaces to help him/her do his/her job in a more effective and error-free way. He holds a BS in mechanical engineering from Stanford University and an MS in nuclear engineering from the University of Virginia. He is a registered professional engineer in nuclear engineering in the states of Pennsylvania and California.

P. J. MORRIS

Mr. Morris is Manager, Instrumentation and Control Systems Licensing, Westinghouse Nuclear and Advanced Technology Division, and has 15 years of professional experience in the nuclear power industry. He has been responsible for the design and evaluation of protection and control systems, plant transient performance analysis, and the startup of nuclear plants. He participated in the 1986-1987 Westinghouse N Reactor safety review. He has held managerial positions responsible for evaluation of the effects of degraded-core accidents, and, most recently, evaluation of the safety of all instrumentation, control, and

electrical systems. He holds a BEE degree from the Georgia Institute of Technology and an MSNS&E degree from Carnegie-Mellon University.

D. J. VOCHINSKY

Mr. Vochinsky is a senior engineer at the Westinghouse Nuclear and Advanced Technology Divisions and has 31 years of experience in the nuclear instrumentation and control field. He is presently developing integrated instrumentation and control systems for advanced light water reactor plants. He participated in the Westinghouse N Reactor safety review. He managed the Beaver Valley No. 2 control room design review. At the Westinghouse Advanced Energy Systems Division he was the FFTF reactor and vessel instrumentation system engineer. He was a systems integration engineer and the main control board design engineer on the CRBRP. At the Plant Apparatus Division for 14 years, he gained extensive experience providing instrumentation and control equipment for submarine and aircraft carrier reactor plants. He holds a BS in electrical engineering from Pennsylvania State University and is a registered professional engineer.

APPENDIX B.4 FIRE PROTECTION

**John R. Bell, Westinghouse Hanford Company Site Representative,
DOE-HQ/ES&H (lead)**

**Robert D. Lichfield, Principal Engineer, Westinghouse Hanford
Company**

B.4.1 SCOPE

We conducted an independent assessment of K Reactor fire protection consistent with the documented charter, scope, and approach established by and for the WISR Committee (see Appendix A.1). Criteria 1, 2, and 4 of Section I were used in assessing the adequacy of K Reactor fire protection.

Compliance with the DOE's mandated fire protection criteria relative to property damage and program interruption limitations was not assessed as part of this review, since these criteria are not directly associated with safety. Further, the review of life safety issues was limited in scope to plant and fire department emergency response personnel (i.e., actions that need to be taken or locations that must be occupied in the event of a fire emergency to ensure and maintain safe shutdown).

This assessment included review and evaluation of existing facilities, operating procedures, design-basis documentation (e.g., safety analysis of SRP reactor operation), and safety reviews and assessments performed by others, including Factory Mutual, Professional Loss Control, Inc., and DOE.

The NRC philosophy of protection for essential safety-related equipment, including fire protection or fire separation of redundant safety systems, was used in assessing the plant's ability to achieve and maintain safe shutdown. The National Fire Protection Association philosophy of protecting facility occupants from heat and combustion products in the event of a maximum probable fire (MPF) was used in assessing personnel safety.

Fundamental to this entire review is the concept of defense in depth. This concept, as applied to reactor plant fire protection, has three objectives: to prevent fires from starting; to detect rapidly, control, and extinguish promptly those fires that do occur; and to provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the safe shutdown of the plant.

B.4.2 GENERAL ISSUES

The SRP reactors have had an excellent fire loss record during their operating history, a record that testifies to the effectiveness of Du Pont's fire prevention program. The quantity of combustibles has been kept low by design,

and the plant procedures regulate the materials that are brought into the plant during maintenance periods.

The consensus of the subcommittee is that more emphasis should be placed on the entire defense-in-depth concept described above. Until now, little has been done to ensure prompt detection and control of fires. Furthermore, studies to show that the reactor can be safely shut down in the event of a fire have been rather superficial. However, efforts are under way now to improve fire detection and to provide firefighting capability.

B.4.3 SPECIFIC SAFETY ISSUES

B.4.3.1 Fire Hazard Analysis

Fire hazard analyses are incomplete for critical areas, systems, and equipment.

Findings.

- The reactor safety analysis report does not include a MPF as one of the design-basis accidents.
- The consequences of fire in any/all plant locations have not been identified in terms of maintaining the ability to shut down the reactor safely or the ability to minimize and control the release of radioactivity to the environment. Work has begun, however.
- An area-by-area analysis directed specifically at determining what fire detection, suppression, or separation is required to ensure the continued operability of systems, equipment, and structures that are important to safety has not been completed. For instance, a fire in the control room may force its abandonment. The fire could also make the REMACS inoperable. Therefore, there may be no way to monitor the minimum number of postshutdown instruments.
- The effect of a fire on the final charcoal filters (the AACS) has not been assessed adequately.
- The potential for inadvertent valve or pump operation in the PWS and ECS as a result of fire has not been addressed adequately.

Recommendations.

- Prior to startup, provide redundant methods of monitoring certain essential parameters. A suggested list is as follows (see also Appendix B.3):
 - Neutron flux monitoring or alternate means of verifying shutdown
 - Reactor tank level and PWS pump speed monitoring or alternate methods of verifying reactor circulation.

These activities must be separated and buffered so that a single fire will not result in the inability to monitor them (see recommendation Essential Core Monitoring).

- Either show that inadvertent PWS valve actuation does not occur or make provisions to prevent it. This procedure should be completed prior to startup (see recommendation Spurious Controls Operation).

B.4.3.2 Emergency Response Procedures

Findings.

- Detailed emergency response procedures have not been prepared to describe actions necessary to place the reactor in a safe-shutdown condition or to monitor the plant condition in the event of an MPF.
- Detailed pre-fire plans for use by the Savannah River Fire Department have not been prepared to address emergency response to a fire in the reactor plant.

Recommendations. Prior to startup, prepare procedures describing how the postshutdown instruments are to be read (see recommendation Essential Core Monitoring).

B.4.3.3. Life Safety Provisions

Findings. Life safety provisions may be insufficient to accommodate required emergency actions.

- Major stairways in the K Reactor complex are not enclosed with fire-resistant construction as normally required.
- Major stairways in the K Reactor complex do not discharge directly to the exterior of the facility as normally required.
- Travel distances to an exit are excessive in many areas of the plant.
- Emergency lighting has not been provided in the plant, but is planned prior to startup.
- Floor-to-floor separation (i.e., fire-rated construction) does not exist in the plant to allow for safe egress from the facility in the event of a fire.
- Not all areas of the plant have two separate means of egress as normally required.

Recommendations. See Section B.4.3.6 below.

B.4.3.4 Water Supplies

Findings.

- No fire hydrants exist within the K Reactor perimeter security fence.
- Only one fire hydrant (with a very marginal supply capability) is accessible to the reactor plant, and its use requires several hundred feet of hose

to be laid by hand through two security gates. Additional water supplies will be provided within the fence as part of the K Reactor startup program.

- There are no fire water standpipe systems in the reactor plant (this situation will be corrected by startup).

Recommendations. See Section B.4.3.6 below.

B.4.3.5 Defense in Depth

Findings.

- There is no management system in place to ensure an independent fire protection review of safety issues and documentation and to ensure appropriate closure of these issues.
- There is no structured system for conducting, on a periodic basis, fire protection engineering surveys of the reactor plant.

Recommendations. See Section B.4.3.6 below.

B.4.3.6 Fire Protection Overview Program

Findings. Defense in depth is lacking.

- There are no fire protection surveillance (of the technical specification type) requirements.
- Automatic rapid detection and suppression systems are lacking throughout the plant.

Recommendations (see recommendation Fire Protection Program). Establish a long-term formal fire protection overview program to ensure that the following are accomplished:

- That area hazards analyses are made
- That fire protection surveillance requirements are in place
- That fire suppression systems are installed where appropriate
- That life safety provisions are considered
- That passive fire protection features are provided where beneficial.

B.4.4 MEETINGS AND INTERVIEWS

Date	Subject	Attendees
1/9/89	K Reactor fire protection for critical safety-related systems and equipment	Walt Futrell, Nuclear Utilities Services Corporation (NUS) Dario Luna (DOE-SR) George Rudy (NUS) Joey Aloieri (NUS) Tim Myers (DOE-SR)
1/10/89	K Reactor walkdown	Walt Futrell (NUS) Dario Luna (DOE-SR) Gary Borba (DOE-SR) Bob Wheeler (Du Pont) Shift Operations Supervisor (Du Pont)
1/11/89	Professional Loss Control, Inc. (PLC) reports	Dario Luna (DOE-SR) Walt Futrell (NUS) Gregg Morgan (DOE-SR)
1/12/89	K Reactor walkdown	Bob Wheeler (Du Pont) Ken Keaton (Du Pont) George Rudy (NUS) Joey Aloieri (NUS) Mark Nelson (Du Pont)
1/13/89	Exit briefing	Tim Myers (DOE-SR) Gary Borba (DOE-SR) Dario Luna (DOE-SR) Tom Harris (Du Pont)

Interviews were conducted with the following:

Walt Futrell	NUS
George Rudy	NUS
Dario Luna	DOE-SR
Gregg Morgan	DOE-SR
Tim Meyers	DOE-SR
Gary Borba	DOE-SR
Bob Wheeler	Du Pont
Tom Harris	Du Pont
Ray Jewell	Du Pont
Dave Trinkler	Du Pont
Ken Keaton	Du Pont
Mark Nelson	Du Pont.

B.4.5 BIOGRAPHICAL INFORMATION

J. R. BELL

Mr. Bell is currently a Westinghouse Hanford Company site representative at DOE-HQ/ES&H. He has 20 years of experience in the fire protection field. He received his BS in fire protection engineering from the University of Maryland and then joined the AEC as a fire protection engineer. He worked for the U.S. Navy and General Services Administration as a safety and fire protection engineer, reviewing the design, construction, and operation of government and naval shore facilities. With Westinghouse Hanford Company he has had assignments as senior engineer and as staff manager providing industrial safety, industrial hygiene, fire protection, and emergency planning services. His most recent position was Manager, Industrial and Fire Protection, Westinghouse Hanford Company. He is a registered professional engineer in fire protection in California.

R. D. LICHFIELD

Mr. Lichfield is a principal engineer at the Westinghouse Hanford Company and has 15 years of experience in the fire protection field. He has BS degrees in occupational safety and health and in aeronautics, both from Utah State University. His current responsibilities include independent review of all fire protection systems/components of existing facilities and those under construction/startup to ensure that an improved risk level of fire protection is maintained. Assignments have required a direct interface with major A/E firms in the conceptual and definitive design of major DOE facilities (FFTF, maintenance and storage facility, fuel cycle plant, and related structures). He has been a cognizant system design engineer responsible for design, construction, and testing of fire protection systems for the FFTF. Currently, Mr. Lichfield is a member of the National Fire Protection Association and the Hanford Fire Protection Engineer Forum.

APPENDIX B.5 CORE DESIGN

Ronald D. Coffield, Fellow Engineer, Westinghouse Nuclear and Advanced Technology Division

Richard A. Doncals, Manager, Nuclear Design, Advanced Energy Systems, Westinghouse Nuclear and Advanced Technology Division

Allan F. McFarlane, Manager, BWR Technology, Westinghouse Commercial Nuclear Fuel Division

Hans Toffer, Manager, Thermal Reactor Physics, Westinghouse Hanford Company

B.5.1 SCOPE

The Core Design subcommittee was charged with examining reactor-initiated incidents such as inadvertent control rod motion, the FI phase of the LOCA, potential fuel-handling accidents, and the calculation of reactor parameters for use in safety analyses. We covered methods, validity of input, conservatism, and organizational process. We focused on the K Reactor and the Mk22 assembly.

B.5.2 FINDINGS

Table B.5-1 displays the subcommittee's conclusions that the SRP reactors meet the NRC's *General Design Criteria* (NRC 1988b) for the reactor core in almost all cases. Sections B.5.2.1 and B.5.2.2 provide further detail on temperature coefficients and the reactivity effects of fuel redistribution. The need for a dropped partlength rod analysis has been addressed by the Safety Analysis subcommittee (see recommendation Part Length Rod Drop).

The subcommittee found the Du Pont staff to be competent and equipped with good analytical procedures. Exceptions in the area of analysis procedures (beyond predicting core performance in the ECS phase of the LOCA, which was the subject of the Power Limit and Accident Propagation subcommittee) are incorporation of FI methodology in accident analysis generally, and prediction of assembly flow during the FI phase of the LOCA. The whole LOCA issue is currently so much in the limelight at Savannah River that the subcommittee felt its attention was better focused elsewhere. Some independent calculations were done, however, to assess the impact of the updated safety rod worth and insertion rates and to estimate the sensitivity of acceptable power level to the forecasted assembly flow (see Section B.5.2.3). It would seem reasonable that a 40% reduction in flow (following the instantaneous double-ended break of an inlet pipe) would be more than compensated by a 50% reduction in initial operating

Table B.5-1. Evaluation of K Reactor in Terms of General Design Criteria.*

- #10...Margin to ensure that fuel design limits are not exceeded during normal operation, including operational occurrences.
We believe that the plant will meet this criterion.
- #11...Net effect of the prompt inherent nuclear feedback characteristics tends to compensate for rapid increase in reactivity. There is a prompt positive reactivity coefficient. It is small and is overcompensated for by the negative moderator coefficient in a few seconds (see Section B.5.2.1).
Considering the potential rate of reactivity insertion, we believe that this criterion is met.
- #12...Design to ensure that power oscillations can be reliably and readily detected and suppressed.
We believe that successful operation to date demonstrates that this criterion is met.
- #13...Instrumentation shall be provided...to ensure adequate safety. Appropriate controls shall be provided.
We believe that this criterion is met.
- #25...Ensure that fuel design limits are not exceeded for a single malfunction of the reactivity control system.
We conclude that this criterion is met.
- #26...Two independent reactivity control systems should be provided...allowance for stuck rods...capable of holding the core subcritical.
With both the control rod system (control rods and safety rods) and the Ink system, this condition is met.
- #27...Reactivity control systems designed to ensure that...under postulated accident conditions...the capability to cool the core is maintained. Under severe-accident conditions there is a (remote) potential for fuel to reconfigure and significantly increase reactivity. This situation deserves continued study under the severe-accident program (see Section B.5.2.2).
We believe that there is a high probability that this criterion will be met.
- #28...Limits on rate of reactivity increase to ensure neither pressure boundary yielding nor core disturbance...rod dropout...
The drop of a part length rod from a high-reactivity worth position would result in a significant reactivity addition; the associated reactor transient should be analyzed.
Pending the outcome of the above analysis, we conclude that this criterion is met.
- #29...Control systems...extremely high probability of performing their functions in the event of anticipated operational occurrences.
The major issue is seismic and is addressed elsewhere.

*10 CFR 50, App. A (NRC 1988b).

power. But the 40% reduction is a core average and some assemblies will have substantially larger flow reductions; consequently, a detailed analysis is required. The analyses carried out by SRL would provide such information, but were not available for the Mk22 core and updated rod worths. The effect of the more conservative safety rod value is discussed in Section B.5.2.4.

Section B.5.2.5 discusses the results of our review of refueling operations; several concerns remain but the long history of safe operation (many thousands of hours of trouble-free operation) provides a basis for putting remedies in the lower priority category.

Section B.5.2.6 describes the results of a review of accidents listed at SRP. In general, a higher level of conservatism would be appropriate. These accidents are not expected to limit power, but an analysis should be on record confirming that scram set points have been appropriately set (see recommendation Safety Margin Evaluation).

The input to prior safety analyses showing the results of various accidents to be acceptable should be clearly documented so that changes can be properly evaluated in subsequent core designs. The subcommittee found that safety analyses generally had been done for any safety issue raised, but the analyses often dated back 10 years or more, and the important assumptions were not being routinely reexamined to ensure continuing validity. Recommendations to prepare a checklist of safety parameters and to establish expeditiously an FSAR close to today's standards have been incorporated by the Safety Analysis subcommittee (see recommendation Safety Documentation).

Fuel and target manufacturing specifications call for certain values of grams of ^{235}U per foot, grams of lithium per foot, ratio of ^{235}U loadings in inner and outer fuel tubes, maximum-to-average and minimum-to-average loadings of ^{235}U and lithium along the length of the target and fuel tubes, and fuel tube azimuthal variation in loading. In addition, the intended core location of a particular assembly is known to manufacturing because different locations require different lithium loadings. A tour was made of the manufacturing facilities, and discussions were held with manufacturing and analytical personnel regarding deviations in specified parameters. A study is under way at SRP to determine the appropriate allowance for manufacturing deviations, but the conclusions are not yet in hand. The results of this study can be used for a routine allowance; however, the adequacy of the allowance should be reconfirmed for each charge. Moreover, the allowance for deviations from nominal parameters must recognize the potential for fuel and targets to be outside their specified limits (see recommendation Fuel/Target Manufacturing).

There has been a long history of good performance with the Mk22 assemblies and the SRP reactors in general. This fact has been both an objective and a subjective factor for the subcommittee in reaching its conclusions. Changes in manufacturing (or other parts of the overall safety assurance system) should be examined carefully to ensure that the excellent safety record at SRP is not compromised. The recent change from 80 wt% ^{235}U fuel to 66 wt% ^{235}U

fuel and the plans to alter the use of the nuclear test gauges should be carefully examined for their potential impact on core design parameters (see recommendation Fuel/Target Manufacturing).

B.5.2.1 Temperature Coefficient Assessment

Changes in fuel assembly dimensions and heavy water content occurring during operation are related to absolute reactivity through temperature coefficients. The inherent nuclear characteristics of an Mk22 core are driven by the reactivity feedback from the fuel assembly (called the coolant coefficient) as well as the moderator region (moderator coefficient). The moderator temperature coefficient has been demonstrated to be always strongly negative and quite large when compared to the coolant coefficient. However, at start of fuel life, the coolant coefficient is small and could be positive.

The coolant coefficient consists of reactivity feedbacks from both density and dimensional changes of the fuel, target, and coolant regions as well as the temperature change of the fuel (Doppler). To provide some insight on the accuracy of these predictions, SRL provided models and temperature changes that permitted similar evaluations to be performed by the Westinghouse Advanced Energy Systems Department and the Westinghouse Hanford Company for the coolant density change in the fuel assembly as well as the Doppler contribution of the fuel tubes. In addition, a model was supplied that permitted the moderator coefficient to be calculated.

Table B.5-2 shows a comparison of these predictions by the participants of this review. Similar comparisons were made for the Mk22 coolant temperature coefficient (Table B.5-3). Further, a coefficient experiment performed by SRL in 1962 was analyzed. While the reactor was operating, approximately 4 cents of positive reactivity was inserted in about 0.075 s. The response was a prompt jump in power of approximately 4% followed by a slower increase of about 3% over 4 s, followed by a decrease in power as the negative moderator coefficient took effect. The corresponding coolant temperature coefficient was $+1.7 \pm 0.5 \times 10^{-5} \Delta K/^{\circ}C$ calculated for this test, while the moderator coefficient was $-11 \pm 2.0 \times 10^{-5} \Delta K/^{\circ}C$.

Thus it is concluded that SRP should use a more positive initial coolant temperature coefficient in its transient analysis than that used in past practice. Likewise, depending on which is most limiting for a particular transient, positive or negative uncertainties should be considered for both the coolant and moderator coefficients (see recommendation Safety Margin Evaluation).

The moderator temperature coefficient is always negative and quite large when compared to the coolant coefficient. At the start of fuel life, the coolant coefficient could be slightly positive. However, as exposure progresses, it becomes negative after about one fourth of the cycle length. Consequently, during approximately three fourths of the cycle, compliance with criterion 11 is easily demonstrated.

To demonstrate compliance with this criterion in the early part of the cycle, one must examine the magnitude and timing of the two coefficients. The experiment analyzed above indicated that the coolant coefficient had a time constant of about 0.3 s, while the moderator coefficient responded after approximately 2 s.

Table B.5-2. Savannah River Plant Benchmark Calculations (Mark 22 Temperature Coefficient Predictions, $\Delta K/^{\circ}\text{C}$).

	Coolant density	Fuel (Doppler)	Moderator density
Savannah River Plant prediction	-2.9×10^{-5}	-0.36×10^{-5}	-4.8×10^{-5}
Advanced Energy Systems prediction	-3.3×10^{-5}	-0.20×10^{-5}	-5.7×10^{-5}
Westinghouse Hanford Company prediction	-3.1×10^{-5}	-0.2×10^{-5}	-6.5×10^{-5}

Table B.5-3. Mark 22 Temperature Coefficient (BOL*) ($\Delta K/^{\circ}\text{C}$ Coolant).

	Savannah River Plant	Advanced Energy Systems	Westinghouse Hanford Company
Nominal calculated value	-2.4×10^{-5}	$+1.0 \times 10^{-5}$	$+0.6 \times 10^{-5}$
Experimental bias	$+2.4 \times 10^{-5}$	0.0×10^{-5}	0.0×10^{-5}
Experimentally corrected value	0.0×10^{-5}	$+1.0 \times 10^{-5}$	$+1.0 \times 10^{-5}$
Limited value	$+1.0 \times 10^{-5}$		

*BOL - Beginning of Life.

On reviewing the accidents at SRL, it was concluded that the worst credible reactivity addition rate during power operation would be due to a gang rod withdrawal, which could insert approximately +1.4 cents/s. The relatively slow rate is much less than the 4 cents in 0.075 s inserted in the 1962 tests. In addition, the transient resulting from a dropped part length rod should be assessed conservatively by SRP prior to drawing a final conclusion on whether the intent of criterion 11 is satisfied (see recommendation Part Length Rod Drop).

B.5.2.2 Parametric Reactivity Studies of Degraded Heavy-Water-Reactor Core Geometries

To assess the magnitude of potential reactivity insertion following fuel redistribution, parametric criticality calculations were performed. In one scenario, the entire fuel content of an Mk22 assembly is assumed to melt and condense to a solid mass of fuel that blocks the coolant tube and is surrounded by the moderator. In the other scenario it is assumed that molten fuel particles are swept into the moderator regions by the coolant flow. Other calculations showed that an isolated molten fuel slug from a single assembly is not a reactivity concern, and that lumping one assembly's fuel into the center or bottom of the assembly tube--targets intact--reduces reactivity by about 60 cents.

Calculations were then performed to evaluate slumping of multiple fuel assemblies. In the analysis, both the fuel ring and the associated aluminum cladding were assumed to melt and slump to a solid cylinder within the coolant tube, just below the original active core. The model then has 33 in. of solid fuel and aluminum inside the assembly tubes. It was assumed that the tubes remain intact; therefore D₂O surrounds each slumped assembly. The target rings remain intact but they are above the molten fuel, not comingled with it. An infinite lattice of this geometry yielded an eigenvalue of 1.41 compared to the base (unmelted) eigenvalue of 1.10. This large delta K was confirmed using a three-dimensional Monte Carlo computer code calculation (MCNP) and a very similar core configuration. Results are tabulated in Table B.5-4.

Fuel melting could cause fuel particles to be swept into the moderator region by the coolant flow. If this were to occur, fuel could possibly be distributed through the moderator region of several fuel assemblies. Figure B.5-1 illustrates the reactivity of HWR fuel as a function of dilution in D₂O. At a fuel volume content of 0.1%, the system k_{eff} is 1.09. This dilution is equivalent to dispersing the Mk22 fuel in four adjacent moderator regions. Clearly, fuel particle dispersal represents a potential for positive reactivity insertions (see Appendix B.9, however, for a discussion of the likelihood of not achieving dispersion).

Savannah River currently has a severe-accident assessment program in progress, and studies of criticality increases from fuel redistribution are a necessary part of that program.

B.5.2.3 Margin to Onset of Significant Void Criterion

This study was performed to help assess the margin to the OSV during the FI phase of a large-break LOCA. Of particular interest was the sensitivity of the results to key parameters such as localized subchannel flow rates, heat fluxes, coolant inlet temperature, and coolant pressure, including appropriate allowances for uncertainties in the data and analytical models.

To ensure that significant voiding will not occur, the Saha-Zuber correlation method is being applied with appropriate uncertainties such that

Table B.5-4. Reactivity Changes Associated With Fuel Melting.

Assembly Scenario	k_{eff}
Individual Mk22 assembly (infinite D ₂ O reflector)	0.49
Individual slumped Mk22 assembly (infinite D ₂ O reflector)	0.56
Infinite lattice of intact assemblies	1.10
Infinite lattice of slumped assemblies	1.41
Full 3D MCNP (base) - NPR	1.16
Full 3D MCNP with 49 slumped assemblies	1.50

78904044.7M

Figure B.5-1. Reactivity Impact of D₂O Dilution on a Single Molten Mark 22 Assembly (Masses=3.2 kg ²³⁵U, 0.92 kg ²³⁶U, and 0.72 kg ²³⁸U).

$$h_{\text{local}} < h_{\text{sat}} - 22 \frac{q''}{G}$$

where

h_{local} = local coolant enthalpy

h_{sat} = slumped assembly tube coolant enthalpy

q'' = heat flux (Btu/h•ft²)

G = coolant mass flux (lb/h•ft²).

To assess how much margin exists relative to this criterion, a series of calculations was performed on a quasi-steady-state basis using the power and flow conditions shown in Table B.5-5 and assuming that the reactor was operating at 50% of full power and 100% flow initially. Results from the analyses performed are given in Table B.5-6, where it is shown that although some margin to the Saha-Zuber criterion exists using global best-estimate type of conditions, this margin can disappear quickly when local power and flow effects and uncertainties are considered. Also, relative to the sensitivity of the results to key parameters, it was found that the reactor inlet temperature has a very significant impact on conclusions relative to the Saha-Zuber margin since it has a direct additive influence on local coolant temperature; and flow uncertainties are about 1.5 times more detrimental than power uncertainties because of their effect on coolant pressure and consequently on coolant saturation temperature.

This high sensitivity to flow points out the need for accuracy in predicting local assembly flow following the break, currently an area of uncertainty in the SRL calculation.

B.5.2.4 Reactor Power Response Relative to Scram Worth and Speed of Response

The purpose of this study was to evaluate the SRP reactor transient for the first several seconds of a large-break LOCA. A rapid decrease in reactor power is particularly important considering the abrupt reduction in flow resulting from this accident. Scram worths shown in Figure B.5-2 were used for the safety rod insertion using worst-case and best-estimate assumptions; step insertion worths of 0.2% and 0.5% (assuming a 0.1-s delay) were used for the ³He injection. Results are shown in Figure B.5-3. Here it can be noted that about a 0.25-s larger period is needed to reach 60% power for the worst-case scram (Case A) versus the best-estimate scram (Case B) of the safety rods. Put another way, at the time when the power would have fallen below 50% using the best estimate curve, the power would still be over 80% using the conservative Case A curve. Also, the beneficial effect of using the ³He injection system during the first second of the transient can be seen (note that the ³He system is not currently in

Table B.5-5. Conditions Assumed for Onset of Significant Voiding Calculation (Flow Instability Phase).

Type of assembly:	Mark 22
Core inlet temperature:	113°F
Core outlet temperature:	166°F
Peak heat flux:	166, 667 Btu/h•ft ²
Axial power shape:	End of cycle (saddle)
Coolant pressure at hot coolant position:	46 lbf/in ² (absolute) (normal) 26 lbf/in ² (absolute) (accident)
Outlet plenum pressure:	28 lbf/in ² (absolute) (normal) 19 lbf/in ² (absolute) (accident)
Full-flow local mass flux:	5.9 x 10 ⁶ lbm/h•ft ²

Table B.5-6. Estimates of Margin to Onset of Significant Voiding During Flow Instability Phase.

Condition	Margin to onset of significant voiding
<u>Case A</u> Best Estimate—no uncertainties or local flow effects	+21°F
<u>Case B</u> Case A with flow at 40% as opposed to 60% to account for local flow effects/uncertainties	-44°F
<u>Case C</u> Case A with 20% increase in power to account for local power effects/uncertainties	+3°F

78904044.5M

Figure B.5-2. Savannah River Plant Mark 22 Scram Reactivity Curve.

78904044.8M

Figure B.5-3. Scram Action with and without ^3He (Westinghouse).

place, nor has the committee concluded that it is necessary. It is introduced here because calculations assuming its presence give illustrative results).

A conclusion from this study is that reasonable agreement would be obtained between the Du Pont and Westinghouse transient power calculations for the first 1.2 s of a LOCA transient (FI phase) if the same conditions are assumed. The magnitude of the differences in rod worth reinforce the subcommittee's conclusion that regular methods confirmation by startup testing is essential (see recommendation Startup Core Testing).

B.5.2.5 Refueling Considerations

The SRL has designed special hardware modifications to lessen the probability of charging fuel into target positions. In addition, an improved system of six in-core detectors has been installed to monitor reactor status during reloading. A computer system controls operation of the refueling machines. This system is able to differentiate between fuel and target assemblies; it can also stop the refueling machines if the wrong type of assembly is being charged. In addition, refueling operations are terminated if vacated positions are not refilled as specified.

The reactor operators must stop operations if the neutron flux increases by a factor of 1.5 after charging an assembly or by a factor of five in any eight-hour period. In addition, the SSS must be tripped if the flux should double. We still have some concerns about this refueling procedure.

- Flux is monitored in the central control room, not the crane control room, with voice communication between the two. This situation introduces a potential for human error.
- There is no interlock between the cranes and the flux detectors to provide an automatic halt to operations.
- The SSS trip is manual, and the Ink injection is relatively slow.
- The 3% shutdown margin is smaller than the 5% in commercial PWRs.
- In the event of criticality during refueling, the speed with which the incident can be stopped is dependent on human reaction time (involving two operators) and the injection speed of the Ink.

Typical practice in the commercial nuclear industry is that an alarm in the containment and the main control room is coupled to the source-range channel. This alarm automatically alerts the loading operators to an indication of high count rate and requires an immediate stop of all operations until the situation is evaluated by plant personnel and technical advisors.

The refueling procedures have the potential to challenge the safe-shutdown condition of the reactors. The primary concern is that the speed with which an assumed refueling accident can be terminated is dependent on human reaction times (involving two people) and the injection speed of the Ink.

At a minimum during refueling, an annunciator (bell or alarm) should be installed that is activated by the neutron flux level (or operator) and that indicates immediately to the crane operator that the refueling step just performed has violated a safety criterion. A report should be issued that documents the procedures, instrumentation, and criteria used to ensure that criticality is not achieved during refueling (see recommendation Refueling Operations).

B.5.2.6 Assessment of Safety Analysis Report Chapter 15 Events

A review of SAR Chapter 15 events was performed to examine the need for required updates based on current SRL analysis:

- Single and ganged rod withdrawal concerns
 - Temperature coefficients have been updated (more conservative) recently for the Mk22 lattice, which will adversely affect the rate of power increase.
 - No quantitative documentation of the AA3 computer code evaluation of shutdown by the SSS is available.
 - Axial power profiles should be calculated for the accident sequence.
 - Inadvertent insertion of a part length rod has not been analyzed for the Mk22 charge.
- Full length and part length rod mispositioning--If a control rod is slightly mispositioned with respect to the other rods in the gang, the power will be slightly tilted. This situation will be detected by the assembly temperature monitors and will result in a scram upon a temperature rise of 5°C. This event is certainly bounded by the single rod withdrawal accident.
- Loss of coolant from pipe break. See Sections B.5.2.3 and B.5.2.4.
- Pump shaft break--Based on operating limits set by the LOCA, the coolant temperature is expected to be 30°C lower than that used in the analysis, a situation that leads to the conclusion that boiling should not occur. The margin to temperature dt saturation will be reduced with the updated temperature coefficients and safety rod worths.
- Loss of D₂O pump power--Previous analysis of this transient during full power operation indicated only a 5°C maximum coolant temperature rise for a safety rod scram. This event is clearly bounded by the pump shaft break.
- Rotovale closure--Maximum temperatures will be significantly lower for the operating power dictated by the LOCA. This event is bounded by the pump shaft break.
- Flow reduction in a single assembly
 - Analysis of this event (either loss of target or loss of fuel) in an Mk22 assembly has not been reported and may be more severe.
 - It is not clear that the most conservative (most reactive) molten fuel configuration has been considered.

- Loss of cooling during or after discharge--Engineered safeguards and accident analysis appear to be adequate.

B.5.3 SUBCOMMITTEE PROCESS

Information was gathered from the following sources and refined in active subcommittee and committee discussion:

- Presentations to the full committee and subcommittee by Du Pont personnel
- Several full-day discussions with various Du Pont personnel, aimed at understanding the details of analytical methods and processes in the area of reactor physics, charge design, and LOCA modeling
 - Facility tours of K Reactor, thermal-hydraulic test laboratory, and fuel/target fabrication plants
 - Review of numerous safety analysis reports
 - Independent calculations (described above).

The information was assessed using the criteria in Title 10, CFR Part 50 (NRC 1988a), relevant NRC documents, and the extensive experience of the subcommittee members. Two areas of difficulty encountered were those presented by the absence of safety documentation typical of commercial nuclear power and by the high rate of change in the status of thermal-hydraulic modeling.

B.5.4 BIOGRAPHICAL INFORMATION

R. D. COFFIELD

Dr. Coffield is a Fellow Engineer in the Westinghouse Advanced Energy Systems Department of NATD with over 24 years of experience in the fields of fluid flow and heat transfer. As lead engineer in thermal and fluid systems engineering, he has been responsible for various transient thermal-hydraulic and nuclear kinetic analyses for design and safety evaluations relating to numerous reactor concepts including liquid metal reactors (LMRs), PWRs, HWRs, and fusion reactors. Dr. Coffield has either authored or coauthored over 75 open literature publications as well as a textbook in the area of thermal hydraulics. He has a BS, MS, and PhD in mechanical engineering and is a registered professional engineer in the state of Pennsylvania.

R. A. DONCALS

Mr. Doncals has over 30 years of experience in the design and analysis of light water, gas-cooled, and liquid metal reactors. In his current position as Manager, Nuclear Design, Advanced Energy Systems, Westinghouse Nuclear and Advanced Technology Division, Mr. Doncals has overall responsibility for the nuclear analysis and design of defense materials production reactors,

lightweight nuclear power plants, advanced LMRs, and other advanced reactor concepts. Mr. Doncals holds a BS (1955) and an MS (1959) from Carnegie-Mellon University in mechanical engineering. Early in his career, he made significant contributions to the development of the NERVA rocket engine as both an engineer and a manager. Prior to his current position, he was manager of nuclear design in the CRBRP. In this position, he contributed significantly to the acceptance of the heterogeneous core in the CRBRP as well as to other U.S. designs. One facet of his current position is the lead coordination responsibility for the critical experiments being performed at the Argonne National Laboratory in support of the SP-100 project. For many years he has been a member of the U.S. Working Group on LMR Foreign Core Physics Exchanges. Mr. Doncals has 38 publications in the field of nuclear engineering.

A. F. McFARLANE

Dr. McFarlane has 20 years of service with Westinghouse, most recently as the manager responsible for the licensing effort for BWR fuel. His experience includes three years in the Operator Training Department of the Nuclear Service Division and two years at the INPO. As manager of fuel projects for the Nuclear Fuel Division, he was responsible for the nuclear fuel contracts for a number of utilities. For approximately 12 years he was a manager of nuclear engineering, supervising nuclear, thermal, and hydraulic design for nuclear fuel for commercial PWRs. Born and educated in Scotland, his first employment was as a reactor physicist for naval nuclear propulsion reactors. Dr. McFarlane holds a BS (1955) and a PhD (1959) from Glasgow University, Scotland, and an MBA (1980) from the University of Pittsburgh.

H. TOFFER

Dr. Toffer has 25 years of experience at the Hanford Site as a manager and individual contributor. Prior employment includes low-energy experimental physics work at the Argonne National Laboratory and at the Ames Laboratory. His technical expertise and major accomplishments are in the area of reactor physics, production reactor technology, isotope production and application, criticality physics, reactor safety, instrumentation development, and new production reactor designs. He has been active in the ANS and the IEEE on both the local and the national levels. He was chairman of the writing group for developing national standards for criticality control and a lecturer for DOE/Argonne National Laboratory safety courses and has received best paper awards in reactor physics and remote systems technology. He has served on special safety review teams and national steering committees in the area of criticality control. Dr. Toffer holds a PhD in nuclear engineering from the University of Washington (1974), an MS in physics (Iowa State University, 1962), and a BS in physics from Muhlenberg College (1959).

APPENDIX B.6 CONDUCT OF OPERATIONS

**Dan J. Swaim, Operations Manager, FFTF, Westinghouse
Hanford Company**

**Keith D. Bonser, Manager, Technical Training, Westinghouse
Hanford Company**

**Richard C. Coulthard, Senior Engineer, Zion Training Center,
Westinghouse Nuclear Training Center**

**Lee S. Legowik, Manager, Engineering Document Control,
Westinghouse Hanford Company**

B.6.1 SCOPE

B.6.1.1 Configuration Control

The subcommittee conducted a review to determine whether the existing method of configuration control ensures that the operating configuration of K Reactor is accurately represented on drawings, in design documents, and in operating documents.

We reviewed the existing SRP procedures for configuration control and interviewed SRP personnel to determine the level of procedure understanding and the degree of procedure implementation and to identify concerns with the system. Criterion 4 of Section I was most applicable.

B.6.1.2 Training/Procedures

We focused on the present knowledge of personnel assigned to support a K Reactor startup and on the quality of training. We covered the training procedures for reactor operations, power operations, component handling, chemistry technician, radiation protection technician, maintenance, and emergency preparedness.

We made our observations in the classroom, in the simulator, and in the plant. We also conducted document reviews and personnel interviews.

The performance of the operations and key support staff is fundamental to the safe operation of the reactors. The operator has a role in each of the four criteria outlined in Section I.

B.6.1.3 Plant Operations

The subcommittee reviewed plant training materials and courses, operating and administrative procedures, engineering drawing control, and maintenance (work control) practices. The subcommittee interviewed a cross section of personnel and made workplace observations in addition to document reviews. Interviews were conducted in two ways: one-on-one discussions and group interviews in which several subcommittee members met with operating units consisting of a senior shift supervisor, shift supervisor, senior reactor operator, and reactor operator. The group discussions allowed anyone to contribute, add to, or correct any information presented by any of the operating staff. On some occasions the sessions were attended by area supervisors. The review efforts focused on the K Reactor, and in-plant walkthroughs were conducted at K Reactor. The subcommittee members believe that the issues identified are generic to the P, L, and K reactors and germane to restart efforts, but concur with the philosophy of a phased restart, concentrating on K Reactor.

B.6.2 GENERAL ISSUES

The subcommittee is well aware that the K Reactor organization is in a state of flux and that conditions in existence at this writing do not reflect the degree of training, the organizational structure, or the operating methods that will exist at the completion of the restart strategy actions now in progress. However, we feel that our observations of current conditions will provide useful guidance and midcourse correction to operations management. The performance of the plant staff is a key element in safe reactor operation and encompasses all four criteria of Section I. We believe that no amount of analysis, design, or overview can ensure safety in the conduct of operations without knowledgeable operators and effective line management. This statement of philosophy translates into an equally concise criterion for the acceptability of the conduct of operations: A strong and continually improving safety-management system must be in place and evident in the workplace culture. The Conduct of Operations subcommittee made a broad examination of the existing organization and the restart plans. We then applied our collective judgment to the acceptability of restart based on current practices and our perception of planned improvements. We looked for the following evidence of meeting the defined criteria:

- Demonstration of conservative operations philosophy
- Demonstration that safety is a line-management function
- Clear lines of authority and responsibility with the Operations

Department in charge

- Plant ownership by the Operations Department
- Plant operation conducted by appropriate, approved, well-thought-out procedures
- Constant self-evaluation and continual improvement

- Technical inquisitiveness and attention to details
- Appropriate configuration control, both in physical plant status and in engineering documentation
- A relentless desire for training
- Respect for radiation
- Emergency preparedness.

The subcommittee reviewed the current operations and the restart strategy action items and concentrated on areas where it appeared that additional work should be required prior to restart. It should be emphasized at this point that these recommendations are the team's judgment and not absolute statements as to safety or risk.

The following sections provide subcommittee findings on specific issues, divided between short term (prior to restart of K) or long term (decision to proceed should be made now, but implementation will continue beyond restart of K Reactor).

B.6.3 SPECIFIC ISSUES

B.6.3.1. Training and Procedures

Findings. The Reactor Operations staff consists of reactor operators (noncertified), senior reactor operators (certified reactor operators), shift supervisor (certified senior reactor operator), and senior shift supervisor (certified senior reactor operator). The training required for each level of qualification is less than that required by commercial nuclear industry standards with respect to time, quantity, and depth. We realize that the SRP reactors operate at lower pressures and temperatures and that the reactor support systems are not as complex as those of commercial nuclear facilities. However, the reactor core is complex and the operations personnel must understand and use more than 2,600 procedures.

The Center Section personnel are required to take and pass written, walkthrough, and oral examinations. The written examination practices have weaknesses. The examinations could easily be compromised, and the overall examination practice does not provide valid evidence of personnel knowledge. Improvements are planned.

The on-the-job training program shows similar weakness. The large number of signatures given in short periods of time were said to be a means of grandfathering. In some cases, the signatures were signed off after a period of training on the basis of exposure alone. The precise status of each case could not be determined from the records.

Interviews with five senior control room supervisors (all degreed), two shift supervisors (one degreed), and four reactor operator/senior reactor operator personnel showed significant weaknesses in emergency response and reactor

plant fundamentals. A training representative was present for some of the interviews. He confirmed that several pertinent knowledge areas are not taught and that the subject material given in restart training during the week prior to these interviews was not retained by the interviewees. The same level of restart training is given to all operators and had been given too quickly for adequate retention.

The senior shift supervisor is acknowledged as the person in charge of the plant. However, this person does not receive training commensurate with these responsibilities in areas outside the control room. Senior supervisors, if they are degreed, may enter a fast-track program requiring little experience or training in refueling operations, power operations, radiation protection, and laboratory section. The present program for such individuals does not allow them to operate plant controls. They are responsible for the coordination and execution of all plant activities including duties as the area emergency coordinator for plant emergencies. The restart training as defined by the November 1988 restart criteria (DOE 1988) does not adequately address the overall weaknesses in the long term. Only two of the eight human performance issues actually address upgrading operator knowledge, while three of the issues address placing on shift people with educational credentials but little SRP operating experience. In general, the restart criteria will adequately upgrade the engineering knowledge available on shift, but will not significantly upgrade the knowledge level of currently assigned personnel.

Component Handling Operations is a separately trained and certified group that performs fuel- and target-handling functions. The people who normally become component handlers come from the Center Section group. The evaluation process used by Component Handling Operations contains weaknesses similar to those found in the Center Section training. The present restart training does not include this group, which may be an oversight. The Component Handling Operations personnel control the refueling operation independently of the reactor control room. The two groups must communicate effectively with each other and should receive similar training.

Maintenance training appears to be the best organized and most highly developed training program among those reviewed. It is developed to provide initial, specialized, and continuing training for maintenance personnel and is nearing the completion of an accreditation process. Each candidate receives 12 weeks of structured training before being allowed to perform in the field. Three weeks of specialized training is required in addition for personnel located in reactor areas. The present experience level averages greater than four years.

The Health Protection Technician training program provides 10 weeks of basic training; however, neither further specialized site training nor continuing training is available. Examination and evaluation processes are generally weaker than in similar programs at commercial nuclear facilities.

Chemistry technicians are normally hired without prior experience. Recently the entry-level requirements were increased to help compensate for the

attrition and dilution of experienced technicians. These technicians perform a wide range of functions from laboratory work to operating the separations facilities. The training program consists of eight weeks of structured classroom and on-the-job training, which prepares personnel for laboratory functions. No other formal training is given.

The Power Operations Group provides electrical distribution and cooling water support to the reactor areas. This group is not part of the Reactor Operations Group and does not directly report to the control room senior supervisor. The experience level of this group is very low; approximately 50% of the personnel have less than one year of experience. The training program consists of nine weeks of basic training and six weeks of area training, half in the classroom and half on the job. The program does not integrate with the Center Section training even though Power Operations personnel control valves for ECS and provide electrical power to safety-related equipment.

A four-person staff handles the function associated with emergency preparedness. Four drills are conducted yearly, one jointly with the Vogtle Nuclear Plant. The control room senior supervisor is the designated area emergency coordinator and receives some training from the EP staff. The area emergency coordinator also coordinates the conduct of on-plant evacuation drills. The management personnel assigned to the emergency operations do not receive training. A reactor site may go for several years between drills. One area superintendent indicated that there were many new people assigned to his site who had not been part of a training drill.

Current nuclear industry standards require a broad base of fundamental understanding of theoretical and practical science and engineering principles as well as a detailed knowledge of plant operation and component specifics. This broad base of science and plant knowledge is acquired prior to supervised on-the-job training in the plant. Not only must personnel follow written procedures, but they are expected to know and understand the reasons for their actions and the expected consequences of the actions taken. The Du Pont philosophy has been that senior reactor operators are nontechnical personnel and do not need to know the basis of reactor core or plant operations. Operators were to respond and operate in accordance with written procedures. Knowledge and understanding of the underlying reasons for the actions required by the procedures were not considered important or required for the operator to successfully execute operating actions. This methodology is inconsistent with the lessons learned from Three Mile Island and other industry experience.

An extensive job and task analysis effort is nearly complete for certified operators. However, interviews with incumbents are performed under the assumption that such personnel are qualified and have the skills necessary to perform their jobs. The results of this analysis may substantiate the current level of training, but do not provide a basis for future improved training.

The current definition of an operational anomaly is "any event or condition that is different from what is normally expected." All operational anomalies

must be reported to DOE within 15 minutes of their occurrence. This broad definition and short reporting time are causing significant concern among operations personnel. The definition of what is to be reported is so broad that correct interpretation, short of a total running dialogue, is unlikely. During interviews, senior operators stated that they were having a problem "calibrating what DOE wants." The reportability problem has been a major concern in the press and between DOE and Du Pont. As a result of the recent incident on the K Reactor CWS, DOE now insists on being informed of all conversations between the senior supervisor on shift and his/her offsite supervision, except for personnel matters. A procedure has been developed to provide some guidance on what is reportable, but DOE has not concurred with this guidance.

Recommendation. Short-Term. The subcommittee does not consider the operational readiness review process adequate to show that the desired and necessary standards for performance have been achieved. An assessment team of peer line managers with proper standards should assess readiness to resume operation based on direct in-the-field observations of the operating and support organizations. Such an assessment should include an integrated emergency drill that results in escalation to a general emergency and extensively exercises most SRP support groups.

Several weeks prior to startup, the K Reactor plant management and WSRC operations upper management should perform a self-assessment to ensure that the personnel, the training, and all the other changes made during the prolonged shutdown are indeed effective and beneficial and that a new operating team has evolved. Demonstration of performance by drills and exercises in addition to observation should be required. It is imperative that line management make the decision that the operators and plant are ready for restart and not relinquish this responsibility to an overview agency. The subcommittee advises that such an assessment be made in a step-wise fashion (i.e., cold plant, fuel load, power ascension, etc.) with sufficient time for corrective actions should weaknesses be discovered (see recommendations Operational Assessment and Assimilation of Massive Change).

Recommendations. Long-Term. The WSRC should establish definitive goals for the level and depth of operator knowledge requirements. The philosophy of 'just follow the procedure' may be safe, but the committee does not believe it can result in excellent operation (see recommendations Operator Knowledge Requirements and Striving for Excellence).

Emergency preparedness training and drills for radiological events should be improved (see recommendation Operator Knowledge Requirements).

Useful guidance should be provided to the Operations Department on threshold levels for event reporting. The DOE's concurrence with the criteria will be required. The 15-minute criterion for event reporting does not allow adequate time for investigation. A new time limit should be negotiated with DOE. As an example, 10 CFR 50.72 (NRC 1988a) allows commercial facilities

up to one hour to review and determine critical events (see recommendation Event Reporting Criteria).

B.6.3.2. Procedures Upgrade

Findings. The Center Section Operations Group has about 2,600 procedures. Many of these procedures cover administration, nonoperational testing, cleaning, QA, charge and discharge, and other operations. We estimate that fewer than a third of these procedures actually affect operations in the control room during startup, power operation, or shutdown.

The procedures are formatted in five sections: frequency, references, general limitations and cautions, information (narrative discussion and outline), and procedure. Initial conditions for the procedure are contained in the procedural steps and not at the beginning where they would have high visibility.

Initial conditions are often missing in procedures or are quite vague. Many of the initial conditions in the startup procedure merely require the performance of 'applicable sections' of other procedures, but do not specify which sections are in either procedure.

The general limitations and cautions section lists a number of precautions, but these are not placed in the body of a procedure in front of a critical or applicable step. Precautions left in a list up front are often forgotten in a long procedure.

Procedures very seldom make reference to technical specifications or technical standards. These limits should be very prominently displayed in the procedures for the operators.

The alarm control console alarm response procedures contain only a statement of the alarm condition, a setpoint, and an action step for the operator. A probable-cause or symptoms list is a quite common and useful part of most commercial nuclear plant alarm response procedures.

The procedures for startup, xenon oscillations, and others grant authority to 'day supervision' to waive many steps and limits in the procedures.

The procedure for operation of the emergency cooling pumps does not contain any hydraulic conditions (flow and pressures) to determine proper pump operations, only normal running current.

Valves and equipment are referred to by number only and almost never by functional name. This practice requires the operator to remember numbers to determine which valve or equipment to operate.

The procedures are being revised and updated continually. It could not be determined whether a program is in place to review periodically the procedures that have not been revised or updated.

Recommendations, Long-Term. The completion and implementation of the new format technical specifications (now scheduled for June 1990) will necessitate a significant procedure revision effort to incorporate the new and revised requirements. In parallel with this effort, a program should be undertaken

to address human factors in the existing procedures as well as some of the observations listed above (see recommendation Safety Documentation).

Mechanisms for procedure waiver, revision, and periodic review should be formalized and updated in accordance with the administrative section of the new plant technical specifications (see recommendation Safety Documentation).

B.6.3.3. Technical Specification Upgrade

Findings. The draft technical specifications now being prepared closely follow current commercial standardized technical specifications in content. The two-column format is more user friendly than NRC-issued technical specifications. The technical specification document provides significantly more bases and background information for proposed technical specifications than the NRC provides for its standardized technical specifications.

The SRP technical specifications now in use generally state only the equipment required for safe operation. The length of time for which a piece of equipment can be out of service is not stated. Action statements indicating required operations when equipment is out of service are not in the technical specifications.

There seems to be some confusion in the training materials about the purpose of the linking document. The draft technical specifications contain surveillance requirements, but the study materials state that the linking document will identify surveillance requirements.

The current plan is to implement some of the new technical specifications prior to restart and the remainder when they are prepared and reviewed. All administrative controls, confinement, electrical power distribution, instrumentation, PWS, and plant system technical specifications will not be phased in until after restart according to the current schedule. Most commercial utilities that have converted from older technical specifications to the standardized technical specifications have done so all at once rather than use a phased approach. This practice, in part, is motivated by the legal status of technical specifications as part of the operating license, but it also facilitates the transition. This transition is generally implemented by having both sets of technical specifications in the control room for some time period (ca. 60 days) prior to making the conversion official. A phased-in conversion may result in extra work and training; however, it does not represent a safety concern for restart. Management, however, may choose to review this approach.

B.6.3.4. Safety

Findings. Du Pont is very conscious of the need for good industrial safety practices. Industrial safety is emphasized at nuclear utility power plants, but not to the extent that it is at SRP.

A lecture on procedure compliance listed four reasons, in order of importance, for procedure compliance. Nuclear safety (referred to as "prevent technical standards violations") was less important than the prevention of personnel injury or equipment damage.

During a discussion of tagouts of reactor safety circuits, the question came up as to whether reactor safety or personnel safety would be a primary concern for a tagout. The reply was that tagouts were strictly to prevent personnel injury.

During discussions of emergency action levels and the reasons for escalating action levels, the concept of potential increased radiation hazards to workers at SRP and even potentially to the public outside the boundary of the reservation was not understood or appreciated.

Recommendation, Long-Term. An effort should be undertaken throughout the K Reactor site and supporting organizations to raise the consciousness of personnel on the importance of nuclear or reactor safety. The potential for radioactive release and its effect on workers throughout the Savannah River Site, and possibly on the public outside the boundaries of the reservation, should be emphasized. Management should emphasize that nuclear safety is as important as industrial safety, without diluting the excellent attention to industrial safety that exists currently (see recommendations Assimilation of Massive Change and Striving for Excellence).

B.6.3.5. Accreditation

Findings. An extensive effort will be required for the maintenance, health protection technician, component handler, power operations, emergency planning, and laboratory technician training programs to be prepared for DOE accreditation (which is intended to be equivalent to INPO accreditation).

- Many of these groups have not established a continuing training or recertification program.
- Training programs will have to be expanded significantly to cover the material that INPO recommends for similar positions in commercial plants. This expansion will demand a significant effort in course materials development, requiring many man-years of work.
- Not all of these groups have instructor training or qualification programs.
- Examination banks will have to be developed, as most programs currently use the same exams repeatedly.
- Training in familiarization with plant systems and operations needs to be developed for all groups.
- Some groups do not have checklists (or qualification cards) for on-the-job training. On-the-job training is often unstructured.

Recommendation, Long-Term. A centralized training group should be established at SRP for all training programs that will be part of the accreditation

effort. The result would be to establish uniform standards for the effort and to eliminate noticeable duplication in developing materials for the various programs (see recommendation Operator Knowledge Requirement).

B.6.3.6. Configuration Control

Findings. Operations personnel do not have adequate and sufficient information available in the control room to understand and troubleshoot system problems. They cannot be inquisitive and questioning if they do not have as-built plant drawings for key systems. Isolating, tagging, and firm plant-condition control require up-to-date knowledge of plant configuration. The control and followup of plant modifications and work control require up-to-date drawings. Training, maintenance, and other organizations that make plant configuration changes or train personnel must have access to and use up-to-date information.

Recommendation. Short Term. Controlled-as-configured P&IDs and electrical single-line diagrams should be placed and used in the control room and in other key places such as maintenance and training. At least the following systems should be covered: process water, cooling water, emergency cooling, water removal and storage, safety rods, control rods, supplementary safety, leak-detection, shutdown-monitoring instrumentation, emergency power, primary reactor shutdown, and automatic backup shutdown. Establish in the control room a controlled-drawing print file of P&IDs, single-line electrical and logic diagrams, and design changes necessary for K Reactor restart. Develop a system to ensure that these drawings and design changes are updated when a revised drawing is issued and that audits are scheduled and conducted on the controlled drawing file (see recommendation Control Room Information).

Recommendations. Long-Term. (see recommendation Configuration Control)—Identify the remaining essential drawings (i.e., those not required at restart) that are required for the continued safe operation of K Reactor.

- Ensure that all design analyses and calculations that support work done at the SRP reactors are under configuration control as part of the total configuration system.
- Ensure that the originals of the controlled drawings are located to support the timely development and incorporation of design changes.
- Coordinate, develop, and implement a configuration control program and a document control and retrieval system.
- Develop and implement a system that ensures that all K Reactor modifications that result in a physical change to the plant operational configuration are made available to the operations procedure development group, training, and other operations support groups for incorporation into existing procedures or for the development of additional ones.
- Develop a work control system within K Reactor that provides for problem identification; problem resolution and evaluation; identification of the type of work to be done (i.e., maintenance, corrective maintenance, or

modifications); detailed work instruction for the performing organization; training; testing and retesting of completed work; documentation of test results; updating of spare parts inventories; turnover to operations of the revision or development of operating procedures; revision of affected drawings and design documents; and approval of the work to be done by engineering, operations, quality, and safety.

- Develop a configuration control and computerized document control system that links the document and drawing control process with both the works management system and the design-change-control process. The configuration control system should include the following:

- Development of an engineering change/notice system
- Development of a system to identify, record, and evaluate 'as-found' conditions and discrepancies in K Reactor
- Development of incorporation criteria for design change
- Development of a system that ensures a review of design and modification changes by QA and Safety.

B.6.3.7. Work Control

Findings. Serialized tags and a master log of tags in the control room will enhance work control. Tags on equipment and valves are tied to a job plan number. They are not serialized and there is no master list of tags on equipment in the control room. It is very difficult for the operators to determine the status of equipment during a shutdown.

The November 1988 Restart Criterion FD-3.1 (DOE 1988) concerning work control mandates that the control room release all equipment for maintenance. The control room will also be responsible for returning all equipment and systems to service. Implementation of this restart criterion includes establishment of a serialized tagging system with a master log in the control room. The potential lack of control room knowledge of system status should be resolved if the restart criterion is met.

B.6.3.8. Plant Management Organization

Findings. Economies of scale may allow efficiency to be gained in operating similar plants; however, the absolute responsibility to operate each plant correctly should not be diluted. The current management lineup at the SRP reactors has an operations management team, but not an effective plant organization. This operations organization draws from a diverse set of support organizations, but does not have total responsibility for plant operations. An example is that the control room team must negotiate with the Power Department for operation of the CWS, as if it were a utility being supplied to the plant. The CWS is in fact the secondary coolant system of this reactor and its operation is

important to safety. Operation of this system should be the responsibility of the Reactor Operations Department.

The current K Area superintendent is an operations superintendent with a small technical support staff. The K Reactor does not have a plant manager in the commercial nuclear power industry sense who is in charge of operations, maintenance, refueling, reactor engineering, technical support, health physics, chemistry, security, etc. Senior supervisors expressed frustration several times at not being able to set priorities for support personnel.

Recommendation, Short-Term. (see recommendation Plant Site Organization)--A plant manager should be identified. The plant manager should ensure that there are clear lines of responsibility and that the operations organization is in charge as the 'plant owner.' The manager should have adequate resources assigned to discharge his/her responsibilities. These include operations, maintenance, engineering, reactor technology, and training. The subcommittee does not consider the existing operations management to have adequate control of these resources.

The plant manager should develop and train his/her staff so that experienced, qualified personnel with the correct standards of excellence for plant operation are assigned to the Operations Department.

The K Reactor plant manager should have control of, and be held responsible for, the following functions as a minimum:

- All maintenance activities
- Operation of all valves, equipment, and breakers in the K Reactor
- The power operations personnel presently providing outside support functions, all of whom should be transferred to Center Section operations
- An engineering support staff to process small modifications, analyze and resolve operational problems, and provide other engineering support functions
- A reactor engineering group sufficient to monitor reactor core burnup and provide operational limits for the K Reactor core
- A radiological health physics organization responsible for all radiation control and as-low-as-reasonably-achievable (ALARA) programs in K Reactor area
- Cognizant engineers
- Work control.

Unless it is determined to be necessary to establish chemistry and/or radiochemistry analytical facilities in the K Area, the chemistry function might be left separate. Because the component handlers move among the three reactors, most of this group might also be left separate under the reactor operations manager.

Some personnel in the new K Reactor organization could be technically matrixed from other support groups to show future career paths. However, these support personnel should be accountable to K Reactor supervision.

B.6.3.9. Plant Staff Knowledge

Findings. The subcommittee is concerned that the pace of training has exceeded the capability of the operators to absorb the material. In addition, several indicated that they did not know why they were being trained on a subject or what the desired end product was. During a discussion of reactor principles with a team of operators, the instructor who had given the training continually had to prompt personnel to recall training recently completed. Throughout the interview session, there were numerous concerns voiced on the pace of training activities. Similar concerns exist in the area of declaring emergency events. Although the training has been completed, the knowledge has not really been assimilated through practice and repetition. Concerns also exist as to whether the senior supervisor will actually utilize the shift engineer and shift advisor who will be assigned to him/her. There appears to have been no training on how to incorporate these people into the shift team. Similarly, training has been conducted on plant modifications, new operating requirements, technical specifications, tagout, and log-keeping procedures, which are themselves not yet complete. The operators are losing the new knowledge prior to actually operating the new equipment.

The review team found many weaknesses in the existing operator knowledge level. Although such knowledge cannot be learned overnight, the team believes that the operating staff should have a solid fundamental understanding of how a reactor works, what the reactors are producing, and how. Some weaknesses found were little knowledge of the delayed neutron fraction; understanding reactivity in terms of k_{eff} ; inability to determine the factors that might be in the period equation; lack of understanding of the rod motion required to establish a certain period or power level change; lack of understanding of rod worths, xenon behavior, effect of process water temperature on moderation, etc.

In addition to the lack of theoretical knowledge, the operating team also has weaknesses in practical knowledge of the plant. Some control room operators could not state all of the scram parameters and how the trip signals are derived (e.g., on loss of an AC motor, whether a scram occurs from low flow, low pressure, low voltage, or an auxiliary breaker contact). The subcommittee also expected that a senior reactor operator should be able to draw the scram system from memory, but such was not the case. The control room teams had difficulty in stating how power level for the reactor was computed. It was evident that power ascent/power level determination was so proceduralized that the operators had lost touch with the basic heat-balance equation. Even experienced personnel indicated that they could not use electrical schematics; this task is deferred to the electrical and instrumentation personnel. Fundamentals of pump operation are not understood. The differences between thermocouples and resistance thermometers are not known. The subcommittee believes that an operator should be inquisitive and should be in a position to lead a troubleshooting effort or analyzing a plant malfunction; thus skills with drawings are mandatory.

Recommendations Long-Term. None of the above examples are meant to denigrate the incumbent operators. Management has not expected such a level of knowledge in the past. The examples serve to illustrate the need for an ongoing program to upgrade the operating staff's depth of technical knowledge. The subcommittee believes that the restart strategy criteria specify adequate measures to restart K Reactor safely; therefore, a short-term recommendation is not provided for this issue.

In a commercial reactor or research reactor, a license candidate will have many reactivity manipulations (either on the plant or on a simulator) prior to startup. Draft Regulatory Guide 1.8 (NRC 1984) and ANS 3.1 (ANS 1987) require a minimum number of reactivity changes for each hot-license candidate, and observing a reactivity change being made does not count as performing a reactivity change. The senior reactor operator certification program at SRP should be revised to comply with these standards (see recommendation Operator Knowledge Requirement).

B.6.3.10. Plant Staff Morale

Finding. This observation is not specifically related to restart of the K Reactor. The subcommittee found incumbent personnel to be honest, straightforward, and helpful during field interviews. It was evident, however, that the staff is suffering from confusion, distrust, and declining morale. Incumbent personnel are proud of their prior operating record, as they should be, and are willing to meet new standards. They are, however, uncertain as to what the new standards are and why the change is needed. At the working level, there is lack of direction, vague destination (e.g., "like a commercial plant"), and no end-point or schedule for completion. As the working level put it, they believe that their management (for whom they have great respect) is being overwhelmed by DOE and has essentially lost control of the operation of the SRP reactors. In addition, they believe that the abundance of committees are punitive in nature and that employees are in jeopardy of disciplinary action for any type of error. On numerous occasions the subcommittee was referred to, or introduced as "Westinghouse investigators," in spite of many assurances to the contrary. Much of the employee concern is due to the sudden influx of DOE overviewers. Although the degree of overview is probably not out of line compared to that at other Government-owned-and-contractor-operated facilities, it is a sudden shock to the previously 'isolated' SRP employees. Additional concerns arise from a sense of loss or abandonment caused by Du Pont's decision to cease SRP operations and from the uncertainty of working for Westinghouse. Such problems may not exist throughout SRP; however, they are evident at the reactor area.

Recommendation Long-Term. As soon as possible, WSRC should take action to demonstrate that the contractor is 'in the driver's seat, and has a firm grip on the reins.' Without such actions to restore confidence, the incumbent

employees will flounder and lose the drive and focus necessary for restart. The WSRC management team will be sorely challenged to demonstrate that customer responsiveness and respect of overview do not dilute the line management authority and responsibility (see recommendations Assimilation of Massive Change and Striving for Excellence).

B.6.3.11. Plant Staff Upgrade

Finding. The operator's job does not seem to be held in high esteem at SRP. People indicated that it was viewed as less skilled than a craft position. Personnel are often upgraded from Traffic and Transportation (i.e., light-truck driver or lawn care) to operator positions. Operators indicated that they often folded and stowed clothes, performed cleanup chores, drove to deliver samples and daily reports to other sites, etc. These activities indicate that the operators in fact are not regarded as the most skilled and responsible employees on the SRP site. It is difficult to imagine that any employee could have more responsibility than the man or woman actually controlling the production reactor.

The subcommittee considers that the current training program does not result in the shift supervisory team's being qualified at the senior reactor operator level as defined in DOE Order 5480.6, *Safety of DOE-Owned Nuclear Reactors* (DOE 1986) or ANS 3.1, *Standard for the Selection, Qualification and Training of Personnel for Nuclear Power Plants* (ANS 1987). Designation as a senior reactor operator requires minimum levels of operating experience at nuclear power plants and at the facility where the individual will certify. The current requirements for shift supervisor (i.e., senior reactor operator) qualification for degreed engineers do not actually require hands-on operation of the facility. The grade 8 personnel designated as senior reactor operators at SRP actually fill the reactor operator position as opposed to the senior reactor operator position as defined in DOE orders, ANS standards, and Title 10, CFR, Part 55 (NRC 1988c).

Recommendation. Long-Term. We believe that the operator job position should be upgraded to reflect the training, knowledge, and responsibility required of the position. The WSRC should move promptly to improve the status of the operator and thereby enhance the ability to place appropriate responsibility on incumbent personnel. The subcommittee suggests the following actions (see recommendation Operator Knowledge Requirements).

- Entry-level requirements should be established that ensure selection in accordance with ANS, medical, and psychological screening standards. In addition, future operators should possess at least a two-year scientific degree or demonstrate success in a rigorous nuclear-reactor-operator training program (i.e., navy nuclear or commercial experience).
- Placement practices should be revised so that on-shift managers actually interview and select future operators as opposed to having candidates simply assigned by Human Resources.

- An entirely separate job progression should be established that recognizes the special skills, knowledge, and responsibility assigned to reactor operators. At this time, reactor operators/senior reactor operators are simply grade 7/8 and are therefore really no different from crafts or power operators. This situation exists in spite of the \$2,500 annual bonus paid to senior reactor operators. Based on the subcommittee's interviews, we concluded that the bonus is not sufficient to keep personnel in the Operations Department.

- Along with the above-mentioned job progression, WSRC should carefully review the job titles. The current senior reactor operator does not perform the functions specified in Title 10, CFR, Part 50 (NRC 1988a), ANS 3.1 (ANS 1987), or DOE Order 5480.6 (DOE 1986). The subcommittee believes that only the senior shift supervisor and the control room supervisor are performing work at the senior reactor operator's level. As such, the senior reactor operator's job title should not be used for the console operator position because of the industry-wide application of 'senior reactor operator' as a title for a licensed individual directing plant operations. The senior reactor operators' certification program should be revised as appropriate.

The WSRC should also recognize that some personnel may be unwilling or unable to meet rising standards of adequacy for theoretical knowledge, rigor of operating principles, etc. Therefore, consideration should be given to the high attrition that could occur over the next few years. Some attrition may be healthy for the organization; however, plans should be in place for a larger- than-expected need for replacement operators.

The K Reactor staff would benefit by increased exposure to industry principles of operation. Training should be given on industry lessons learned and the whys behind the many changes the staff are facing and should not consist just of 'here's the new way.' This training should include exposure to other facilities through visits, INPO workshops, ANS meetings, etc. Publications such as *Nuclear News*, *Nucleonics Week*, *Nuclear Plant Safety*, etc., should be routed regularly through the operating crews. Special articles should be required reading and should be used for topical training.

The WSRC should also recognize that the on-shift management is in many cases relatively young. The WSRC should invest heavily in management training for this supervisory team. A strong management team, consisting of more than just engineers, will be needed to succeed in the K Reactor restart effort.

B.6.4 SUBCOMMITTEE ACTIVITIES

B.6.4.1. Training

B.6.4.1.1 Operations (Center Section) Training. The following activities were conducted concerning operations training.

- Observed Cycle 1 restart training, week of December 5, 1988.

- Observed two days of Cycle 2 restart training on February 1 and 2, 1989.
- Reviewed Westinghouse Nuclear Services Division observer reports for Cycles 1 and 2 of restart training.
- Reviewed Instructor Qualifications, Initial and Recertification Tests and Records, System Qualification and Practical Factor Records, and Test Statistics between January 4, 1989, and January 6, 1989.
- Conducted interviews with reactor operators, senior reactor operators, and certified senior reactor operators engineers on February 6 and February 7, 1989.

B.6.4.1.2 Training for K Reactor Support Groups. Two-hour interviews were conducted with personnel cognizant of training efforts as noted below:

- Maintenance training, C Area, on January 6, 1989
- Health protection technician training, 3/700 Area, on January 9, 1989
- Component handler training (fuel charging/discharging), C Area, on January 9, 1989
- Power operations training, K Area, on January 10, 1989
- Emergency planning training, 3/700 Area, on January 10, 1989
- Laboratory (chemistry) technician training, H Area, on January 11, 1989.

B.6.4.1.3 Organization of K Reactor. The following interviews were conducted.

- Interviewed five current and former senior supervising operators.
- Interviewed maintenance personnel on work control practices.

B.6.4.1.4 Technical Specifications. The following materials related to specifications were reviewed:

- Draft technical specifications on the reactor
- Procedures concerning technical-specification-related activities
- Current SRP technical specifications
- Restart training materials for technical specifications.

B.6.4.1.5 Center Section Procedures. The following center section procedures were reviewed:

- The K Reactor master startup procedures
- Selected procedures on ECS pumps, 105 Building operations, xenon oscillations, and high-level flux monitor adjustments
- The abnormal condition control alarm response procedures for the CWS
- The master control procedure for emergency response.

B.6.4.1.6 Criteria for Reportability to DOE. The following activities were conducted relative to reportability to DOE:

- Discussions during Cycle 1 restart training
- Interviews with supervisory operators.

B.6.4.1.7 Morale of K Reactor Staff. Interviews were held with about 20 members of the K Reactor staff including supervisors, senior reactor operators, reactor operators, and maintenance personnel.

B.6.4.1.8 Reactor or Nuclear Safety. The following activities concerning safety were conducted.

- Observed Cycle 88-1 restart training concerning procedure compliance.
- Interviewed K Reactor personnel during week of February 6, 1989.

B.6.4.1.9 Tagouts of Equipment and Work Control. The following activities were conducted.

- Interviewed operations and maintenance personnel on work control, February 8, 1989.
- Toured K Reactor plant, February 9, 1989.

B.6.4.2. Site Operations

Partial or full subcommittee meetings were held as follows:

- December 6-8, 1988, SRP, introduction and orientation
- January 3-6, 1989, SRP, paper review and site visit
- January 20, 1989, Hanford Site, planning for site visit, interim recommendations
- February 6-9, 1989, SRP, detailed site visit, interviews, and plant walkdown.

The main focus of the subcommittee was to assess the current status of operations in comparison with the restart strategy actions (DOE 1988) and determine whether the actions were adequate to resolve any observed weaknesses. It was made clear that any subcommittee recommendations would be provided to the full WISR committee for inclusion, as appropriate, in the final report.

Subcommittee members reviewed a substantial number of documents. Personnel interviews were also conducted. The subcommittee cleansed the report so that findings in the report would not be traceable to specific individuals.

B.6.4.3. Interviews Conducted

We conducted a group interview of K Reactor personnel on emergency actions. Personnel included a shift senior supervisor, a reactor supervisor from the central control room, a senior reactor operator, and a reactor operator. All individuals were certified, and at least one degreed engineer was included. The duration of the interview was about three hours. Major topics covered were operation of ECS, emergency procedures (format, usage, etc.), event recognition, and declaration of emergency levels.

We conducted a group interview of K Reactor personnel on reactor principles. Personnel included (as a minimum) a reactor supervisor from the central control room, a senior reactor operator, a reactor operator, and a member of the training staff responsible for reactor physics/principles instruction. These personnel were different from those listed above. At least one of the individuals was a degreed engineer (or in training if a certified person were not available). The duration of the interview was about three hours. Major topics covered were reactor principles, rod control, rod position indication, startup procedures, reactor anomalies, and procedure usage.

We conducted an interview on event recognition and event reporting. Personnel included a senior shift supervisor and an area superintendent (preferably from K Reactor). The duration of the interview was about two hours.

We interviewed the reactor operations department manager, the K Area superintendent, an additional area superintendent, and a senior shift supervisor. The topic was managing a cultural change in event recognition and reporting. The duration of the interview was about two hours.

We performed an in-depth plant tour with a certified operator. The tour covered all accessible areas of the plant and included the operator's routine duties. Topics that were covered with the operator during the tour included log taking, communications, procedure usage, deficiency identification, watchstanding principles, shift turnover practices, etc. It was expected that the tour would be conducted in conjunction with the operator's routine job assignment. The duration of the tours was about eight hours.

We performed an in-depth surveillance of the control room. The duration of the interview was at least four hours and overlapped the shift change (turnover). It was expected that control room personnel would perform their normally assigned duties as long as they could talk with the team member on a not-to-interfere basis. If this were not possible, a full-time escort, senior reactor operator-certified, was provided. The topics covered during this period were control room resources, control room access control, formality, procedures (formal usage, change control), alarm response, and other topics of a similar nature.

We conducted an interview on work control practices. Personnel included a senior shift supervisor, a supplementary shutdown system operator, a reactor supervisor from the central control room, a senior reactor operator, a maintenance first-line supervisor, and an instrument craft person. Topics

included work control, deficiency identification, equipment status, and removal and return of equipment from service. The duration of the interview was about two hours, with a contingency for a one-hour walkdown at the end of the tour.

B.6.4.4. Configuration Control

Twenty-one SRP personnel were contacted during the course of this review. Approximately 16 man-days were spent during this portion of the review.

B.6.5 BIOGRAPHICAL INFORMATION

D. J. SWAIM

Mr. Swaim is currently the Operations Manager for the FFTF, an advanced liquid metal test reactor operated for the U.S. Department of Energy by Westinghouse Hanford Company. He has 15 years of experience on the FFTF project in the areas of construction, testing, and operations. He was one of the initial cadre of engineers selected to supervise the performance of the Acceptance Test Program. He has six years of previous experience in the nuclear field in the navy nuclear submarine program. He is a member of the American Nuclear Society. He has a BS in mechanical engineering from Washington State University.

R. C. COULTHARD

Mr. Coulthard is currently a senior engineer at the Westinghouse Zion Nuclear Training Center, with responsibility for various consulting, regulatory, and audit activities of the training center. He has twenty years of commercial nuclear power experience and has participated in the startup of many nuclear power plants both domestic and international. He was manager of Nuclear Training at Kansas Gas & Electric for three years. He has a BES in nuclear energy from the University of Texas and an MS in nuclear engineering from the University of Missouri. He is an NRC-certified senior reactor operator instructor on the Surry Nuclear Plant (Docket No. 55-7286) and a member of the American Nuclear Society.

K. D. BONSER

Mr. Bonser brings 19 years of nuclear operations and training experience to the Conduct of Operations subcommittee. He is currently with the Westinghouse Hanford Company as the manager of Technical Training at N Reactor. His experience base includes senior reactor operator certification on a GE BWR; control room supervisor/shift manager, certified at N Reactor; and nine years in the navy nuclear program. He has developed operations training programs for INPO accreditation and coordinated the building and program

development for a full-scope control-room simulator project. He has been active with the NRC Region V Interoperating Utility group and has worked with the NRC in redefining the license examiner standards. Mr. Bonser holds a BS from Central Washington State University.

L. S. LEGOWIK

Mr. Legowik brings 17 years of configuration management and document control experience to the Conduct of Operations subcommittee. He is currently the manager of Engineering Documentation Control for the Westinghouse Hanford Company. His experience includes development of a uniform configuration management system and implementation of a standard document control system for the consolidated Westinghouse Hanford Company. Mr. Legowik is currently a member of the American Nuclear Society and the Nuclear Information and Records Management Association. Mr. Legowik holds a BA in economics and history from the University of Montana.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

APPENDIX B.7 PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENTS

Michael J. Hitchler, Manager, Plant Operations and Risk Improvement, Westinghouse Nuclear and Advanced Technology Division

Gerald R. André, Senior Engineer, Plant Operations and Risk Improvement, Westinghouse Nuclear and Advanced Technology Division

Beverly Cassidy, Scientist, Plant Operations and Risk Improvement, Westinghouse Nuclear and Advanced Technology Division

Robert J. Lutz, Jr., Fellow Engineer, Containment and Operational Analysis, Westinghouse Nuclear and Advanced Technology Division

Michael D. Zentner, Manager, Probabilistic Risk Assessment, Westinghouse Hanford Company

B.7.1 SCOPE

We assessed the capability of the Savannah River production reactors to prevent or mitigate severe accidents. The subcommittee investigated the frequency of initiating events that could lead to severe accidents, the reliability and availability of systems used to prevent initiating events from propagating to severe accidents, and the action of the plant operating staff in responding to initiating events. The subcommittee also investigated the capability of plant systems, confinement, and the plant operations staff to mitigate the consequences of a severe accident.

A comprehensive PRA and severe-accident assessment are in progress at SRP. The efforts of this subcommittee are not intended to duplicate or substitute for the ongoing effort, but to identify key severe-accident issues and to render recommendations related to SRP restart and operations based on these issues.

To carry out this assessment, the subcommittee focused on the following major areas:

- Component performance
- Systems reliability
- Accident sequence analysis
- Safety goal and confinement assessment
- Title 10, CFR, Part 100 assessment (NRC 1988d).

B.7.1.1 Component Performance

Several kinds of reviews were performed to evaluate current component performance at the Savannah River reactors:

- An aging trend analysis to determine whether component failures were increasing
- A brief evaluation of valve failure reports for potential common-mode failures
- A graphic and tabular comparison of the SRP component failure-rate data base with N Reactor and the interim reliability data base (Carlson et al. 1983)
- An evaluation of similarities and variation in types of failure modes in the valve population.

B.7.1.2 Systems Reliability

Systems important to plant safety were examined to assess their reliability and to provide system unavailability values to the severe-accident core-damage assessment (accident sequence analysis). We reviewed system design information. Discussions were held with Du Pont and Westinghouse personnel to obtain information on system operability requirements, system response to accidents, success criteria (tied directly to the core damage assessment), and test and maintenance requirements. Judgments based on qualitative review, previous experience, comparisons to reliabilities of comparable PWR systems, and importance of the system to accident mitigation determined the key systems with respect to plant safety. We performed more detailed assessments on these systems. If necessary, the detailed assessments calculated system unavailability using fault-tree techniques. Both qualitative and quantitative assessments were used to identify system vulnerabilities.

B.7.1.3 Accident Sequence Analysis

Several classes of accident-initiating events will be addressed in the full-scope level 1 PRA being performed at SRP. The scoping analysis performed by this subcommittee addressed only those events expected to pose the greatest challenge to the mitigation systems.

An initial review of accident classes indicates that all accidents (at power) would require reactor shutdown and long-term decay heat removal. The accident initiators included in this scoping analysis are the large and small LOCA and the worst-case LOPA. These events challenge the ECS and the CWRSS. The success criteria for these mitigating systems for each of the accident initiators were developed on the basis of discussions with other subcommittees. On the basis of available level 1 PRA information, scoping-event trees were constructed to model the accident progression. The frequencies of the LOCA events are based on the leak-before-break assessments. Only the worst-case cooling water

break, causing almost immediate flooding of the Bingham pumps, is evaluated for the LOPA. It is assumed that this case bounds all other breaks of lesser magnitude. Worst cases for these accident initiators were defined in terms of break flow, frequency of break, and success criteria.

B.7.1.4 Safety Goal and Confinement Assessment

The method used to assess the capabilities of the confinement structure and related systems consisted of the following:

- Interviews with Du Pont personnel to identify the available information (physical data, systems descriptions, analyses, etc.) related to the confinement
- A walkdown of the K Reactor confinement
- Interaction with other WISR subcommittees (e.g., Mechanical Systems and Safety Analysis)
- An independent assessment, including scoping analyses, of the SRP confinement and related systems.

B.7.1.5 Title 10, CFR, Part 100

The method used to assess the capability of the SRP reactors to meet the Title 10, CFR, Part 100 siting criteria (NRC 1988d) consisted of the following:

- Review of previous SRP analyses related to compliance with Title 10, CFR, Part 100
- Independent calculations to compare the SRP with Title 10, CFR, Part 100 siting criteria.

B.7.2 RESULTS

The following describes the results and observations for the component performance, systems reliability, accident sequence, safety goal and confinement, and Title 10, CFR, Part 100 assessments.

B.7.2.1 Component Performance

No particular problems were observed in component behavior at SRP. However, the mechanical binding failure mode is encountered more frequently at SRP than at other sites. The specific results of the various reviews are as follows.

- No significant aging trends were identified in the components evaluated. However, since the information source was valve-related reactor incident reports, minor performance degradations may not have been included in this data

base. Since early aging indicators may tend to be of this minor type, insufficient information is available to make a final judgment. The analysis should be expanded to include all available information, including other component types.

- Some common-mode failure categories were identified. Most are human-error related, maintenance and design problems, and some operator errors.

- The SRP specific data base compared satisfactorily with that of N Reactor and the requirements of the Interim Reliability Evaluation Program (Carlson et al. 1983) data bases. No problems or significant outliers were observed in the subset of data that was considered. However, the practice of identifying failure rates among components at the building level may tend to skew the data. We felt that it would be better to form broader failure groups for similar valves at each reactor instead of specific failures per building. Such a practice will tend to minimize inadvertent random failures' skewing the data. Analyses of the type described below should be performed to ensure that information available in data is not lost.

- It is apparent that some failure modes occur primarily in specific valves. It is also apparent that some valves have more than their share of failures; some have several failure modes, while others have only one. The plant staff may find it helpful to perform a more detailed evaluation of this type to identify and rank order component and equipment upgrades.

B.7.2.2 Systems Reliability

The systems reviewed were the ECS, CWRSS, CWS, PWS, CHRS, AACS, RSS, and AIAS.

We reached two general conclusions. (1) The reliability of normally operating systems used in accident mitigation is judged to be acceptable. These systems include the PWS, CWS, and AACS. The assessment of the AACS does not include failure of the filters, which is addressed in the level 2 PRAs. (2) The reliability of most of the standby systems will improve with more frequent testing. Current testing for the majority of these systems is limited to a semiannual or annual basis.

The following discussion addresses the individual system assessments in more detail. It should be noted that the acceptability of the unavailability of these systems will be based on the core damage assessment, and not on the unavailability assessment, since the core damage assessment indicates the relative importance of these systems to accident mitigation.

B.7.2.2.1 Emergency Cooling System. System unavailabilities for 24-hour mission times and several success criteria are as follows:

Success criteria	Surveillance frequency	
	6 mo	3 mo
One pump source through 2 of 3 injection lines (large LOCA)	3 E-02	1 E-02
One pump source through 2 of 4 injection lines (large LOCA)	2 E-02	9 E-03
One sump source through 1 of 3 injection lines (small LOCA)	9 E-03	4 E-03

The unavailability is dominated by failure of the injection lines, which is related to failure of the motor- and hydraulic-operated valves to open as a result of common-mode problems. Each injection line contains two valves in series; both are required to open. The relatively high failure probabilities of the valves are directly related to the test frequency. Sufficient pumping sources with enough diversity are available to reduce the contributions of loss of pumps as a significant contributor to the system unavailability. The pumping sources consist of cooling water 1 header, cooling water 2 header, and the ECS pumps (of which one of three is required). The polybor header represents a single failure point, and for this analysis its reliability is assumed to be $1.0 \text{ E-}04$. Based on discussions with SRP personnel, this value may be too low because of the potential for biological fouling for the filters.

As noted above, significant improvements in system reliability can be expected by implementing more frequent surveillance testing. The affected valves are those required to open in each injection line and also those required to open from the pump sources.

Reliability could also be improved by changing the position of one of the series valves in each injection line so that it opened normally. If this change were implemented, then the AIA response to LOCAs, in addition to operator response and corresponding response procedures, would need to be modified. The implications of potentially increasing spurious injections of light water into the PWS would also need to be considered. This type of change is not recommended, because it would require significant operator retraining (for LOCA mitigation) and might also affect plant performance adversely.

Values are not reported for 500-hour mission times. Increasing the mission time only affects the run time of the system, which, in turn, affects only the pump sources. Since the pump sources are not significant contributors to a system unavailability (the valves dominate), increasing the mission time has a minor effect on unavailability.

B.7.2.2.2 Contaminated Water Removal and Storage System. System unavailabilities for 24-hour and 500-hour mission times for several success criteria are as follows:

Success criteria	Surveillance frequency		
	12 mo	6 mo	3 mo
9,000 gal/min removal required*			
– 24-h mission time	4 E-02	2 E-02	6 E-03
– 500-h mission time	1 E-01	6 E-02	4 E-02
5,000 gal/min removal required**			
– 24-h mission time	7 E-03	1 E-03	3 E-04
– 500-h mission time	2 E-02	9 E-03	6 E-03

*Large LOCA.

**Small LOCA.

The unavailability for cases with 24-hour mission times is dominated by failure of the pumps to start and by failure of the pumps to run with 500-hour mission times. The high probabilities of failure of the pumps to start are directly related to infrequent system testing (once per year). As noted above, significant improvements in system reliability can be expected by implementing more frequent surveillance testing.

It should also be noted that there may be insufficient screening and filtering of the water entering the pumps. If so, then the probability of the pumps' failing to continue to run should be substantially increased (the pumps may be operating in 'adverse' conditions), which would further degrade the ability of the system to respond to accidents.

B.7.2.2.3 Cooling Water Systems. The CWS is normally operating. Following most accidents it is required to continue to operate, but in a reduced configuration. That is, fewer loops are required for process water heater exchanger cooling than in normal operation. This assessment assumed that typically three of five pumps will be required to run with a mission time of 500 hours. The reliability, based on the above assumptions and on a qualitative assessment, is judged to be adequate with respect to the CWS's required function following an accident.

B.7.2.2.4 Process Water System. The PWS is normally operating and is required to continue to operate following an accident for decay heat removal purposes. Currently, four pumps are required to continue to operate, driven by their DC motors. This assessment assumes that the pumps are designed to operate in the environment expected following most accidents, in particular for LOCAs (they are assumed to fail in the environment expected following a large LOPA).

The reliability of the PWS, based on the above assumptions and a qualitative assessment, is judged to be adequate with respect to its required function following an accident.

B.7.2.2.5 Confinement Heat Removal System. System unavailability is calculated to be $2 \text{ E-}02$ and is dominated by the operator action required for system actuation and failure of both pneumatic valves to open. The operator action could be changed to an automatic action, as it is in L Reactor, by controls on the three monitor pins located in the bottom of the reactor.

Failure of the system without consideration of the operator actuation is calculated to be $9 \text{ E-}03$. It is dominated by the failure of both pneumatic valves to open. The failure of these valves to open is directly related to the test frequency (yearly test). Increasing the frequency of testing of the system will substantially improve reliability. Based on quarterly testing, the system unavailability is calculated to be $3 \text{ E-}03$. This system is not important to core damage mitigation, but it is important to releases.

B.7.2.2.6 Airborne Activity Confinement System. System unavailability is calculated to be $3 \text{ E-}03$ based on a success criterion of two of three fans required to run, assuming that the fans are designed to operate in the environment expected following an accident. This issue is further addressed in the confinement assessment. The AACS is a normally operating system with a mission time following an accident of 35 days. The mission time is based on filter cooling requirements. Failure of the filters is not included in this assessment. Filter failure is dependent on the accident conditions and is assessed in the confinement review. This system is not important to core damage mitigation, but it is important to releases.

B.7.2.2.7 Automatic Incident Actuation System. The reliability of the AIAS, based on a qualitative assessment, is judged to be adequate with respect to the systems it is required to actuate while it is operable. That is, the AIAS will not be a limiting factor in accident mitigation; the ECS will be more limiting. The judgment is conditioned by the phrase "when it is operable," since there are no restrictions on the number of channels allowed in bypass; therefore, the system could be inoperable if sufficient channels are placed in bypass. However, if enough input channels are bypassed to render the AIA system inoperable, an alarm sounds.

Reliability would be improved with increased surveillance frequencies (currently, signal conditioning calibration is twice per year, and logic and actuation relay tests are once per year). Quarterly testing is recommended for components amenable to testing while at power and semiannual testing (or between charges at the most) for components not amenable to testing at power.

B.7.2.2.8 Reactor Shutdown Systems. The reliability, based on a qualitative assessment, is judged to be adequate. Diverse shutdown means are

available (shutdown rods and Ink injection system). The actuation systems have a degree of diversity: scram circuits in addition to the safety computers are able to actuate the shutdown rods. It is indicated that all trip functions have diverse backup protection for at-power accidents except for localized core situations. Not all the trip functions use multiple channels to measure a single parameter; therefore, the failure of a single channel could cause failure of a protective feature if it does not have a backup. A review was made of the protective trip functions available for the LOCA and LOPA events, and it was determined that sufficient backup is available. Reliability would be improved with increased surveillance frequencies.

B.7.2.3 Accident Sequence Analysis

As discussed previously, the large and small LOCA and the maximum LOPA events were considered in this assessment because they present the greatest challenge to the safety systems. If a LOCA occurs, ECS must be activated to inject cooling water to the reactor tank. Because some of the ECS injection flow will spill to the -40-ft level of the 105 Building, the CWRSS pumps are activated to remove this flow. If the ECS injection flow is greater than the capability of the CWRSS pumps, the Bingham DC motors would be flooded, preventing forced recirculation. The procedures instruct the operator to throttle ECS flow if the water level at the -40-ft level increases. If ECS injection is successful and CWRSS is capable of removing the excess water from the -40-ft level, long-term decay heat must be removed via the PWS (Bingham pumps and their associated heat exchangers). If the leaks cannot be isolated, the ECS and CWRSS would be required to function until the core was discharged (about 500 hours). The adverse radiation environment would preclude repair or replacement of any components in these systems. This situation presents a greater challenge to the mitigation systems than equivalent systems in a PWR.

The most probable condition for a large LOCA is that all four ECS injection lines are available. The ECS injection flow then may be greater than the CWRSS removal capability, requiring the operator to throttle ECS flow. Core damage is postulated if any one of the following fails: the ECS, operator action to throttle ECS flow, CWRSS, or long-term heat removal.

The most probable condition for a small LOCA is that only three injection lines are available, and the operator will not be required to throttle flow unless pump failures occur in the CWRSS. In addition, if the leaking pipe can be identified and isolated, only long-term decay-heat removal would be required and ECS injection and the CWRSS operation could be terminated. Once-through cooling via the ECS is also postulated if the Bingham pumps fail either from flooding (failure of CWRSS) or from failing to run. Once-through cooling is successful if the operator closes the rotovalves and ECS remains in operation until the fuel is discharged.

Large breaks in the CWS inside the reactor building could lead to an almost immediate loss of the Bingham pumps (LOPA). In this case, the operator could have as few as 2.7 minutes to initiate ECS injection. Decay-heat removal could only be accomplished with once-through cooling via the ECS, after the closing of appropriate rotovalves. However, ECS injection would be initially degraded if one of the cooling water injection sources contains the broken pipe. If the operator isolates the wrong cooling water source, ECS injection could be further degraded, especially if components in the ECS controls are shorted and become inoperable. If the operator does not initiate ECS within 2.7 minutes, if the ECS fails, or if once-through cooling fails, core damage is postulated.

Based on available information and the accident scenarios described above, scoping event trees were constructed to model the accident progression of large and small LOCAs and the maximum LOPA. For those sequences resulting in core damage, the state of the confinement is addressed. If core damage is postulated, the CHRS cools air exhausted from the below-grade areas. The operator opens the appropriate valves and the pump room floor is flooded to a depth of 8 to 10 inches. To maintain this cooling function, the operator would also be required to stop any running CWRSS pumps. If the water is cooled, then the AACS maintains the subatmospheric pressure to prevent direct leakage to the environment and filters fission products from the exhaust stream. The success and failure combinations of the CHRS, operator action to stop the pumps, and AACS define the plant damage stages, given core damage.

The event trees were quantified for the base conditions (current plant conditions), and the following was concluded: all three accident initiators are highly dependent on operator actions to mitigate the event. In particular, the conditional probability of core damage, given either the large LOCA or large LOPA, is a function of the failure probability of the operator rather than the unavailability of safety systems.

The frequency of core damage is the product of the frequency of the event and the conditional probability that the accident cannot be mitigated. Therefore, the frequency of core damage calculated for each of these initiators is also highly dependent on the expected frequency of the postulated accident.

The event trees were quantified again with the following changes and assumptions.

- The large pipes in the CWS are inspected, and surveillance is maintained on this system to identify potential leaks, such that the initiating event frequency of a large LOPA is about $1 \text{ E} - 04/\text{yr}$.
- The procedures and operator training are improved to meet industry standards.
- The times between surveillance intervals for critical components in the ECS and CWRSS are decreased, thereby increasing the reliability of these systems.

When these assumptions were taken into account, the frequency of core damage from the three events was judged to meet DOE goals.

The dominant possibilities include the following:

- Failure of the operator to initiate ECS with a LOPA
- Failure of the operator to establish once-through cooling with a LOPA
- Failure of a CWRSS pump and failure of the operator to throttle flow and establish a once-through cooling with a small LOCA
- Failure of the ECS to start with a small LOCA.

The small LOCA contributes more than 50% of the total core damage frequency. The frequency of a large LOCA is estimated to be more than two orders of magnitude less than the frequency of a small LOCA. Therefore, even with the more restrictive requirements on the operator during the large LOCA, the contribution of the large LOCA is less than two percent of the total core damage frequency calculated for the three events.

B.7.2.4 Safety Goal and Confinement Assessment

B.7.2.4.1 Offsite Safety Assessment. The DOE safety goal criteria for production reactors (DOE 1989) specify that the risk of immediate accidental death or of latent cancer deaths to the general public in the vicinity of the plant should be increased by less than 0.1% as a result of operation of the facility. Based on experience with commercial LWR risks, this figure translates to a severe-accident risk criterion. The background accidental fatality risk in the U.S. is 0.0005/yr and the background cancer risk is 0.002/yr. In terms of safety goals, the acute fatality risk should be less than $5 \text{ E-}07$ for individuals within one mile of the site, and the latent fatality risk should be less than $2 \text{ E-}06$ for individuals within 10 miles of the site.

The PRA study for the Savannah River reactors was not sufficiently complete to provide direct input to this evaluation. Several evaluations of the progression and consequences of selected severe-accident sequences have been completed. These show that the potential releases from the SRP facility are within the range of those predicted for commercial LWRs. In addition, detailed studies have been performed to quantify the effectiveness of the AACS. These conclude that the AACS filters can perform their intended function in the event of a severe accident, provided that other confinement safety features are operable.

Independent analyses have been performed to verify and extend the work presented in the SRP published materials. The results of these analyses or evaluations lead to the following conclusions.

- The confinement structure is capable of withstanding the transient conditions during a severe accident. Therefore, releases of radioactive materials from the core will initially be contained within the confinement.

- No major airborne-release pathways have been identified that bypass the confinement structure. Continued operation of the CWRSS after a core melt could result in significant quantities of highly radioactive liquid being removed from the confinement.

- Some traditional severe accident phenomena are not applicable to the SRP reactors. Included in this nonapplicable category are direct containment heating (low system pressures), hydrogen combustion (low hydrogen generation for aluminum-uranium fuel and high exhaust flows in the confinement), and steam explosions (low fuel/coolant intermixing rates).

- Hydrogen formation is evaluated for current commercial light water reactors where the oxidation rate for the cladding material (Zircaloy) becomes significant at a temperature ($\sim 1200^{\circ}\text{C}$) well below its melting point ($\sim 1800^{\circ}\text{C}$). These rates are in contrast to those for the SRP reactors, where significant oxidation rates of aluminum require temperatures ($\sim 1400^{\circ}\text{C}$) that are well above the melting point for the fuel and the cladding material ($\sim 630^{\circ}\text{C}$). It follows that extremely fine particulation would be required to cause any significant H_2 production near the melting point of the reactor fuel material. However, explosive fuel/coolant interactions that result in such fine particulation would be self-limiting because of associated vapor production and therefore would result in relatively low conversion ratios in terms of H_2 or D_2 produced.

Furthermore, mechanistic considerations of the core melt progression suggest the absence of elevated temperatures approaching 1400°C . The occurrence of recriticalities with the highly enriched SRP fuel that could produce such temperatures would appear very unlikely since the fuel would not separate from the target material as the fuel meltdown process takes place.* Following fuel relocation, a recriticality event would therefore require the presence of the moderator dispersed in the molten fuel/target material, a condition that would be prevented by the inherent vapor production, which would keep the fuel and the moderator apart. At the same time, the fuel would be coolable by conduction as a result of its excellent thermal properties as long as an overlying layer of water is available.

In summary, mechanistic considerations suggest that relatively small quantities of H_2 or D_2 would be produced in case of a postulated severe accident. This conclusion is consistent with the SPERT reactor tests and the SL-1 incident, which involved meltdown of similar metal fuel and aluminum cladding in the presence of water.

*Considerations of the important role played by fission gas in metal fuel dynamics suggest that substantial mixing of the fuel and the target material would take place as a result of swelling or foaming of the fuel upon melting.

- Long-term debris coolability for the aluminum-uranium fuel in the confinement areas is expected. If water is present in these areas, the high thermal conductivity of aluminum-uranium fuel will result in adequate heat removal to the water. If no water is present, the high thermal conductivity of the aluminum-uranium fuel, combined with natural convection flows in the confinement, is expected to result in the capability to remove the decay heat from the fuel and prevent significant core/ concrete interactions.

- The critical system for determining the severe-accident airborne releases for the SRP reactors is the AACS. In particular, the AACS filters require a continued high flow of relatively cool air to prevent the filter heat loads from becoming excessive. Excessive heat loads in the filters could result in desorption of iodines previously trapped on the filters and/or ignition of the filters; in either case, the airborne releases could be quite large. The filter heat loads can be shown to be acceptable if the following conditions are met:

- Short-term operation of the RRSS to reduce the filter inlet air temperatures. Initiation of the RRSS requires a manual operator action. Operation of the RRSS is required between the time of initiation of core overheating and the time of failure of the reactor tank

- Long-term operation of the CHRS to maintain any core debris in the confinement in a coolable state. This condition ensures that the filter inlet temperatures will be maintained below the saturation temperature of steam (at or near atmospheric pressure). In addition, a coolable debris configuration ensures that the aerosol loading on the filters is not excessive, thereby preventing partial or complete blockage, which can reduce the air flows through the filters. Initiation of the CHRS requires manual operator action; long-term operation requires additional actions. The CHRS operation is required for a time period beginning prior to reactor tank failure and continuing for a period in excess of 35 days.

- Termination of the CWRSS to prevent draining of the CHRS input to the confinement. This action ensures that water will be present in the confinement for core debris cooling as discussed above. Termination of the CWRSS is an operator manual action that must be performed coincident with initiation of the CHRS

- Short-term operation of at least two exhaust fans and long-term operation of at least one fan. These fans ensure that sufficient air will be drawn through the filters to maintain filter cooling. The survivability of the fans in a severe-accident environment is questionable in their original design configuration; upgrades in the bearing lubricant and the cooling air supply have been previously recommended, and the implementation of these upgrades is assumed.

Independent analysis of the severe-accident progression and consequences has resulted in the definition of expected fission product releases (hereafter called source terms) for a limited range of possible severe-accident sequences. A catalog of expected source terms is provided.

Savannah River Plant Severe Accident Source Terms (% of total core inventory)					
Nuclide	Case 1	Case 2	Case 3	Case 4	Case 5
Xe-Kr	100	100	100	100	100
I-Cs	<0.01	<0.01	< 50	< 10	< 10
Te-Sr	<0.01	<0.01	< 50	< 10	< 10

where

Case 1 = AACS, RRS, and CHRS operating; CWRSS terminated.

Case 2 = AACS and CHRS operating; CWRSS terminated; RRSS failed.

Case 3 = AACS and RRSS operating; CHRS failed.

Case 4 = RRSS and CHRS operating; AACS failed; CWRSS terminated.

Case 5 = CHRS operating; AACS and RRSS failed; CWRSS terminated.

The mean value of offsite consequences, as predicted by the MAACS computer code, for the source terms given above were defined for the SRP site. The consequence analyses provide a risk value for each of the source terms; combining these consequence values with the probability of occurrence of each of the source terms, as determined from the severe-accident plant analysis, yields an overall risk value. Results of the scoping analyses show that the mean risk of acute fatalities for the public within one mile of the site was found to be several orders of magnitude below the DOE safety goal (DOE 1989), and the latent fatality mean risk within 10 miles of the site was found to be well within the DOE safety goal (DOE 1989). The scoping analyses also show that the DOE safety goals (DOE 1989) for protection of offsite populations can be met for a reasonable range of uncertainty in the severe-accident progression and consequences.

The subcommittee concluded that upgrading the RRS may be ineffective in reducing severe-accident releases. Scoping analyses performed as part of the SRP review and detailed severe-accident analyses performed as part of the SRP severe-accident analysis program indicate that the releases will be controlled by the performance of the AACS. For the AACS to perform according to its design basis, the incoming gases must be maintained at or near the saturation temperature of steam at atmospheric pressure. The RRSS is an integral part of the performance of the AACS during the severe accident when the core is overheating and melting in the reactor vessel. Analyses show that the present RRSS is capable of keeping the air/steam mixture in the inlet to the AACS at acceptable temperatures during this time period. Upgrading the heat-removal capability of the spray system would not significantly improve the performance of the AACS.

During its period of operation, the RRSS could remove radioactive materials from the process room atmosphere. The actual removal capability of the RRSS is a function of the assumed chemical composition of the radioactive materials. Noble gases are unaffected by spray system performance; elemental and methylated iodines are removed through adsorption onto the spray droplets, but the adsorption is significant only if there is a chemical additive (e.g., sodium hydroxide, sodium thiosulfate, hydrazine, etc.). Aerosols require impaction of the aerosol by the spray droplets. However, because of the high turnover rate of the process room air by the AACS, the residence time for radioactive materials in the process room is limited. The performance of the RRSS in removing radioactivity is therefore compromised by the high turnover rate.

The subcommittee concludes that releases with an AACS system that functions according to specifications will result in an acceptable offsite risk. Further, it is the opinion of the subcommittee that other means of mitigating the radioactivity releases associated with severe accidents should be considered, in addition to improving the RRSS, to determine the risk-reduction benefits and optimal improvements. The subcommittee believes that improvements to the reliability of the AACS, especially long-term operation, may provide a greater risk-reduction benefit than improvements to the RRSS (see recommendation Improved Reactor Room Spray).

B.7.2.4.2 Onsite Severe-Accident Assessment. In addition to the offsite safety assessment, an independent assessment of the safety of onsite personnel was made for severe-accident sequences. Specifically, the onsite dose rates and dose commitments from airborne releases and from direct radiation from the confinement building AACS filters were evaluated.

The whole-body dose to a person standing downwind from the stack under adverse meteorological conditions (Pasquill 1983) for a 100% core melt might exceed the lower bound of the lethal dose range (200 rem) for distances closer than one mile (for a 50%-power case, no potentially lethal doses would be predicted). Detailed calculations were not performed for very close distances; it is expected that potentially lethal doses would not occur within the first 50 to 100 m because of the stack elevation releases. We expect that the dose would not be near the potentially lethal range in the plant control room.

The whole-body dose rate to a person standing in direct line of sight of the AACS filters was also evaluated for a full-core-melt severe accident, assuming that the filters trapped all radioactive materials released from the core. At one hour after the accident, the dose rate at 300 m from the filters could be nearly 3,000 rem/h (controlled by iodines). After one year, the dose rate could decrease to approximately 200 rem/h (controlled by cesiums). Because of the geometry of the SRP plants, the control room is not in direct line of sight with the filter units (with the exception of the L Reactor). Taking into account the approximately 2 m of concrete between the control room and the filters or between the control room and the confinement structure, the dose rate in the control room

should be less than 50 mrem/h; the integrated dose rate over one month should be less than 5 rem.

B.7.2.5 Title 10, CFR, Part 100 Assessment

The NRC's siting criteria for commercial reactors, as contained in Title 10, CFR, Part 100 (NRC 1988d), require that offsite doses for a maximum hypothetical core melt accident be less than 25 rem whole body and 300 rem thyroid at the site boundary in the first two hours following the accident. The criteria also specify identical dose limits at the low-population zone in the first 30 days following the accident. For the Savannah River site, the site boundary and low population zone coincide at a point 4.5 miles from the center of C Reactor. Title 10, CFR, Part 100 (NRC 1988d) requires a conservative and nonmechanistic methodology, known as TID-14844 (Di Nunno et al. 1962), for evaluating compliance with the offsite dose criteria.

Information on the Savannah River reactors indicates that the Title 10, CFR, Part 100 criteria cannot be met for a maximum hypothetical reactor accident involving a 100% core meltdown as specified in TID-14844 (Di Nunno et al. 1962). The whole-body dose criterion is exceeded by a factor of approximately 9; the thyroid dose criterion is exceeded by a factor of approximately 4. The published information further concludes that the AACS filtration unit will meet its design basis for a 100% core melt (filter efficiency of 99.95% for iodine and 0.017% filter desorption) using TID-14844 (Di Nunno et al. 1962).

Independent calculations and evaluations, based on currently acceptable commercial LWR licensing practice (i.e., 1988), allow the conclusion that the offsite doses for a 100% core-melt accident exceed the Title 10, CFR, Part 100 (NRC 1988d) criterion by a factor of 5.5 for whole-body doses (controlled by noble gas releases); the offsite thyroid doses are only 28% of the Part 100 criterion. Sensitivity analyses performed to investigate design alternatives indicate that no feasible design options exist to permit the Title 10, CFR, Part 100 criteria (NRC 1988d) to be met using a 100% core melt. The only design modification that would permit meeting the Part 100 criterion for noble gases is a reduction of leakage from the confinement and termination of the AACS at core melt; this modification would also require modification to the filtration units to provide adequate cooling at the reduced ventilation air flows.

Independent evaluations performed on the filtration system indicate that it is expected to perform its intended function under the environmental conditions specified for the nonmechanistic accident sequence (see further discussion under Safety Goal Assessment).

B.7.3 RECOMMENDATIONS

B.7.3.1 Before Startup

- **Procedural Guidance**

- Reduce selected surveillance intervals for the following systems: ECS, CWRSS, CHRS, AIAS, CWS, RRSS, and rotovalves. Apply testing at quarterly intervals where possible and shutdown intervals (between charges) for systems not amenable to quarterly testing (see recommendation Procedural Guidance).

- Implement selected technical specification allowable-outage time requirements (i.e., restrict number of channel/components allowed in bypass or allowed to be out of service) (see recommendation Procedural Guidance).

- Update procedures/training for break isolation, ECS initiation, CHRS and RRSS actuation, and CWRSS termination for core-melt scenarios, and rotovalve closure on loss of loop flow (see recommendation Improved Training and Procedures).

- Review the onsite emergency plan for SRP personnel to ensure that adequate protection is afforded in the event of a severe accident (see recommendation Procedural Guidance).

- **Equipment**

- Demonstrate that the exhaust fans will continue to operate in the environment expected following an accident (see recommendation Confinement Exhaust Fan Design Review).

- **Other**

- The level 1 PRA should be used in the evaluation and prioritization of plant changes (see recommendation Procedural Guidance).

- Institute an inspection program to ensure the integrity of the CWS piping (see recommendation LOPA Event Frequency).

B.7.3.2 Long Term

- Complete the full-scope PRA and severe-accident analyses in an expedited manner (see recommendation Procedural Guidance)

- Demonstrate that the confinement will meet the DOE safety goals (DOE 1989), and confirm the subcommittee's findings (see recommendation Confinement Performance).

- Develop a program of component failure root cause analysis and feed the results back into plant maintenance (see recommendation Root Cause Analysis).

- Upgrade capacity of the CWRSS (see recommendation Sump Water Removal Capability).

- Reevaluate the improvement to the RRSS in light of the overall level of risk reduction afforded (see recommendation Improved Reactor Room Spray).

B.7.4 SUBCOMMITTEE ACTIVITIES

Members of the subcommittee made several visits to the SRP site to obtain information related to plant layout, system design, and operation, and to discuss PRA-related information with the PRA group. The primary interactions were as follows:

- December 6, 1988 - Meeting with SRP PRA personnel
- December 7, 1988 - Simulator tour
- December 8, 1988 - Plant walkdown
- January 10-11, 1989 - Meeting with SRP PRA personnel
- January 30-February 1, 1989 - Meeting with Los Alamos and SEA
(to discuss the Los Alamos independent risk assessment of SRP)
- Miscellaneous meetings with SRP PRA personnel following WISR
meetings in Aiken, S.C.

B.7.5 BIOGRAPHICAL INFORMATION

M. J. HITCHLER

Mr. Hitchler is manager of the Plant Operation and Risk Improvement Group in the Risk Management and Operations Improvement Group of Westinghouse Nuclear and Advanced Technology Division. He has managed and participated in more than 100 projects involving the application of probabilistic technologies to the nuclear industry. Mr. Hitchler has provided expert testimony and defense using probabilistic arguments before the NRC, Atomic Safety and Licensing Board, Advisory Committee on Reactor Safeguards, and other public forums. He has served on numerous industry standards, peer review, and technical conference committees that define the utilization of probabilistic methodologies to the nuclear industry. Mr. Hitchler has also been active on Atomic Industrial Forum and IEEE committees on the Development of Risk Criteria and the Utilization of PRA-Approach Licensing and is one of the members of the group that prepared the industry/NRC procedures guide under the sponsorship of ANS and IEEE. Mr. Hitchler has been in his current position for eight years and has been with Westinghouse for 14 years. He has a BS in mechanical engineering/nuclear engineering from Lowell Technological Institute and an MS in mechanical engineering from Carnegie-Mellon University. He has authored or coauthored a number of papers on reactor safety and risk assessment and is a member of the ANS, ASME, and the Society of Risk Analysis.

G. R. ANDRE'

Mr. André is a senior engineer in the Risk Management and Operations Improvement Group in Westinghouse Nuclear and Advanced Technology Division. He has experience in unavailability, severe-accident, support-state, and human reliability analyses and fault tree and operability tree techniques.

Mr. André has the lead responsibility on numerous projects including the level 1 PRA of the AP-600 advanced reactor design and the new production reactor. He has participated in numerous PRA studies and has coauthored nine PRA-related technical papers. Mr. André has also worked in the Advanced Energy Systems Division in thermal and fluid systems engineering and has coauthored two related technical papers. He has been with Westinghouse for nine years. Prior to joining Westinghouse, Mr. André was with Owens-Corning Fiberglas as an engineer in the Process Technology Laboratory supporting the development of new processes and the improvement of existing processes for producing glass fibers in manufacturing facilities. Mr. André holds a BS and MS in mechanical engineering and a BS degrees in physics from Rutgers University, is a licensed professional engineer in Pennsylvania, and is a member of the ASME.

B. G. CASSIDY

Ms Cassidy has been with the Westinghouse Risk Management Group for seven years. She has participated in a number of PRA studies. She has extensive experience in all phases of level 1 analyses. She has been responsible for the initiating events, accident progression (event trees), and quantification of dominant sequences. Ms Cassidy is responsible for all external event analyses and has performed a number of these assessments. She has also been responsible for the reactor pump seal LOCA model, anticipated transients without scram (ATWS) model, and mode-4 LOCA model for the Westinghouse Owners Group. She has coauthored seven PRA-related papers. Ms Cassidy has a BS in physics, is completing an MS in nuclear engineering from Pennsylvania State University, and has an MS in health physics from the University of Pittsburgh.

R. J. LUTZ, JR.

Mr. Lutz is a Fellow Engineer in the Risk Management and Operations Improvement Group of the Westinghouse Nuclear Safety Department of the Nuclear and Advanced Technology Division. He has extensive experience in the modeling and analysis of the progression and consequences of severe accidents, particularly the complex physical and chemical process that can occur during a core-melt sequence. Mr. Lutz has been the principal investigator for a number of commercial LWR severe-accident analyses and accident management activities including the Millstone Unit 3 and Beznau level 2 probabilistic risk assessment studies, the Seabrook and Ringhals (Sweden) development of severe-accident procedures, and special severe-accident-phenomena investigations for the Neckarwestheim and Muelheim-Kaerlich plants in the Federal Republic of Germany and the Sizewell B Plant in the United Kingdom. He was recently a member of the In-Vessel Expert Panel for the quantification of uncertainty for the NRC plant reanalyses. Mr. Lutz has worked in the Westinghouse Nuclear Safety Department for nearly 20 years and has authored or coauthored over 30 technical publications. He holds a BS in mechanical

engineering and an MS in engineering management from the University of Pittsburgh; he has also completed some graduate level studies in health physics.

M. D. ZENTNER

Mr. Zentner is currently manager of the Probabilistic Risk Assessment Section at Westinghouse Hanford. He has 14 years of experience in the nuclear industry and six years at the Hanford Site. Mr. Zentner's experience includes being lead engineer for the N Reactor Safety and Reliability Evaluation Program and a member of the independent safety review organizations at DOE and NRC nuclear facilities. He has established review programs at one DOE and one NRC reactor, was a senior reactor operator for the Advanced Test Reactor Critical Facility, investigated accident/unusual occurrences, and has been involved in a variety of projects sponsored by the DOE, the U.S. Department of Defense, and the NRC. Mr. Zentner holds an MS in nuclear engineering from the University of Washington, a BS in physics from Lewis and Clark College, and is a licensed professional engineer in Idaho.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

APPENDIX B.8 SAFETY ANALYSIS REVIEW

Tobias W. T. Burnett, Advisory Engineer, Nuclear Safety Department,
Westinghouse Nuclear and Advanced Technology Division
Timothy S. Andreychek, Engineer, Nuclear Safety Department,
Westinghouse Nuclear and Advanced Technology Division
Donald S. Love, Engineer, Nuclear Safety Department, Westinghouse
Nuclear and Advanced Technology Division
Robert W. Steidler, Advisory Engineer, Nuclear Safety Department,
Westinghouse Nuclear and Advanced Technology Division

B.8.1 SCOPE

We assessed the adequacy of the safety analyses performed for the SRP reactors, including the information derived from such analyses that may be used to assess the functionality and operation of reactor protection systems (scram and SSS) and engineered safety features; i.e., we reviewed the kinds of analyses customarily found in chapter 15 of a SAR for NRC-licensed facilities. We endeavored to answer two questions: Is there an appropriate selection of events to be analyzed? Are they appropriately evaluated?

The set of events we studied is commonly referred to as design-basis events. We feel that term can be misleading when applied to scenarios constructed long after a system was designed. In this appendix, we use the term evaluation-basis events for those closely defined events that are formally evaluated in accordance with a prescribed model to make decisions affecting permissible conditions of operation. In the body of the WISR report, this interpretation should apply wherever the term design-basis events is encountered.

B.8.2 OBSERVATIONS AND FINDINGS

B.8.2.1 Overview

This review has been conducted with the full cooperation of Du Pont personnel. The individuals with whom we spoke were very open and cooperative. Their observations were volunteered freely.

Compared to those at commercial power plants, the SRP reactors are extremely simple, permitting design and operation that minimize the frequency and consequences of malfunctions or errors. They are operated at low temperature and pressure and are closely coupled with their heat sinks (river water or cooling pond). They are thus exempt from transients caused by load perturbations. By the same token, they neither need nor have control systems for power,

pressure, or flow necessary to cope with load changes and are thus exempt from malfunctions of such systems.

The absence of the numerous and complex auxiliary systems found in a commercial power plant permits greater emphasis on the systems that do exist at SRP. As an example, the SRP main control board has a complete mimic panel for all fluid systems. This feature is not found in commercial nuclear power plants.

Under normal conditions or expected malfunctions, bringing an SRP reactor to a safe cold shutdown is simple, because of the low- temperature and -pressure operation, compared to the process involved at a commercial reactor. No change in system alignments is required other than to scram the reactor. Not a single valve or motor must change state. Further, loss of AC power poses no challenge to decay-heat removal. Emergency AC power is needed, however, for instrumentation, lighting, and ventilation, and for engineered safety features. Multiple, diverse safety systems for the reactor are provided. A redundant SSS for injection of soluble neutron poison has been added as a backup to scram of the safety rods. For all malfunctions and most postulated accidents (with the possible exception of large LOCA), either scram or SSS actuation would be expected to prevent any fuel damage. A best estimate suggests that specified acceptable fuel design limits could be violated if the scram rods failed and SSS worked, but that no fuel damage would be expected.

Protection is provided for every fuel assembly and is monitored by multiple outlet temperature detectors and by flow monitors. Multiple actuation devices (safety computers and gang temperature monitors) are also available for actuation of SSS as backup to the scram rods.

The Du Pont individuals we interviewed were extremely knowledgeable and competent in their fields. They were also clearly conscientious and took pride in their work. Their sense of professionalism was evident, and they do not appear threatened by the need to work under a new set of rules for safety oversight.

Overall, we found that the events analyzed to specify the safety set points (scram and SSS) were well selected, and the process for calculating and implementing them is satisfactory. The few exceptions are noted in the following sections.

A fixed set of evaluation-basis events is analyzed for each charge design to determine scram set points. The process used appears satisfactory; i.e., analyses are done in accordance with approved procedures, using, in most cases, documented computer codes with independent review and provisions for retrievability of results or their duplication at a later time. Formal review and approval of all inputs, as well as of the analysis methods, are also part of the process.

The safety record at the SRP reactors has been excellent. No radiological events have occurred to cause injuries to workers or excessive doses to the public. However, we have reviewed the safety analysis from the perspective of

commercial nuclear practice. Facilities under NRC license must provide a very visible demonstration of safety in the public record. That is, it is not enough to be safe; one must be able to point to documents of record that show safety margins and must be able to show that the plant is being operated in accordance with these formally documented safety analyses.

The SRP is moving to provide the documented and enforceable safety margins that are the practice in the commercial nuclear field. We endorse this effort.

Nowhere is the contrast between SRP and commercial nuclear practice more obvious than in the area of licensing documentation. In commercial practice, the licensing basis is found in the FSAR and its references. Operation is constrained by the plant technical specifications, which enforce the bases of the FSAR safety evaluation. The FSAR and technical specifications are subject to extensive adversarial review, approved, available in public records, and used as the basis for subsequent safety evaluations. At SRP, routine safety analyses are governed by internal technical manuals, and operations are limited by procedures written to implement technical specifications. Numerous analyses that have formed the basis for the present operating methods exist only in internal reports. Auditing of safe operation would be very difficult for a conventional regulator.

An SAR exists for SRP. It has recently been expanded to a ten-volume draft written in conformance with the NRC's regulatory guide for format and content. We reviewed it and found it a useful tutorial as an introduction to SRP safety analyses. But it does not claim to report the limiting analyses for actual operations; nor does this draft SAR have a standing in the hierarchy of SRP documents, and there is no existing schedule to use it. We consider Chapter 15 of that draft not very useful as a basis for making safety evaluations or establishing technical specifications. The information in the technical manuals and the training manuals is far more pertinent, but these documents do not present much of the information found in a typical commercial SAR.

B.8.2.2 General Safety Analysis Process (non-LOCA)

Reactor core protection limits are maintained by the protection system set points. Before 1987, such set points were more restrictive than either the transient protection limits (TPLs) or confinement protection limits (CPLs). To date, the TPLs have been more restrictive. The TPLs are calculated for each charge. The CPLs are calculated generically and repeated only when something changes. The process appears satisfactory; analyses are done in accordance with approved procedures, using documented computer codes, with independent review of the routine calculation and provisions for retrievability. Formal review and approval of all input is also performed.

Since 1987, LOCA limits have been more restrictive than either the TPLs or CPLs. Scram set points on assembly outlet temperature and SSS actuation

points are determined by the TPLs, CPLs, or LOCA operating limit, whichever is most restrictive. The process of implementing these setpoints appears satisfactory; the process, checks, and documentation are adequate to avoid errors.

For each charge, controlled documents indicate the TPL calculation and scram setpoints and reference the applicable CPL and LOCA analyses.

Within the last several years, LOCA analyses with more sophisticated models have established more restrictive limits for FI. This FI technology also applies to non-LOCA events and is expected to result in more restrictive TPLs and CPLs than those presently calculated. A LOCA is most sensitive to the penalty associated with the new FI technology, and setting operating limits based on LOCA therefore maintains safe operation. There is a long-standing intent at SRP to upgrade the non-LOCA analysis methodology and remove known non-conservatisms.

When non-LOCA analyses are judged by commercial nuclear practice, several weaknesses can be observed.

- Input assumptions are often best-estimate or nominal values and are not necessarily used to establish design or operating limits. That is, there is no assurance that actual operating conditions meet the assumptions used in the safety analysis. The SRP is now developing more formal technical specifications, similar to those used in NRC-licensed facilities. Assumptions employed in the safety analysis will be reflected in these technical specifications, and conservatisms must be used in the safety analysis to permit verification that plant operation meets the assumptions. Technical specifications for reactivity control, power distribution, and process water leakage are being developed and will be used for the next restart. Technical specifications for other areas will follow.

- Models and correlations used for present fuel design are not necessarily conservative. Current LOCA efforts have shown that existing thermal-hydraulic analyses are nonconservative. The more conservative subchannel analysis now being developed for LOCA is also expected to reduce the protection limits required for non-LOCA transients.

- In general, a wide variety of events is analyzed. However, there has been no visible mechanism to ensure that the selection of evaluation-basis events covers all events. Drop of a part length rod is not addressed: there is no justification provided as to why it is not credible, nor is there a claim that it is bounded by other events usually analyzed in a SAR chapter 15.

- The APOLLO code set, used to calculate TPLs, is considered obsolete and has modeling assumptions that are not defensible (e.g., correlations used to develop critical effluent temperatures). But there is no existing schedule to replace or defend it. The Reactor Technology Department has official responsibility for the code itself but some portions of the code are considered to be a 'black box' that is only addressed by SRL. The SRL personnel primarily utilize the newer AA3 code instead to analyze the same transients and to generate CPLs. Formalized procedures that would precipitate code change or defense appear to be lacking. In general, ownership of analytical methods and their use is scattered

too widely to facilitate management overview of routine safety analyses. Code ownership appears to follow the individual rather than the organization.

- There is no single source that documents the currently applicable safety analysis bases or sources. Such documentation would normally be the purpose of the SAR but such a SAR does not exist for SRP. The SRP management recognizes that generation of a SAR meeting the NRC's format and content guide is only a first step in establishing a SAR adequate to serve for safety evaluations.

- The various evaluation-basis events are not categorized with respect to frequency of occurrence. The ANSI-N-18.2 (ANSI 1973) classification system describes four "conditions of design," but these conditions are not applied in the actual analysis of evaluation-basis events. Lack of such classification makes it more difficult to determine the degree of safety margin appropriate for each event.

B.8.2.3 LOCA Findings

As noted before, the LOCA analysis methodology and supporting data base are in a state of development. The objectives of the development program are to define the acceptance criteria for the analyses; to define and develop models and methods that will conservatively predict the core response to a hypothetical LOCA; and to use the acceptance criteria, models, and methods to establish a defensible power level at which the reactor may be operated. The development program being executed by SRP personnel has a high priority in terms of program tasks, is reviewed at the highest level of SRP local management, and provides for input from technical experts in both industry and academe. In the past, there had been insufficient interaction between analysis development and the experimental programs, which led to inefficiencies in the test program and difficulties in analysis development. The SRP management recognizes the communication problem and has taken steps to alleviate it.

In general, we judge that the experimental programs are beginning to address the technical issues associated with the LOCA phenomena for SRP reactors (see Appendix B.9, and Section 9 of Part II).

Many of the test programs are quite mature, being in the later stages of implementing instrumentation and defining test matrices. The pace at which the programs are proceeding appears to be adequate to support restart of K Reactor. One possible shortcoming in the current heat-transfer test program is the use of fuel assembly simulators (heater assemblies) that have a nonprototypic thermal response. Consideration should be given to heat-transfer experiments using aluminum-heated surfaces that more closely simulate the actual thermal response of a fuel assembly under possible dryout conditions.

Previously, there had been little consideration of industry computer codes as alternatives to SRP-developed codes (for example, use of COBRA-NC instead of FLOWTRAN). The development, verification, documentation, and defense

of new codes is generally a costly and time-consuming process. The SRP management may wish to consider some industry codes as alternatives to further development of SRP codes.

Analysis methodology has not yet been established. Codes to be used have been identified in draft technical manuals, but these have not yet been approved by SRP management. Further, many input assumptions (Table B.8-1) have not yet been selected nor has the degree of conservatism to be applied for uncertainties. Also, the acceptance criteria for the long-term portion of the LOCA are not yet defined. Finally, the methodology and acceptance criteria are subject to change in the course of DOE oversight review. Thus, a final LOCA analysis is not yet in sight.

Our subcommittee makes no recommendation as to the degree of conservatism appropriate for the large-break LOCA analysis. Conservatism comparable with current commercial practice is relatively easy to define. However, there are significant differences between SRP and commercial reactors, such as low operating temperatures and pressures (no high-energy lines). In terms of these differences, LBB considerations could well justify less conservatism (see Appendix B.9). In all areas other than large-break LOCA, we have no hesitation in recommending that conservatisms be comparable to those in commercial practice (i.e., to provide a safety margin commensurate with expected frequency and to permit the generation of technical specifications to verify operation consistent with safety analysis assumptions).

B.8.2.4 Reactivity Insertion Accidents

A reactivity insertion accident (RIA) is a potential core-disruptive event for the SRP reactors if too much reactivity is added too quickly or if the event is not promptly terminated. None of the presently analyzed SRP reactivity addition events come anywhere close to being a core-disruptive RIA. Further, our review has not found any remotely credible RIA scenarios for the Mk22 core design as long as scram and SSS actuation are not delayed significantly. However, a mechanical failure of a part length rod drive mechanism can cause the rod to drop in less than one second from a high-worth to a low-worth region. Although the resulting reactivity addition does not lead to prompt criticality, this event is not analyzed, nor does it appear to be bounded by existing analyses. The present K Reactor restart program calls for a Du Pont and Westinghouse review of startup accident analyses including scenarios, likelihood, and comparison with commercial practice. This program provides a good opportunity to complete a broad review of reactivity accidents.

Because of the potential for serious consequences from RIAs, we believe that it is important to maintain and develop SRP expertise in the phenomenology and potential mechanisms for core-disruptive RIAs. Therefore, we commend the decision to include RIAs in the severe-accident program being conducted by

**Table B.8-1. Analysis Input Assumptions
to be Reviewed for Uncertainty.**

The list below covers analysis input assumptions (i.e., variables that generally are not calculated as part of individual safety analyses, as distinct from analysis model uncertainties). These items are plant parameters subject to verification by plant surveillance and are commonly incorporated in some fashion in plant technical specifications in NRC-licensed plants.

- Initial process conditions: reactor inlet temperature, process water pressure, assembly power, and flow rate
 - $q(r,z,t)$ = Time and spatially dependent power generation
 - $q(r,z)$ = Steady-state power generation
 - $dk(t)$ = Reactivity scram curve:
 - Number of stuck/inoperable rods
 - Initial flux shape (and calculated flux redistribution during scram)
 - $dk(t), SSS$ = Reactivity insertion for SSS
 - Protection system scram delay
 - Power shift during scram (if not part of scram curve)
- $P(t)$ = Pressure in top and bottom of tank (from TRAC or RELAP computer code)
 - Bingham pump characteristics, including two-phase air-water
 - Loop geometry (loss coefficients, elevations, momentum)
 - ECS injection head-flow curve
 - Plenum liquid level (from FLOOD84 computer code) as a function of assembly location and time
- Manufacturing tolerances.

The items below are reactor physics constants generally considered as analysis input assumptions. These are justified as part of the analysis methodology rather than plant surveillance:

- Reactivity coefficients
- Delayed neutron fraction and lifetime

Decay heat (now per ANSI-5.1 without uncertainties.)

SRL. This expertise and awareness should help ensure that such an event will not happen and is a useful addition to defense in depth.

B.8.2.5 Overpressure Protection

Neither the possibility nor the consequences of overpressurizing the vessel gas blanket space has been thoroughly explored. There may be significant implications of overpressure limits on other actual or postulated scenarios, and we feel that these implications require consideration (see Appendix B.2 and recommendation Gas Plenum Overpressurization).

Actuation of ECS appears to be the most likely way to pressurize the blanket gas space and perhaps cause the anchors to yield. In commercial practice, spurious ECS actuation would be considered an 'event of moderate frequency.' However, actuation of ECS at SRP during normal operation is benign since, with PWS pumps driven by their AC motors, plenum pressure is too high to permit discharge from the ECS into the PWS. The ECS actuation during shutdown, with PWS pump AC motors off, is a costly event; it would drain valuable D₂O, pressurize the system, and discharge radioactive tritium from the PWS. Documentation that we reviewed conflicted on whether the plenum roll anchors would yield for spurious ECS without the AC Bingham pump motors running. Further, other mechanisms could conceivably pressurize the gas blanket. These include transients with failure to scram (the basis for the confinement protection limits) and steam generation after shutdown (e.g., following LOPA with degraded or delayed ECS). Progress on operator emergency response procedures and on the severe-accident program will be hampered by lack of knowledge as to both the actual overpressure limits and the consequences of exceeding them. Leaks may simply open at the top of the moderator tank to relieve the pressure (see Appendix B.2 for a more complete discussion of this event).

B.8.2.6 Loss-of-Pumping-Accident Considerations

One of the major evaluation-basis events is the LOPA. Since the SRP reactors will not support natural circulation, loss of forced process water circulation requires ECS to provide core cooling. At present, the calculated power limit for LOPA is higher than for LOCA. However, ECS acceptance criteria proposed for LOCA must also be shown to be adequate for LOPA.

Potential causes of a LOPA include the following: large cooling water line rupture with flooding of the DC motors for the Bingham pumps (this is the evaluation-basis event; it places very stringent requirements on operator action); freezing of D₂O in the heat exchanger (D₂O freezes at 4°C); common-mode failure of DC motors or their supply, coupled with loss of the AC motors; common-mode closure of rotovalves in all loops; and plugging of all heat exchangers (e.g., with debris from another accident).

Current LOPA analysis does not consider driving forces from the natural convection of warmer water in the assemblies. At low ECS injection flows, we believe that these forces could cause the actual circulation patterns to deviate significantly from those predicted in the analysis. We believe that adequate core cooling would exist, but information displayed to the operator may not be as expected and could lead to confusion during recovery. We understand that SRP is reevaluating this incident and will examine the effects of thermal driving forces for various operator actions.

B.8.3 RECOMMENDATIONS

B.8.3.1 Prior to Restart

- **LOCA:** The LOCA methodology development now under way should be completed. Development should include selection of the analysis acceptance criteria, specification of the code sequence to be used, support from test programs as needed, justification of break location and size as 'worst appropriate case,' specification of failures to be assumed, selection of degree of conservatism (best-estimate vs 'two sigma,' etc), and perturbation analyses to support prescribed operator action, with allowance for operator error. The uncertainties listed in Table B.8-1 should be reviewed systematically to define the desired degree of conservatism (see recommendation Basis for Power Level).

- Evaluate the effects of possible nonconservatisms and uncertainties of the accident analysis methodology to justify a margin to be applied to the non-LOCA limits for both TPLs and CPLs. This evaluation should include both model uncertainties and nonconservatisms (APOLLO or AA3 vs FLOWTRAN computer code) and the analysis input assumptions shown on Table B.8-1. Justification for the adequacy of this margin for each event should be documented and approved by SRP management. We expect analyses of some limiting events (such as gang rod withdrawal and Bingham pump shaft shear) to be done as a necessary part of justifying the assigned margin. Also, we expect the assigned margin to limit power to about 60% to 80% power. The SRP management may wish to set this margin equal to the LOCA penalty at the time of restart (see recommendation Safety Margin Evaluation).

- As an interim measure, the margins assigned above should be applied in such a way that the scram and SSS actuation set points would continue to be conservative even if LOCA limits were removed. Procedures for establishing scram setpoints should be revised to incorporate this margin in calculating the non-LOCA limits (both TPLs and CPLs) (see recommendation Safety Margin Evaluations).

- Evaluate the consequences of the rapid drop of a part length rod (mechanical failure of drive mechanism), and complete the review of the reactivity addition events required by K Reactor restart task 3.1 of the DOE criteria (DOE 1988) (see recommendation Part Length Rod Drop).

- Complete K Reactor restart task DB-3.2 (DOE 1988), to establish reactivity control technical specifications, and identify a longer term process to implement technical specifications in other areas, specifically those in Table B.8-1 (see recommendation Safety Documentation).

B.8.3.2 Long Term

The following should be incorporated into the reactor safety improvement project program.

- As a long-term measure, the non-LOCA methodology should be upgraded to incorporate the new LOCA technology. At the same time, all input assumptions (see Table B.8-1) should be formally reviewed to ensure adequate conservatism to cover uncertainties and to permit verification that plant operation is in accordance with analysis assumptions. This review should include all related non-conservatisms (see recommendation Safety Documentation).

- The SAR should be established as the single document to reference all current safety analyses for each reactor. It should report current generic analyses and reference charge-specific reports.

- Safety analysis reports should be prepared in SAR style and format, and identify assumptions, methods of analysis, tabulated and plotted results, and conclusions.

- Checklists should be prepared identifying the range of applicability of generic analyses (see recommendation Core Charge Calculations).

- The basis for the dryout calculation (BOR) should be documented, since it was developed for an older, different fuel design. This process may require dryout tests on current fuel designs. Alternately, eliminate BOR as a core safety limit if it can be demonstrated always to be bounded by the FI limit (see recommendation Basis for Dryout Calculation).

B.8.4 BIOGRAPHICAL INFORMATION

T. W. T. BURNETT

Toby Burnett is an Advisory Engineer in the Westinghouse Nuclear and Advanced Technology Division with 26 years of experience in nuclear safety, including analytical, functional design, communications, licensing, and management. His primary area of expertise is in the transient analysis of PWRs and BWRs. His experience includes functional design of control and protection systems, computer modeling, extensive non-LOCA transient analysis, plant startup testing, licensing and hearing support, and technical liaison for public information and media relations. He has an MS in nuclear engineering from the University of Virginia and is a registered professional engineer in Pennsylvania.

T. S. ANDREYCHEK

Mr. Andreychek is currently a Principal Engineer in the Nuclear Safety Department of the Westinghouse Nuclear and Advanced Technology Division. He is working on developing improved LOCA models and methods for application to the SRP reactors. Mr. Andreychek's technical expertise is in thermal hydraulic tests and analyses associated with reactor safety. He holds both a BS and MS in mechanical engineering, and an MS in industrial engineering and engineering management, all from the University of Pittsburgh.

D. S. LOVE

Mr. Love is a senior engineer in the Nuclear Safety Department of the Westinghouse Nuclear and Advanced Technology Division. He currently works in the area of non-LOCA transient analyses where he provides training, development of current non-LOCA safety analysis codes, and technical support to both Westinghouse and utility personnel. Mr. Love graduated from the U.S. Naval Academy with a BS in mathematics and completed the Navy Nuclear Power School and Navy Nuclear Prototype training. His training includes four years of nuclear operating experience on Navy nuclear-powered surface ships.

R. W. STEITLER

Robert Steitler has been involved in a wide variety of transient analysis activities for more than 20 years. These have included the development of a process to define consistent reactivity input for transient codes, development of transient models for ATWS events, development of licensing strategies for ATWS, management of a group responsible for developing transient models for BWRs, responsibility for generation of plant technical specifications, and development of data bases to describe all the inputs and outputs associated with transient analyses and their impact on operations. He has a BS in engineering science from Iowa State University and an MS in nuclear engineering from Carnegie-Mellon University.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

APPENDIX B.9 POWER LIMIT AND ACCIDENT PROPAGATION

**Michael Epstein, Vice President, Fauske & Associates, Inc.
George H. Clare, Vice President, Fauske & Associates, Inc.
Robert E. Henry, Vice President, Fauske & Associates, Inc.**

B.9.1 SCOPE

This subcommittee was formed to review information and programs related to the resolution of LOCA issues and other issues that could limit the power level. Independent scoping calculations were performed to determine fuel performance following a postulated large-break LOCA, including consideration of both the FI and ECS phases. An approach to establish an acceptable power level was identified. We reviewed the LBB technology and assessed its applicability to the SRP reactors. We have provided a prognosis for establishing a practical power level.

We have also examined the phenomena following postulated blockage of a process assembly and whether such an event would propagate to involve an appreciable fraction of the reactor core.

B.9.2 APPROACH TO ESTABLISH ACCEPTABLE POWER LEVEL

B.9.2.1 Consideration of Candidate Design-Basis Events

Prior to shutdown in August 1988, the operating power level of the SRP reactors had been reduced in stages from 100% to approximately 50% as a result of concerns about ensuring reactor coolability following a DEGB of a pipe in the PWS.

Historically, the DEGB has been a design-basis accident for the SRP reactors. This position was established in the early years of reactor development, prior to the development and application of LBB technology. Leak before break means that if system components were to develop a crack, crack growth would be slow and result in penetration of the coolant boundary and a slow leak rather than propagating rapidly to the point of gross failure. The slow leak is detectable because of the tritium and provides adequate warning for an orderly reactor shutdown.

Increased knowledge of reactor materials and failure mechanisms and the development of sensitive leak-detection and warning systems have made the DEGB a decreasingly plausible event, even for high-energy cooling systems such as LWRs. The NRC has approved LBB as a basis for eliminating

jet-impingement barriers and pipe-whip restraints in 39 LWRs. However, the NRC still requires the ECS in those LWRs to be based on the presumption of a DEGB.

In a case much more pertinent to the SRP reactors, the NRC accepted LBB as a basis for establishing the design-basis leak for the primary coolant system in the CRBRP. At a maximum system pressure of about 200 lbf/in² (gage) and a coolant temperature below saturation, the CRBRP primary system was classified as a moderate energy system. The material of the system was stainless steel, and a sensitive leak-detection system was available for early identification of leaks. The CRBRP project satisfied all requirements for a construction permit, and the NRC had issued a safety evaluation report (NRC 1983) prior to project cancellation. Based on piping integrity, fracture mechanics material behavior, preservice and in-service inspections, and a sensitive leak-detection system, CRBRP was not required to analyze a DEGB as a design-basis accident. The design-basis leak for the primary coolant system transient analyses was 8 gal/min.

The SRP conditions pertinent to LBB are very similar to the CRBRP conditions. The system is low-to-moderate energy. The material is ductile and tough and subject to low stresses and considerably lower temperatures than CRBRP. Thermal and mechanical fatigue is low. Highly sensitive leak-monitoring systems are available based on detecting tritium in the heavy water. A thorough inspection program is being implemented prior to restart and an ISI program has been defined. One significant difference from the CRBRP is that the SRP reactors are subject to IGSCC. However, an evaluation of the impact of IGSCC on LBB shows that although IGSCC increases the probability of a leak, it does not invalidate the basic principle that a small leak will develop and will be detected long before a crack could propagate to the point of gross failure. On the positive side, the SRP reactors have demonstrated LBB during the course of their operation, including demonstration of the highly sensitive leak-detection system.

We find the arguments for LBB in the SRP reactors to be persuasive. We believe that a smaller leak than the DEGB is appropriate as the design-basis leak. The largest break credible under this analysis is failure of a bellows, resulting in a large leak with a 55-in² opening, which appears to be a rational choice for the design-basis leak in the PWS. This leak should be analyzed using conservative assumptions typical of design-basis accident analyses.

The LBB analyses result in a very low probability of a leak larger than the design-basis leak. Nevertheless, the spectrum of leaks up to the DEGB should be considered and analyzed in the context of the PRA. Such analyses normally employ realistic data and modeling.

Safety analyses include a spectrum of events other than LOCAs that can result in core transients and possibly limit the power. These include reactivity insertion events such as inadvertent control rod withdrawal and flow-reduction events such as the mechanical failure of a pump shaft. These events should be

analyzed using conservative assumptions typical of design-basis accident analyses.

Leaks larger than the design-basis leak normally would not be considered in establishing operating constraints. However, it is important to recognize that the LBB position is still under review. Until the LBB position has been accepted, it is prudent to establish a power level at which we would expect core coolability even for a DEGB, based on analyses using realistic data and modeling.

Application of such an approach would result in the power level's being established based on the most limiting of the following evaluations:

Events	Evaluation basis
Design-basis leak (55-in ² opening)	Conservative
Leak beyond design basis (up to DEGB)	Realistic
Non-LOCA flow and reactivity transients	Conservative

B.9.2.2 Prognosis for Establishing a Practical Power Level

It was beyond the scope of our subcommittee to define an operating power level. Considerable analysis and testing currently in progress are expected to support a power-level determination in the relatively near term.

Our review of previous and ongoing work, along with some independent assessment (described below), leads us to believe that a practical power level is achievable.

Because of the focus to date on the DEGB, not much attention has been given to the analysis of the 55-in² break, associated with failure of a bellows. However, based on parametric analyses of a spectrum of leak sizes and locations, we expect a conservative analysis of the 55-in² break to show that the break can be accommodated for power levels at or near 100%.

Evaluation of very large leaks, up to and including the DEGB, requires consideration of two critical times during the event (Figure B.9-1):

- Power-to-flow mismatch during early depressurization, referred to as the FI phase
- ECS equilibrium phase.

These phases are addressed separately below.

B.9.2.2.1 Flow Instability Phase. The postulated large-break LOCA results in a sudden decrease in the inlet plenum pressure from about 100 lbf/in² (absolute) to 55 lbf/in² (absolute) and a corresponding flow reduction in the reactor assembly flow of about 40%. The reactor power, however, would remain close to nominal for about two seconds before the reactor is shut down by rod motion. This delay in shutdown and the resulting power-to-flow mismatch

78904044.6M

Figure B.9-1. Schematic of Power and Flow Decay for a Large-Break Loss-of-Cooling Accident.

would result in conditions that satisfy the requirements for fundamental Ledinegg boiling FI (Figure B.9-2) if initial power were 100%.

For a given power level, as long as the coolant is subcooled, the flow decreases monotonically with decreasing pressure drop across the core (from A to B in Figure B.9-2). However, for flows less than that resulting in bulk boiling (point B of Figure B.9-2), the large liquid-to-vapor density ratio of the water coolant at low pressure would cause a large volume change and corresponding rapid changes in two-phase momentum and frictional pressure drops. If the available pressure drop across the core remained constant at about 25 lbf/in², the flow would decrease rapidly to point C. However, as the flow to the core is decaying rapidly, the pressure in the inlet plenum would have to increase quickly to about 130 lbf/in² (absolute) to accommodate most of the primary flow through the break. This redistribution in pressure would lead to a flow excursion, ending at point D rather than at point C of Figure B.9-2.

Clearly, at point D, the heat removal is largely by latent heat of vaporization as compared to sensible heat at point A. To estimate the heat-removal

78904044.4M

Figure B.9-2. Flow Versus Pressure-Drop Stability Considerations for Savannah River Plant Mark 22 Core Configuration.

capability corresponding to point D of Figure B.9-2, we will consider the limiting condition of saturated vapor flow leaving the active fuel region. Assuming an inlet temperature of about 30°C and an assembly power of 6.5 MW, the flow required per assembly would be 2.4 kg/s, which corresponds to a mass flow rate of 733 kg/m² · s in an Mk22 assembly. Considering vapor choking at the exit of the fuel region, a vapor flow rate of 733 kg/m² · s would correspond to a critical pressure of 40 lbf/in² (absolute). At this pressure, the vapor-specific volume would be 0.67 m³/kg. The pressure drop across the core can be estimated* from

$$\Delta P_c = \Delta P_M + \Delta P_F$$

* Because of the reduced liquid flow (<10% of nominal flow across the core), inlet losses will be negligible.

$$\Delta P_c = \Delta P_M + \Delta P_F$$

where

$$\Delta P_M = G^2 \Delta v \approx 733^2 \cdot 0.67$$

$$\approx 3.6 \cdot 10^6 \text{ Pa} = 52 \text{ lbf/in}^2$$

$$\Delta P_F = \frac{1}{2} f \frac{G^2 \bar{v} L}{R_H}$$

$$\approx \frac{1}{2} (0.005) \frac{733^2 \cdot 0.15 \cdot 3.8}{3.4 \cdot 10^{-3}}$$

$$\approx 2.2 \cdot 10^6 \text{ Pa} = 32 \text{ lbf/in}^2.$$

The above calculation results in a plenum pressure requirement of about 120 lbf/in² (absolute), which compares to the anticipated available pressure of 130 lbf/in² (absolute), which would be sustained as long as single-phase flow is pumped from the reactor tank (at least 10 to 15 s). It follows that the onset of FI in connection with a postulated large-break LOCA will not lead to overheating of the fuel prior to reactor scram (approximately 2 s). However, until experiments become available to confirm these calculations, we recommend a conservative value of about 50% of nominal power for the purpose of reactor startup. For this power level, the required inlet pressure to remove the heat by latent heat of vaporization is estimated to be only about 60 lbf/in² (absolute).

It is important to note that such experiments should emphasize the flow excursion and the subsequent two-phase-flow heat-removal capability in addition to observing the onset of the FI. In other words, a success criterion that bases a safe power level on the onset of FI rather than on the two-phase cooling mode following the flow excursion would appear to be unnecessarily conservative considering the very low probability of the postulated large-break LOCA and the short duration before the reactor scrams.

B.9.2.2.2 Emergency Cooling System Phase. During the equilibrium-ECS phase of the accident, the downward flow in the process assemblies is largely dominated by gravity and is complicated by possible gas entrainment. Furthermore, flow distribution among assemblies as well as among channels and subchannels within each assembly can vary substantially. Analyses as well as isothermal experiments suggest a lower limit of the assembly flow (20 gal/min) during the ECS phase, a flow that is more than sufficient to remove the decay heat as sensible heat (i.e., in the absence of net steam production). As such, the isothermal measurements suggesting an essentially even flow split among the three principal coolant channels for assembly flows larger than 20 gal/min should also apply to reactor or heated conditions. Unfortunately, the same cannot be claimed for subchannel flow distribution within a given coolant channel, since

gravity-driven downward flow appears to be inherently unstable on a subchannel basis. The latter phenomenon can be significantly affected by the "interconnected channel effect" under prototypic heating conditions. The presence of power tilting for most of the assemblies suggests that different flow regimes can persist in adjacent subchannels, with most of the coolant flowing down the lower power subchannels as long as bulk-boiling conditions are not reached in these channels.

As illustrated in Figure B.9-3, basic flooding considerations suggest that net steam generation for power levels of interest will lead to water expulsion. Process assembly flows in excess of 10 gal/min will prevent this phenomenon from occurring. It should also be noted that process assembly flows in excess of 20 gal/min result in essentially even distribution of flow among assembly channels.

78904044.1M

Figure B.9-3. Minimum Water-Supply Rate versus Process-Tube Energy-Input Rate to Maintain Cooling and Avoid Water Expulsion (curve based on the Wallis flooding correlation).

Fortunately, a technically defensible power limit of practical interest can be established by recognizing that the controlling mechanism and associated power limit are closely tied to the highly conductive fuel material; i.e., a detailed knowledge of the flow distribution within a coolant annulus is not required. An example of an extreme or worst-case coolant distribution among subchannels within a given assembly is shown in Figure B.9-4. Even for this case, where the coolant is largely limited to only one out of the four subchannels within a given coolant channel, the maximum temperature in the nonwetted portion is below the fuel-melting temperature because of the highly conductive nature of the SRP fuel (see Figure B.9-4). At 50% of nominal power, the maximum fuel temperature is limited to about 350°C, which is well below the fuel failure threshold value at which fission products migrate (~450°C) or fuel melts (~630°C).

However, the most compelling evidence that SRP reactors can be operated safely at practical power levels can be obtained from past experience related to successful discharge cooling of the extremely high-power density Mk18 assemblies. As can be seen from Table B.9-1, even if these assemblies were discharged from the reactor 3 h after shutdown (i.e., at a decay heat level of 0.3%), the power conditions are remarkably similar to the Mk22 assemblies for the postulated large-break LOCA. Furthermore, the discharge machine coolant flow of about 8 gal/min results in a very similar power-to-flow ratio. Based on these similarities, including geometric considerations such as hydraulic radius and surface heat flux (see Table B.9-1), we conclude that safe operation can be argued at least at the 50% power level. In fact, the suggested low limit of 5 gal/min for the discharge machine coolant flow suggests a power-to-flow ratio equivalent to 100% power operation of the Mk22 assemblies.

In summary, with a minimum flow of about 20 gal/min to the process assembly during the ECS phase, a power of at least 50% of nominal full power is believed to be technically defensible based on the above analysis and available experience with postdischarge cooling. In this context, it would appear necessary to reexamine current as well as future experiments to ensure at least prototypic conditions equivalent to those reflected by the postdischarge cooling experience. Testing in multiple annulus geometry may demonstrate that the power removal capabilities are largely independent of the flow distribution in both the subchannels and the coolant channels. Simply ensuring sufficient overall assembly flow to remove the heat by subcooled water may be adequate.

B.9.2.2.3 Non-Loss-of-Cooling-Accident Flow and Reactivity Transients. Certain non-LOCA flow transients, such as the mechanical failure of a pump shaft, could encounter an FI phase. However, the condition would certainly be less severe than the transient associated with a DEGB. Based on analyzing the non-LOCA flow and reactivity events conservatively, it is anticipated that a power of at least 60% to 80% of nominal power can be shown to be acceptable for these events.

$L = 0.15 \text{ m}$, Maximum non-wetted perimeter of fuel.

100% power level (4% decay heat)

$$T_{\max} = T_c \frac{L^2 Q}{8k} = 100 + \frac{0.15^2 \cdot 3.6 \cdot 10^7}{8 \cdot 200}$$

$$\approx \underline{600^\circ\text{C}}$$

50% power level:

$$T_{\max} \approx \underline{350^\circ\text{C}}$$

78904044.9M

Figure B.9-4. Schematic of a Cross Section of a Mark 22 Assembly Indicating Worst-Case Subchannel Coolant Distribution. Note that with this distribution (all other subchannels are assumed dry), only 3/8 of the fuel element's perimeter is in contact with the coolant. Note also that the concentrated heat flux in the liquid-filled subchannels is well below the critical heat-flux limit; i.e., dryout in these channels is not predicted. Furthermore, flooding or expulsion will not occur as long as bulk boiling conditions are not reached.

Table B.9-1. Comparison of Discharge Cooling of High-Power Density Mark 18 Assemblies to That Expected for Mark 22 Assemblies (50% of Full Power) Following a Large-Break Loss-of-Cooling Accident with Emergency Cooling System Actuation.

Assembly type	Mk18	Mk22
Hydraulic radius (cm)	0.32	0.34
Core length (cm)	183	381
Power (MW)	20	3.25 (50%)
Time after shutdown (s)	10,800	30
Decay fraction (%)	0.3	4
Assembly specific power (kW/ft)	10	10.4
Power/flow [kW/(gal/min)]	7.5 ^a	6.5
Surface heat flux (W/cm ²)	3	4

^aA limiting value of 12 was suggested for the discharge requirement, which compares to an Mk22 limiting value at full power (6.5 MW) of 13.

Larger leaks are highly improbable and should be evaluated using realistic data and modeling. Until the LBB review has been completed and the position accepted, it is prudent to establish a power level such that core coolability would be expected even for a DEGB, based on analyses using realistic data and modeling. Non-LOCA flow and reactivity transients must also be evaluated conservatively to assess any limitations on power level (see recommendation Basis for Power Level).

Of all of these events, our review indicates that the most limiting is likely to be the DEGB, which should be evaluated using realistic assumptions. An approach to such analyses was presented. We believe that power levels of 50% or more can be defended based on current data and analytic capabilities. Forthcoming prototypic experiments are likely to demonstrate the acceptability of higher powers, even approaching 100% (see recommendation LOCA Experimental Program).

B.9.3 ACCIDENT PROPAGATION FROM LOCAL FAULTS

B.9.3.1 Overview

The possibility of a local fault, such as an inlet blockage of a process assembly and subsequent fuel meltdown leading to a whole-core accident, is of fundamental importance to the overall safety assessment of SRP reactors.

A sudden and relatively large inlet blockage is believed credible only during startup of the reactor, while a slowly developing blockage may be possible during normal operation. Since both flow and temperature are monitored in each process assembly, the occurrence of such events would lead to reactor shutdown. In the case of a complete inlet blockage, decay heat alone would be capable of voiding the assembly; this situation would be followed by overheating, fuel melting, and relocation.

In examining the behavior of the metal fuel material within the assembly following the postulated flow blockage in the inlet region of the assembly, the important role played by fission gas in metal fuel dynamics must be recognized. Fuel overheating would lead to rapid evolution of matrix fission gas once the fuel melting point is exceeded, resulting in radial expansion of the fuel melt. The concentric-ring design of the Mk22 assembly would cause the expanding fuel to accumulate on the inside and outside surfaces of the outer and inner target material rings, respectively. The fuel would freeze rapidly because of the relatively cold target, then remelt, melting the target material and mixing with it while draining to the bottom of the assembly. Detailed considerations of these processes suggest that the substantial mixing of the fuel and the target material will take place as a result of swelling or foaming of the fuel upon melting; i.e., the fuel would not separate from the target material as the fuel meltdown process takes place. Consequently, any significant reactivity addition or the occurrence of recriticality in connection with fuel meltdown and relocation can probably be ruled out.

The potential for fuel relocation within the incident assembly as well as outside the assembly in the moderator space depends largely on the power level. At decay power levels, the refreezing of the draining fuel/target material would prevent this material from advancing very far below the melting zone, and since refreezing would occur in considerably less time than fuel heating and subsequent fuel melting, frozen fuel/target buildup would occur. That is, the draining rate of melted fuel/target material at decay power would be so slow compared to the rate at which it would refreeze that the potential for a completely refrozen fuel/target blockage of the assembly channels would be high. Moreover, owing to the high thermal conductivity of the fuel/target material, the dense frozen block of fuel/target material subject to decay heating would be coolable inside the process tube by the surrounding D₂O moderator. It follows that whole-core involvement would not occur as a result of the inlet flow blockage and subsequent meltdown process.

However, if the power level is assumed to remain near full power during the meltdown process, sustained fuel/target draining would seem inevitable and would result in the relocation of most of the assembly fuel/target material to the bottom of the reactor tank, where it would undergo thermal interactions, breakup, and quenching. While the potential would exist for transferring the fuel/target material to the active moderator region, thereby possibly adding reactivity, the time scale for such a postulated scenario would be well beyond the anticipated reactor scram time. Since the negative reactivity associated with reactor shutdown would be more than enough to counteract the most pessimistic configuration associated with fuel relocation, even assuming separation between fuel and target during meltdown, we conclude that a whole-core event can be ruled out.

B.9.3.2 Initial Fuel/Target Behavior Within a Blocked Savannah River Plant Assembly

In examining the initial behavior of metal fuel material within a process tube (assembly) following a hypothetical flow blockage in the inlet region of the assembly, the important role played by fission gas in metal fuel dynamics must be recognized. Fuel overheating will lead to rapid precipitation of large quantities of matrix fission gas once the fuel melting point is exceeded, resulting in radial expansion of the fuel melt. The concentric-ring design of the assembly demands that the expanding fuel accumulate on the inner and outer surfaces of the outer and inner target material rings, respectively. Thus there exists a strong potential for the fuel to melt the target material and mix with it while draining to the bottom of the assembly. The neutronic history of the flow blockage accident is intimately related to the degree of mixing between fuel and target material. It is demonstrated below that substantial mixing of these materials is likely to take place as a result of swelling or foaming of the fuel upon melting.

Figure B.9-5 shows schematically and sequentially the physical nature of the fuel/target materials heat-transfer and mixing problem. Under full-power conditions the fission gas will evolve in an almost explosive manner. Accordingly, it is reasonable to assume that the molten fuel will be driven in both the positive and negative radial directions such that half the fuel-melt deposits are on the inner target and half are on the outer target. It follows from the total fuel-volume inventory that, on average, a 4-mm-thick fuel layer will deposit on the inner target while a 2-mm-thick fuel layer will deposit on the outer target. The fuel is cooled rapidly by conduction to the cold target structures, temporarily forming a frozen fuel layer that clings to the target surface, as shown in Figure B.9-5.

78904044.3M

Figure B.9-5. Illustration of events leading to dilution of fuel by mixing with target material.

This preliminary freezing stage of the target/fuel mixing process is substantiated by consideration of the solidification rate

$$\delta \approx 2\lambda\sqrt{\alpha t}$$

where

δ = the instantaneous thickness of the frozen fuel deposit)

α = the thermal diffusivity of the deposit ($\sim 6.4 \times 10^{-5} \text{ m}^2 \cdot \text{s}^{-1}$)

λ = is the so-called growth constant (~ 0.75 for fuel solidification on target substrate at 100°C)

t = time.

The time required to bring the frozen fuel back up to its melting temperature at full power is about 1.0 s, as compared to the period of freezing of about 0.1 s for the fuel deposited on the inner target and 0.03 s for the fuel deposited on the outer target.

Ultimately, internal heat generation will begin to reheat the fuel deposit. This heat will also be conducted into the target substrate, causing its temperature to rise as well. The fuel deposit will melt before the underlying target material undergoes substantial melting. Thus the most likely picture at this point is that

of a draining film of remelted fuel along a vertical wall of target material, as shown in Figure B.9-5.

Clearly, the time of target melting cannot be longer than the time required for the temperature profile within the target material to become uniform. From heat-conduction theory this time is given approximately by the equation

$$t = 1.5 \delta_T^2 / \alpha$$

where

δ_T = the thickness of the target material

From this expression we estimate that complete melting of the inner target ring will follow the melting of its fuel deposit by only 0.47 s. The time lag between melting of the outer target ring and its fuel deposit is estimated to be only 0.1 s.

The film drainage equation for turbulent flow is

$$u \sim (2 g \delta / f)^{1/2}$$

where

u = the drainage velocity

f = the wall friction factor (~ 0.1)

δ = the thickness of the film.

This expression reveals that the remelted fuel on the inner target drains, at most, a distance of 1.3 m before the melting of the target material is complete. Melting of the outer target will take place before the fuel film drains 0.2 m. These results, when compared with the 4.0-m length of the active fuel region, suggest that both the fuel and target material will become molten before a significant fraction of the fuel is removed by gravity from the active core region.

It is clear from the above arguments that the most likely fuel removal (draining) configuration for most of the fuel inventory within the assembly is one in which two parallel vertical streams of fuel and target material flow side by side toward the bottom of the assembly, as shown in Figure B.9-5. The two streams will mix as a result of an instability mechanism of the Kelvin-Helmholtz type. It can be shown that the time it takes to mix the two streams is on the order of $t \sim \delta/u$, or about 4 m·s. Indeed, rapid mixing of the target and fuel streams is anticipated.

B.9.3.3 Fuel Motion Within a Blocked Savannah River Plant Assembly

The previous section addressed the incipient fuel motion and the subsequent mixing of the fuel with the target material. This section demonstrates that if the power level in the blocked assembly is at decay heat level, the rapid solidification of melted fuel is likely to result in the formation of a coolable fuel agglomerate. That is, the fuel is not expected to leave the assembly at low power

levels. However, at high power levels fuel draining is inevitable and should result in the relocation of most of the molten fuel to the bottom of the reactor tank. To simplify the analyses, only the fuel rings are considered below. However, the basic conclusions would not change if the target material were included.

B.9.3.3.1 Fuel Motion at Low Power Levels. The first consideration is the drainage process that would occur as the concentric cylindrical shells of fuel are melted by internal heating at low power levels. The maximum rate at which the fuel melts down may be estimated by equating the decay energy input rate to the latent heat-release rate

$$\dot{m} h_{fs} = \dot{Q} \quad (9-1)$$

where

$\dot{m}$ = the rate of fuel melting ($\text{kg} \cdot \text{s}^{-1}$)

h_{fs} = the latent heat of melting

$\dot{Q}$ = the decay heat rate for a single assembly ($\text{J} \cdot \text{s}^{-1}$).

Substituting the decay heat rate $\dot{Q} = 2.6 \times 10^3 \text{ J} \cdot \text{s}^{-1}$ and the estimate $h_{fs} = 3.2 \times 10^5 \text{ J} \cdot \text{kg}^{-1}$ into Equation 9-1 yields

$$\dot{m} = 0.81 \text{ kg} \cdot \text{s}^{-1} \quad (9-2)$$

for the fuel assembly meltdown rate

Under the influence of gravity, the fuel will drain downward. It is reasonable to assume that the fuel will flow as films over the relatively cold fuel concentric-cylindrical structure (rings) located below the zone of melting. Assuming that the thicknesses of the films are spatially uniform and that the films fall in laminar flow, the instantaneous average length of the films, X , within the assembly is given by the differential equation

$$\frac{dX}{dt} = \frac{\rho g \delta^2}{3\mu} \quad (9-3)$$

where

δ = the instantaneous average thickness of the draining fuel films

g = the gravitational constant

ρ = the density of the molten fuel material

μ = the viscosity of the molten fuel material.

The mass rate of draining must be equal to the rate of melting, so that

$$\dot{m} = \rho C \delta \frac{dX}{dt} \quad (9-4)$$

where

C = the wetted perimeter of the fuel assembly structure.

Eliminating δ between Equations 9-3 and 9-4 and integrating the result gives

$$X = \left(\frac{g \dot{m}^2}{3 \mu \rho C^2} \right)^{1/2} t \quad (9-5)$$

for the instantaneous film length as a function of time. The average film thickness can be estimated by eliminating dX/dt between Equations 9-3 and 9-4 to obtain

$$\delta = \left(\frac{3 \mu \dot{m}}{\rho^2 C g} \right)^{1/2} \quad (9-6)$$

Now, the total wetted perimeter of the concentric fuel cylinders within the assembly is $C = 0.83$ m. Using the property estimates $\rho = 3.6 \times 10^3 \text{ kg}\cdot\text{m}^{-3}$ and $\mu = 2.9 \times 10^{-3} \text{ kg}\cdot\text{m}^{-1} \text{ s}^{-1}$, we estimate from Equation 9-6 that the average thickness of the drainage fuel films is $\delta = 0.41$ mm. This film is rather thin and is not likely to flow very far before it refreezes on the cold-fuel surface just below the melting zone. In fact, the refreezing process can result in the blockage of the assembly channels (see below).

The familiar square-root crust growth law for the instantaneous thickness of the frozen material, δ_s , namely

$$\delta_s = 2\lambda \sqrt{\alpha t} \quad (9-7)$$

can be used to predict, approximately, the fuel refreezing rate. The quantity λ is the growth constant, which is a function of the physical properties and initial temperatures of the draining melt and substrate solid materials and α is the thermal diffusivity of the fuel material. For the sake of simplicity, it is assumed here that the physical properties of these materials are the same. For the case of fuel melt refreezing by conduction of heat into an underlying fuel cylinder subcooled not more than about 200°C below the melting point of the fuel, λ is well represented by the expression

$$\lambda = \left(\frac{c\Delta T}{2 h_{fs}} \right)^{1/2} \quad (9-8)$$

where

c = the heat capacity of the fuel material

ΔT = the subcooling of the fuel substrate.

The characteristic time for freezing of the draining fuel films is, then, from Equations 9-7 and 9-8 and the condition $\delta = \delta_s$,

$$t = \frac{\delta^2 h_{fs}}{2c\alpha\Delta T} \quad (9-9)$$

Substituting the previous estimate $\delta = 0.41 \text{ mm}$; together with the property estimates $c = 0.753 \times 10^3 \text{ J}\cdot\text{kg}^{-1}\cdot\text{K}^{-1}$, $\alpha = 4.06 \times 10^{-5} \text{ m}\cdot\text{s}^{-2}$, and a fuel structure subcooling of $\Delta T = 10\text{K}$, into Equation 9-9, we find that the draining fuel will refreeze in 0.012 s. This time should be compared with the time it takes internal heating to raise the fuel temperature $\Delta T = 10^\circ\text{C}$, namely 0.46 s. Equation 9-5 reveals that the melt film drains a distance of only 7.8 cm at the instant it is frozen in place. Of course, molten fuel is supplied continuously to the refreeze zone by decay heating. Since the refreezing of the draining fuel prevents the fuel film from advancing very far below the melting zone, and since refreezing occurs in considerably less time than heating and subsequent fuel melting, radial frozen fuel buildup must occur. The final thickness of the refrozen fuel is limited by the heat capacity of the intact underlying fuel-ring structure. Therefore the draining rate of the melted fuel material is so slow compared to the rate at which it refreezes that the potential for a complete refrozen fuel blockage of the assembly channels is high. The presence of water just below the melting zone would aid the refreezing process and practically ensure that all the 'void space' left by the receding water is filled with refrozen fuel.

It is necessary to determine whether the dense frozen block of fuel that fills the entire assembly cross section is coolable by the surrounding heavy water bath. It can readily be shown that the temperature at the center of an internally heated cylinder of radius R is

$$T_c = T_o + \frac{Q_v R^2}{4k} \quad (9-10)$$

where

T_o = the temperature at the surface of the cylinder

Q_v = the volumetric heat generation rate $\text{J}\cdot\text{m}^{-3}\cdot\text{s}^{-1}$

k = the thermal conductivity of the cylinder (refrozen fuel).

A simple energy balance indicates that the heat flux q at the surface of the cylinder is

$$q = \frac{1}{2} R Q_v \quad (9-11)$$

For the blockage to be stable, the heat flux q cannot exceed the critical nucleate boiling heat flux of water of approximately $q = 2 \times 10^6 \text{ J}\cdot\text{m}^{-2}\cdot\text{s}^{-1}$. The corresponding internal heating rate is obtained from Equation 9-11 and, since $R = 0.052 \text{ m}$, is $Q_v = 7.7 \times 10^7 \text{ J}\cdot\text{m}^{-3}\cdot\text{s}^{-1}$. This result represents about 5.1% of

full power. It follows from Equation 9-10 (with $k = 120 \text{ J}\cdot\text{m}^{-1}\cdot\text{s}^{-1}\cdot\text{K}^{-1}$ and $T_0 = 100^\circ\text{C}$) that the temperature at the center of a dense blockage subject to this internal heating rate is 534°C , which is about 130°C below the fuel melting point. Based on the estimates obtained in the foregoing, we can conclude that a complete assembly blockage of refrozen fuel is coolable for power levels below 5.0% of full power.

B.9.3.3.2 Fuel Motion at High Power Levels. Repeating the calculations of the preceding section for full power conditions, we can predict that the draining fuel-melt films are, on average, 1.2 mm thick and traverse a distance of 4.2 m in 0.74 s before resolidifying. This distance exceeds the 4.0-m length of the active fuel region. Moreover, the resolidification time, again based on the fuel subcooling $\Delta T = 10^\circ\text{C}$, is much greater than the 0.018 s required for the full-power heating rate to 'absorb' ΔT . Thus, while the axial power variation may result in the formation of temporarily frozen fuel rivulets that cling to intact fuel rings, at full power all refrozen and intact fuel will be quickly melted and moved under gravity toward the bottom of the process tube.

The draining fuel is likely to follow the normal flow path through the bottom fitting of the process tube (Figure B.9-6). The fuel will first accumulate in the plenum located between the bottom of the active fuel zone and the pressure plate shown in Figure B.9-6. The plate will present some initial resistance to the downward flow of fuel, as the fuel must flow through the twenty-four 0.368-in.-dia holes that penetrate the plate. However, the plate will be quickly 'wiped away' by very rapid ablation by the fuel flow through the holes.

The proposed plate-melting process is illustrated in Figure B.9-7 and involves the melting of the edges of the holes by immersing the plate in a laminar flow of hot liquid having thermophysical properties similar to those of the plate metal (aluminum). From boundary-layer theory, the heat flux $\dot{q}$ to the edge of a hole through which molten fuel, superheated above its melting temperature by ΔT degrees, flowing with velocity u is

$$\dot{q} = 0.332 \text{ Pr}^{1/3} k \Delta T \left(\frac{u}{\lambda v} \right)^{1/2} \quad (9-12)$$

where

k = thermal conductivity

v = kinetic viscosity

Pr = Prandtl number of the flowing melt

δ = the thickness of the plate through which the hole is drilled.

78904044.10

Figure B.9-6. Typical Bottom-Fitting Insert. Arrows Indicate Probable Path of Molten Fuel to Reactor Tank Bottom.

78904044.2M

Figure B.9-7. Diagram Illustrating Fuel Flow Through an Ablating Hole in a Pressure Plate.

The mean superheat ΔT of the fuel-melt pool above the pressure plate can be estimated in the following manner. The energy increment dE , contributed to the pool by an incremental mass $A\rho dx$ that falls a distance x under gravity through the active core region, is

$$dE = c(T(x) - T_{mp}) A\rho dx \quad (9-13)$$

where

A = the cross-sectional area of the intact fuel rings

$T(x)$ = the temperature of the fuel increment, originally located a distance x above the bottom of the active fuel region, upon entering the plenum.

Assuming that the fuel increment falls freely through the active region, its temperature rise from full-power volumetric heating Q_v is

$$T(x) - T_{mp} = \frac{\dot{Q}_v}{\rho c} \left(\frac{2x}{g} \right)^{1/2} \quad (9-14)$$

$$E = A\dot{Q}_v \int_0^L \left(\frac{2x}{g}\right)^{1/2} dx = \frac{2}{3} A\dot{Q}_v \left(\frac{2L^3}{g}\right)^{1/2} \quad (9-15)$$

where

L = the total length of the active fuel rings.
The energy E is related to the average fuel superheat by

$$E = \rho c L \cdot \Delta T. \quad (9-16)$$

Equating 9-15 and 9-16 and solving the result for ΔT gives

$$\Delta T = \frac{2\dot{Q}_v}{3\rho c} \left(\frac{2L}{g}\right)^{1/2}. \quad (9-17)$$

At full power $\dot{Q}_v = 1.5 \times 10^9 \text{ J}\cdot\text{m}^{-3}\cdot\text{s}^{-1}$. The total length of the fuel rings is $L = 4.0 \text{ m}$. Thus from Equation 9-17 we can estimate an effective fuel superheat of

$$\Delta T = 333\text{K}. \quad (9-18)$$

The velocity of the fuel u through the openings in the pressure plate can be estimated from the Bernoulli equation:

$$u = (2gH)^{1/2}. \quad (9-19)$$

Taking H to be the vertical distance of 0.15 m between the bottom of the fuel rings and the pressure plate, Equation (9-19) gives

$$u = 1.71 \text{ m}\cdot\text{s}^{-1}. \quad (9-20)$$

Substituting Equations 9-18 and 9-20 into Equation 9-12 together with the physical property estimates $Pr = 0.02$, $k = 100 \text{ J}\cdot\text{m}^{-1}\cdot\text{s}^{-1}\cdot\text{K}^{-1}$, $\nu = 8 \times 10^{-7} \text{ m}^2\cdot\text{s}^{-1}$, and the plate-thickness dimension $\delta = 3 \times 10^{-3}$, yields

$$\dot{q} = 8.0 \times 10^7 \text{ J}\cdot\text{m}^{-2}\cdot\text{s}^{-1} \quad (9-21)$$

for the heat flux that impinges on the edges of the holes that penetrate the pressure plate. The value of the heat transfer coefficient, h , readily follows from Equations 9-18 and 9-21:

$$h = \frac{\dot{q}}{\Delta T} = 2.4 \times 10^5 \text{ J}\cdot\text{m}^{-2}\cdot\text{s}^{-1}\cdot\text{K}^{-1}. \quad (9-22)$$

Since the initial temperature of the aluminum pressure plate, T_0 , is 100°C , the effect of the fuel melt flowing through the holes does not immediately result in melting of the aluminum. The plate-edge temperature must first rise to the aluminum melting temperature, $T_{mp} = 660^\circ\text{C}$, before the melting process begins.

The solution for the plate surface temperature, T_w , before melting starts (Carslaw and Jaeger 1959) is

$$\frac{T_w - T_\infty}{T_o - T_\infty} = \exp \left[\frac{h^2 \alpha_s t}{k_s^2} \right] \operatorname{erfc} \left[\frac{h \sqrt{\alpha_s t}}{k_s} \right] \quad (9-23)$$

where

α_s = the thermal diffusivity

k_s = thermal conductivity of the aluminum plate

T_∞ = the temperature of the flowing fuel ($T_\infty = \Delta T + T_{mp}$)

t = time.

The time to plate melting is found by setting $T_w = T_{mp}$ in Equation 9-23 and solving the result for t . Using Equations 9-22 and 9-23 and the appropriate property values, we estimate that it takes only 0.007 s for the surface of the plate to rise to its melting temperature.

Once melting begins, the temperature of the ablating surface (edge of hole) remains constant in time and, therefore, the impingement heat flux at the edge is also time invariant. The temperature profile within the plate, in the radial direction beneath the edge of the hole, will asymptotically approach a simple, steady exponential form (Carslaw and Jaeger 1959). The relaxation time to steady state in the melting plate is readily seen to be comparable to the time it takes the thermal wave thickness $(\alpha_s t)^{1/2}$ to span one steady-state boundary layer thickness, $\alpha_s / \dot{r}$, where $\dot{r}$ is the steady-state rate of increase of the hole radius because of melting. Thus the transient melting process will die out in about the time

$$t = \frac{\alpha_s}{\dot{r}^2} \quad (9-24)$$

From the results of the calculations presented below, $\dot{r} \approx 3 \times 10^{-2} \text{ m} \cdot \text{s}^{-1}$ and, since $\alpha_s = 4 \times 10^{-5} \text{ m}^2 \cdot \text{s}^{-1}$, the relaxation time for attainment of steady state is less than 0.045 s, which is small on the time scale of plate meltout (> 0.1 s, see below). Clearly, the initial transient conduction and melting stages can be ignored and the melting process can be assumed to occur under steady-state conditions.

A steady-state energy balance at the melting edge of a plate hole yields the following relationship between the hole growth rate $\dot{r}$ because of melting and the heat flux $\dot{q}$:

$$\dot{r} = \frac{\dot{q}}{\rho [h_{fs} + c_s (T_{mp} - T_o)]} \quad (9-25)$$

where

c_s = the heat capacity of the aluminum plate.

From Equation 9-21 and the relevant property values, we estimate from Equation 9-25 a hole growth rate of

$$\dot{r} = 3 \times 10^{-2} \text{ m}\cdot\text{s}^{-1}. \quad (9-26)$$

From geometrical considerations, the half-distance between hole centers $r_{1/2}$ is calculated to be $8.15 \times 10^{-3} \text{ m}$. The time it takes for each hole to grow from the initial hole size (radius) $r_o = 4.67 \times 10^{-3} \text{ m}$ to $r_{1/2} = 8.15 \times 10^{-3} \text{ m}$ should correspond approximately to the time it takes to melt away the entire pressure plate. This time is, from Equation 9-26,

$$t = \frac{r_{1/2} - r_o}{\dot{r}} = 0.12 \text{ s}. \quad (9-27)$$

Thus the pressure plate is rapidly ablated away and should present little additional resistance to the downward relocation of the fuel melt. Likewise, the superheated fuel melt should readily flow from the main cavity, through the shell, to the bottom of the reactor tank (see Figure B.9-5). Without presenting the calculations, it can be shown that the holes that penetrate the shell will grow rapidly by ablation and merge into a single opening through which the fuel should readily pass.

B.9.3.4 Fuel Behavior Outside the Incident Process Assembly

Below the active fuel region inside as well as immediately outside the incident process assembly, inefficient fuel/coolant interactions would take place (Fauske and Henry 1982) leading to transfer of energy to the water and partial breakup of the molten fuel. Because of the moderator flow pattern, the potential exists for the particulate fuel/target material to be carried up into the active moderator space. Assuming optimum fuel particulate (in the absence of target material) moderator configurations, positive reactivity additions on the order of $\% \Delta K \approx 0.5$ have been calculated. The time scale for such reactivity addition would be well in excess of the nominal reactor scram time, and since the worst possible reactivity addition is well below the reactor shutdown worth, a whole-core event would indeed appear to be an incredible event. Note that only a small fraction of the incident assembly fuel (which would include target material)

would reach the active moderator space, with the majority of the fuel remaining in a frozen and coolable geometry either within the lower portion of the assembly or on the reactor tank floor.

B.9.4 BIOGRAPHICAL INFORMATION

M. EPSTEIN

Michael Epstein is Vice President of Consulting Services at Fauske & Associates, Inc., Burr Ridge, Illinois. He previously had a nine-year association with the Argonne National Laboratory where he was manager of the Post-Accident Heat Removal Section in the Reactor Analysis and Safety Division. He served as a consultant to various industries and on several government committees and review panels. His research centers on thermal-hydraulics and transport phenomena in turbulent and multiphase systems, with particular emphasis on nuclear and chemical reactor safety applications. He is the author of more than 60 publications on fluid mechanics and thermal science, and was a technical editor of the *ASME Journal of Heat Transfer* from 1979 to 1985. He holds a PhD in mechanical engineering from the Polytechnical Institute, Brooklyn, New York.

G. H. CLARE

George Clare is Vice President, Operations, at Fauske & Associates, Inc. He has 14 years of experience in the design, analysis, and licensing of nuclear facilities, including nuclear reactor plants and high-level and low-level radioactive waste management facilities. When employed by Westinghouse, he supervised the licensing activities of the lead reactor manufacturer and subcontractor organizations for the CRBRP. He worked extensively with engineers, analysts, and NRC staff to interpret NRC regulations and guidelines (written for LWRs) for application to an LMR. He has supervised a wide range of design and analysis activities for waste-management facilities, including spent-fuel management facilities and a deep geologic repository. He has up-to-date knowledge and involvement in DOE Office of Civilian Radioactive Waste Management licensing activities through consulting activities in support of DOE's Chicago Operations Office. He holds a BS in engineering physics and an MS in nuclear engineering, both from Cornell University.

R. E. HENRY

Vice President and cofounder of Fauske and Associates, Inc., Dr. Henry was involved in the Zion and Indian Point probabilistic safety studies as well as the Limerick PRA. More recently, he made numerous contributions to the industry degraded-core rulemaking program in which his company had the responsibility for developing computer codes for analyzing the response of PWRs and BWRs during severe accidents. The modular accident analysis

program has gained widespread acceptance in the domestic and foreign nuclear industry. The program specifically treats such phenomena as concrete attack, hydrogen formation, distribution and combustion within the containment, debris distribution, debris-bed coolability, and fission-product behavior. Dr. Henry was also the manager for the issue resolution and individual plant evaluation tasks in the IDCOR Phase II Program, which culminated with the individual plant evaluation methodology. During the IDCOR program, he was one of the industry representatives in the U.S. delegation to the International Atomic Energy Agency in Vienna to hear the Soviet description and interpretation of the Chernobyl Unit 4 accident. Following the Chernobyl accident, he served on review panels for both the N Reactor and the Savannah River reactors with respect to potential severe-accident conditions. He holds a PhD in mechanical engineering from the University of Notre Dame.

This page intentionally left blank.

**DO NOT MICROFILM
THIS PAGE**

APPENDIX C: References

APPENDIX C. REFERENCES

- ASME, 1973, *Stress Criteria Section III Classes 2 and 3, Piping Subject to Upset, Emergency and Faulted Operating Conditions*, Code Case 1606, American Society of Mechanical Engineers, New York, New York.
- ASME, 1986a, "Pressure Vessels," Section VIII, *ASME Boiler and Pressure Vessel Code*, American Society of Mechanical Engineers, New York, New York.
- ASME, 1986b, "Rules for Construction of Nuclear Power Plant Components, Division 1, Subsection NC, Class 2, Components," Section III, *ASME Boiler and Pressure Vessel Code*, American Society of Mechanical Engineers, New York, New York.
- ASME, 1986c, "Rules for Inservice Inspection of Nuclear Power Plant Components," Section XI, *ASME Boiler and Pressure Vessel Code*, American Society of Mechanical Engineers, New York, New York.
- ANS, 1987, *Standard for Selection, Qualification and Training of Personnel for Nuclear Power Plants*, ANS 3.1, American Nuclear Society, LaGrange Park, Illinois.
- ANSI, 1973, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," ANSI N18.2-1973, *Annual Book of Standards*, American National Standards Institute, New York, New York.
- ANSI, 1986, "Power Piping," ANSI/ASME B31.1, *Annual Book of Standards*, American National Standards Institute, New York, New York.
- ANSI, 1987, "Chemical Plant and Petroleum Refinery Piping," ANSI/ASME B31.3, *Annual Book of Standards*, American National Standards Institute, New York, New York.
- ANSI/ASME, 1986, *Quality Assurance Program Requirements for Nuclear Facilities*, ANSI/ASME NQA-1-86, American National Standards Institute/American Society of Mechanical Engineers, New York, New York.
- ASTM, 1982, *Standard Specification for Pressure Vessel Plates, Carbon Steel Low-and Intermediate Tensile Strength*, ASTM A285-82, American Society for Testing and Materials, Philadelphia, Pennsylvania.
- ASTM, 1987, *Standard Specification for Pipe, Steel, Black and Hot-Dipped, Zinc-Coated Welded and Seamless*, ASTM A53-87b, American Society for Testing and Materials, Philadelphia, Pennsylvania.

- Carlson, D. D., D. R. Gallup, A. M. Kolaczowski, G. J. Kolb, and D. W. Stack, 1983, *Interim Reliability Evaluation Program Procedures Guide*, NUREG/CR-2728, U.S. Nuclear Regulatory Commission, Washington, D.C.
- Carslaw, H. S. and J. C. Jaeger, 1959, *Conduction of Heat in Solids*, 2nd ed., Oxford University Press, Oxford, England.
- Chang, T. Y. and N. R. Anderson, 1987, *Regulatory Analysis for Resolution of Unresolved Safety Issue A-46, Seismic Qualification of Equipment in Operating Plants*, NUREG-1211, U.S. Nuclear Regulatory Commission, Washington, D.C.
- Crowley, D. A. and W. W. Yau, 1983, "Dynamic Responses of Fuel and Target Assemblies of a Production Reactor," *Transactions of the 7th International Conference on Structural Mechanics in Reactor Technology, Chicago, Illinois, August 22-26, 1983*, Vol. C, paper C6/8, pp. 257-263, North Holland Publishing Company, Amsterdam, The Netherlands.
- Di Nunno, J. J., F. D. Anderson, R. E. Baker, and R. L. Waterfield, 1962, *Calculation of Distance Factors for Power and Test Reactor Sites*, TID-14844, U.S. Atomic Energy Commission, Washington, D.C.
- DOE, 1986, *Safety of Department of Energy-Owned Nuclear Reactors*, DOE Order 5480.6, U.S. Department of Energy, Washington, D.C.
- DOE, 1988, *Savannah River Plant K Reactor Restart Strategy*, U.S. Department of Energy, Washington, D.C., November 25, 1988.
- DOE, 1989, *Nuclear Safety Policy* (draft February 10, 1989); *Attachment 3* (draft February 15, 1989), U.S. Department of Energy, Washington, D.C.
- EPA, 1975, *Protection Action Guides and Protection Actions for Nuclear Incidents*, EPA 5201-75/001, U.S. Environmental Protection Agency, Washington, D.C.
- EPRI, 1988, *Guidelines for Utilization of Commercial Grade Items in Nuclear Safety Related Applications, (NCIG-07)*, EPRI NP-5652, Electric Power Research Institute, Palo Alto, California.
- Fauske, H. K. and R. E. Henry, 1982, "Mechanisms of Liquid-Liquid Vapor Explosions," presented at AIChE Spring National Meeting, Anaheim, California.
- ICBO, 1950, *Uniform Building Code*, International Conference of Building Officials, Whittier, California.
- IEEE, 1987, *Practice for Maintenance, Testing and Replacement of Large Lead Storage Batteries for Generating Stations and Substations*, IEEE 450, Institute of Electrical and Electronics Engineers, New York, New York.

- NAS, 1987, *Safety Issues at the Defense Production Reactors: a Report to the Department of Energy*, National Research Council, Committee to Assess Safety and Technical Issues at DOE Reactors, National Academy of Sciences, National Academy Press, Washington, D.C.
- NRC, 1973a, *Damping Values for Seismic Design of Nuclear Power Plants*, Regulatory Guide 1.61, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1973b, *Design Response Spectra for Seismic Design of Nuclear Power Plants*, Regulatory Guide 1.60, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1973c, *Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems*, Regulatory Guide 1.47, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1976, *Combining Modal Responses and Spatial Components in Seismic Response Analysis*, Regulatory Guide 1.92, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1983, *Safety-Evaluation Report Related to the Construction of the Clinch River Breeder Reactor Plant*, NUREG--0968, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1987, *Qualification and Training of Personnel for Nuclear Power Plants*, Regulatory Guide 1.8, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1988a, *Domestic Licensing of Production and Utilization Facilities*, Title 10, Code of Federal Regulations, Part 50, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1988b, *General Design Criteria for Nuclear Power Plants*, Title 10, Code of Federal Regulations, Part 50, Appendix A, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1988c, *Operator's Licenses*, Title 10, Code of Federal Regulations, Part 55, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1988d, *Reactor Site Criteria*, Title 10, Code of Federal Regulations, Part 100, U.S. Nuclear Regulatory Commission, Washington, D.C.
- Pasquill, F. and F. D. Smith, 1983, *Atmospheric Diffusion*, Halstead Press, New York, New York.
- WHC, 1987, *Safety Assessment of N Reactor*, WHC-EP-0035, Westinghouse Hanford Company, Richland, Washington.

**DO NOT MICROFILM
COVER**

Prepared for the U.S. Department of Energy
under Contract No. DE-AC09-88SR18035

Westinghouse