DP-MS-72-57

CONF-730217--3

DEFENSE-IN-DEPTH IN REACTOR SAFETY

by

Samuel Mirshak

E. I. du Pont de Nemours and Co.
Savannah River Laboratory
Aiken, South Carolina 29801
United States of America

Proposed for presentation at the IAEA Symposium on Principles and Standards of Reactor Safety at Jülich, Federal Republic of Germany on February 5-9, 1973.

DEFENSE-IN-DEPTH IN REACTOR SAFETY

by

Samuel Mirshak

E. I. du Pont de Nemours and Co.
Savannah River Laboratory
Aiken, South Carolina 29801
United States of America

To be presented at the IAEA Symposium on Principles and Standards of Reactor Safety at Jülich, Federal Republic of Germany, on February 5-9, 1973.

DEFENSE-IN-DEPTH IN REACTOR SAFETY

S. Mirshak

Savannah River Laboratory
E. I. du Pont de Nemours and Co.
Aiken, South Carolina 29801

ABSTRACT- The system to ensure continuing safety in the large reactors at the Savannah River Plant is based on defense-in-depth in all phases of operation: the organization of skilled technicians, theorists, and operating personnel; effective administrative controls and procedures; safety limits; and engineered safety features. The lines of defense are delineated and maintained by procedural control. Reactor safety is still a top priority consideration at Savannah River after almost 20 years of reactor operation.

A vital part of reactor safety at Savannah River is continuing experimental and theoretical analyses to understand more fully the mechanism of response of the reactor processes to postulated abnormal conditions. Detailed analyses of postulated accidents and reactor response are defined for cases up to and including the highly unlikely melting of a full core. This fuller understanding has resulted in improved procedures, new operating limits for protection against postulated reactor transients, new safety equipment including on-line computers, and improvement of protective systems. These improvements provide an additional margin of safety, both by reducing the probability of postulated accidents and by mitigating the consequences should accidents occur.

INTRODUCTION

The Du Pont Company operates the Savannah River Plant and Laboratory for the United States Atomic Energy Commission. The Atomic Energy Division was formed within one of the twelve operating departments of Du Pont as the functional organization to administer and operate these facilities.

The Atomic Energy Division is composed of two major subdivisions: the Manufacturing Division, which is responsible for the operation of the Savannah River Plant, and the Technical Division, which is primarily responsible for the Savannah River Laboratory.

The production reactors at the Savannah River Plant have been in operation for about twenty years and reactor safety is still a top-priority consideration.[1] Defense-in-depth is utilized at Savannah River to ensure continuing safety in the operation of these reactors. This defense-in-depth concept covers all phases of

reactor operation, including the organization, administrative controls, safety limits, and engineered safety features. In this paper, the principal methods used to provide defense-in-depth are described for each of these areas.

Some improvements also are described that are an outgrowth of the continuing safety program. These improvements increase the margins of safety by reducing the probability of postulated accidents, and by mitigating the consequences should accidents occur.

The Savannah River reactor buildings, Figure 1, are large concrete structures. Although each building is slightly different, all contain the following major process areas: a Reactor Area, an Assembly Area, a Disassembly Area, and a Purification Area. Conventional containment is not provided. Instead, an on-line activity confinement system is provided that includes mist eliminators, particulate filters, and charcoal filters for the once-through ventilation systems to limit activity releases under accident conditions.

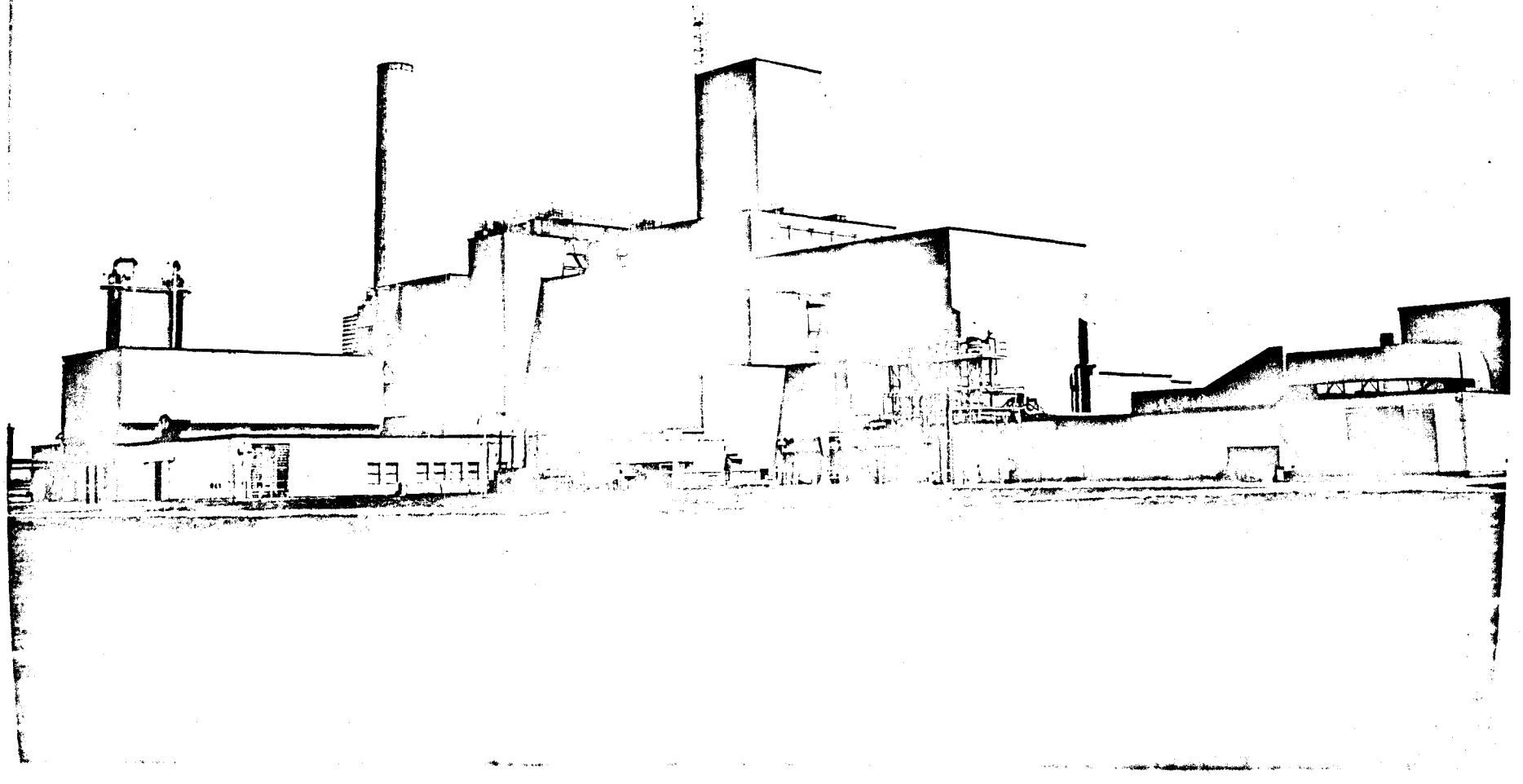
The reactors are heavy-water moderated and cooled. Heat generated by fission is removed from the core assemblies by circulating heavy water in the closed loop -- past the fuel elements, out to and through external heat exchangers, and back to the reactor. Heat exchangers are cooled by light water.

A schematic diagram of the reactor cooling system is shown in Figure 2. The reactor concept is essentially a pressure tube arrangement except that the heavy water coolant flows out of the pressure tubes, through the moderator space, and back to the six pumps in each of the six circulating loops.

SAVANNAH RIVER APPROACH TO DEFENSE-IN-DEPTH

The overall concept of defense-in-depth is usually depicted as a series of physical barriers that are effective at various stages in a series of events leading to undesired consequences as shown in Figure 3. This concept is utilized at Savannah River.

This paper, however, does not specifically treat the sequence of events and barriers peculiar to Savannah River operation but rather describes the defense-in-depth involved in each phase of the operation to make the barriers highly reliable and to maintain their effectiveness. These phases or areas are identified as the organization, administrative controls, safety limits, and engineered safety features.



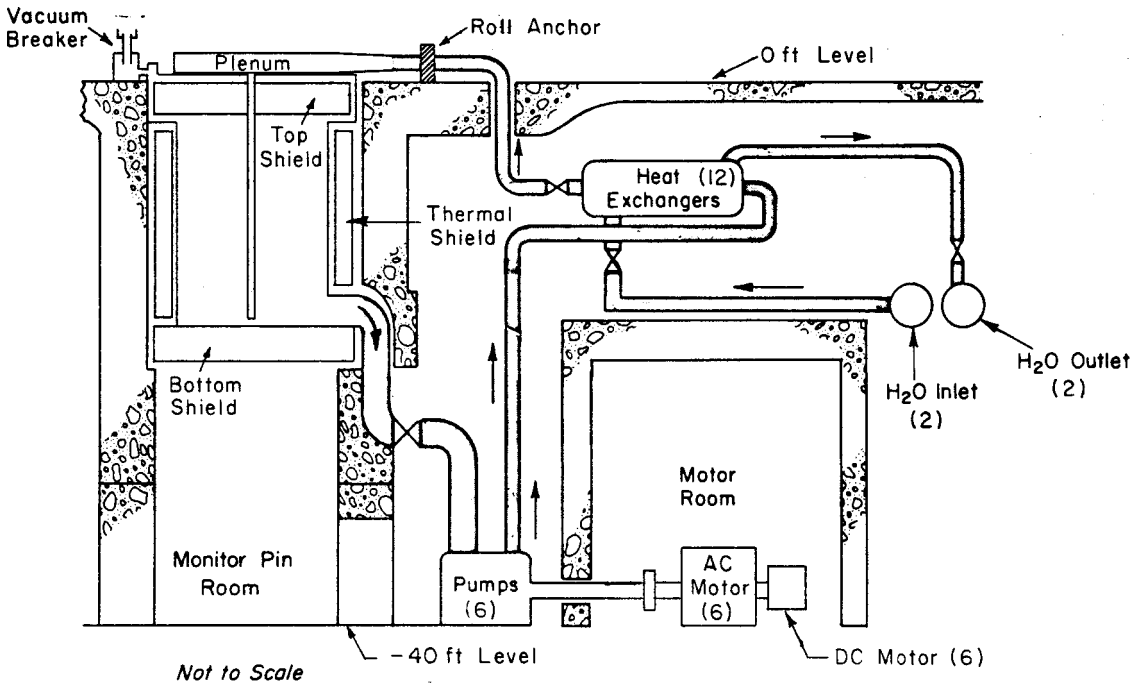


FIGURE 2. Schematic of Reactor Cooling System

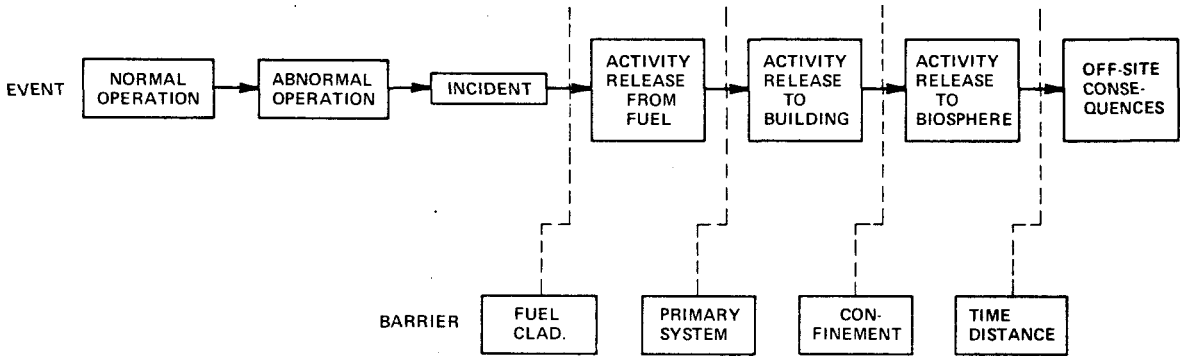


FIGURE 3 Defense-In-Depth Through Multiple Barriers

Figure 4 illustrates how this defense-in-depth is provided to ensure that a barrier performs its intended function when called upon.

The defense-in-depth in the organization, administrative controls, safety limits, and engineered safety features at Savannah River is described in the following sections.

ORGANIZATION

Manufacturing Division

Within the Manufacturing Division (SRP) there are two groups which have major responsibility for nuclear safety of the reactors - the Reactor Department and the Reactor Technology Section. The Reactor Department operates the reactors and associated equipment in accordance with the process supplied by the Reactor Technology Section and the Technical Division. The operations are carried out in accordance with written procedures prepared by the Reactor Department. Design, maintenance, and testing of critical components in the system are the responsibility of supporting departments in the Manufacturing Division. The Reactor Department, however, has the overall responsibility and is custodian of the reactors.

The Reactor Technology Section is responsible for the technical support of reactor operation, for technical aspects of reactor safety, and for technical improvements to the process.

Defense-in-depth in the organization is provided by the Reactor Technology Section to the Reactor Department by:

- Providing technical assistance
- Maintaining surveillance of process and equipment performance as related to reactor safety and continuity of operation
- Recognizing, defining, and solving problems
- Improving safety of reactor operation
- Improving understanding through process analyses
- Preparing Test Authorizations
- Initiating Reactor Startup Authorizations
- Conducting detailed charge design calculations

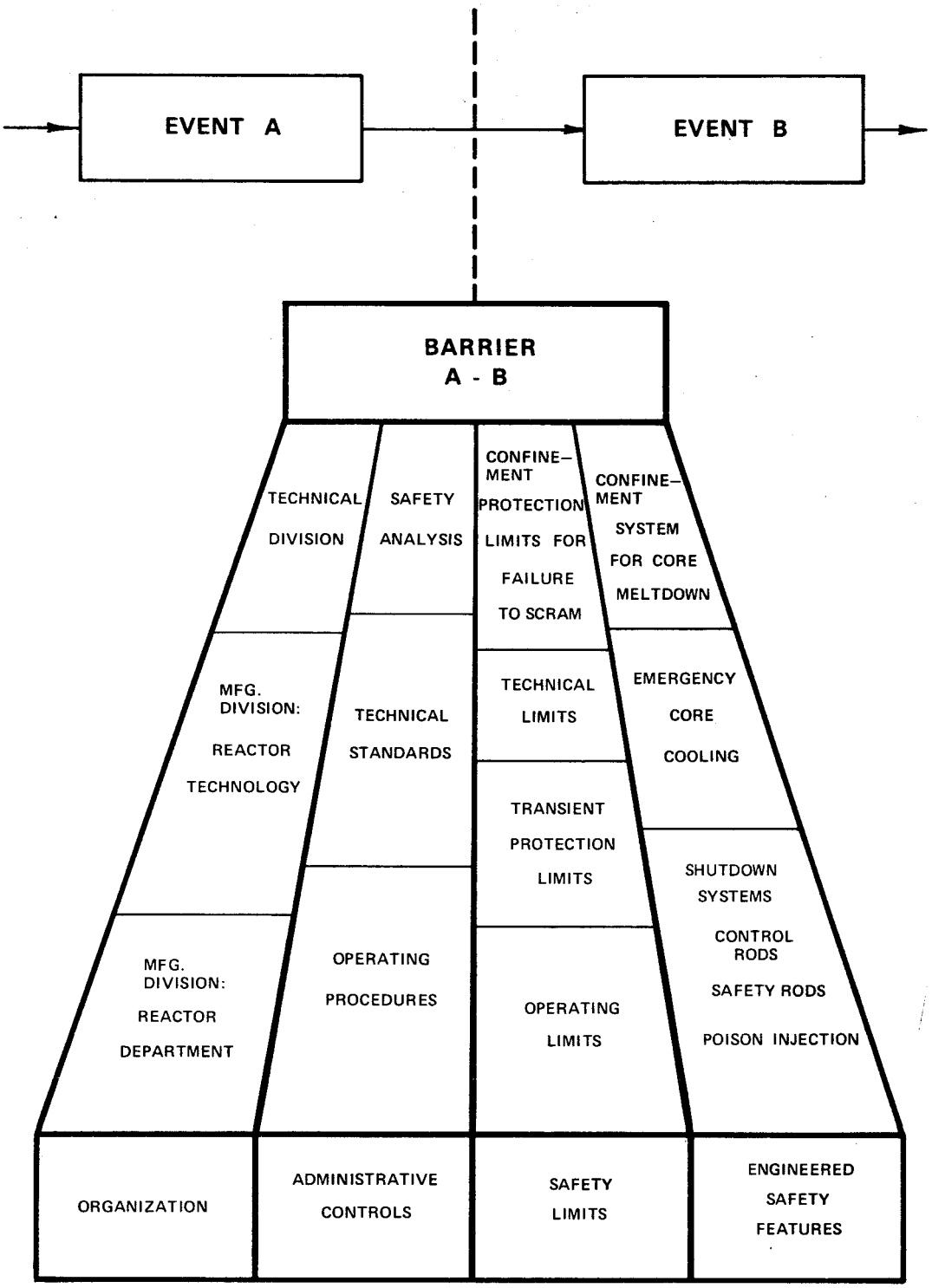


FIGURE 4 Defense-In-Depth in All Phases of Operation

Technical Division

The other arm of the Atomic Energy Division is the Technical Division. This Division, along with having responsibility for research and development and providing in-depth technical support to Reactor Technology, has responsibility for the following:

Providing and updating:

- o Technical Manuals which give the technical bases for plant processes
- o Technical Standards, which give the requirements and bases within which plant processes must be operated
- o Safety Analysis Reports and Compliance Letters, which provide an evaluation of the nuclear hazards associated with each operation

Reviewing and approving:

- o Test Authorizations for operation outside the limits imposed by Technical Standards
- o Reactor Startup Authorizations for Savannah River Plant reactors

Providing technical assistance to the Manufacturing Division when requested

In addition to these general responsibilities, the Reactor Safety group within the Reactor Engineering Division (Figure 5) has the responsibility for providing informal surveillance of reactor operations as related to items affecting reactor safety. This group serves to provide an overview to identify areas in which safety of reactor operations can be improved. Informal reviews of operating procedures and incident reports are provided and the Technical Division management is advised of areas of operations which have potential for affecting reactor safety. This group originates or reviews Safety Analysis Reports, Technical Standards, Technical Manuals, Test Authorizations, Reactor Startup Authorizations, Operating Procedures, and Incident Reports.

Technical Support

As just described, two lines of defense are provided to the Reactor Department in the organization to provide the understanding needed for the operation of the complex, potentially hazardous operation of the reactors. These are in addition to the technically trained engineers who are in the Reactor Department.

This depth in technology provides the understanding needed to design a safe process, to operate a safe process, and to provide engineered safety features. Without this understanding, it would not be possible to, first, identify the need for these items and, second, to provide the effective protective systems, whether administrative or engineered. The flow of information from the various groups in the Technical Division to the Manufacturing Division is shown in Figure 5. A research and development program together with the continuing technical support not only provides the basis for further improvements to reduce the probability and consequences, but it also provides the environment for sustaining the effectiveness of existing multiple defenses such as: skilled technicians and theorists, trained operating personnel, good instruments, and engineered safety features.

ADMINISTRATIVE CONTROL

Reactor operations at the Savannah River Plant (SRP) are administratively controlled by the imposition of written operating procedures which are strictly observed. Procedures are designed such that basic and important decisions are made by management after review throughout the organization. All decisions that could affect reactor safety or operability, even minor ones, are reviewed by the Reactor Technology Section and the Technical Division together with the Reactor Department, which is charged with direct responsibility for operation. Inherent in this concept of control is the principle that all process operations be performed according to detailed written procedures. These procedures are reviewed to preclude unsafe consequences, directly or indirectly, resulting from a possible chain of untoward events.

The relationships among the administrative controls are shown in detail in Figure 6, along with responsibility for the preparation of the documents. Primary limits are found in the Technical Standards, which are derived from, and find bases in, Technical Manuals and Safety Analysis Reports. On the bases of these Technical Standards and Mechanical Standards, operating procedures with appropriate margins are provided. The reactors are operated in strict accordance with these procedures.

These relationships among administrative controls provide for appropriate review at several levels of management of Du Pont's Manufacturing and Technical Divisions, as well as the AEC.

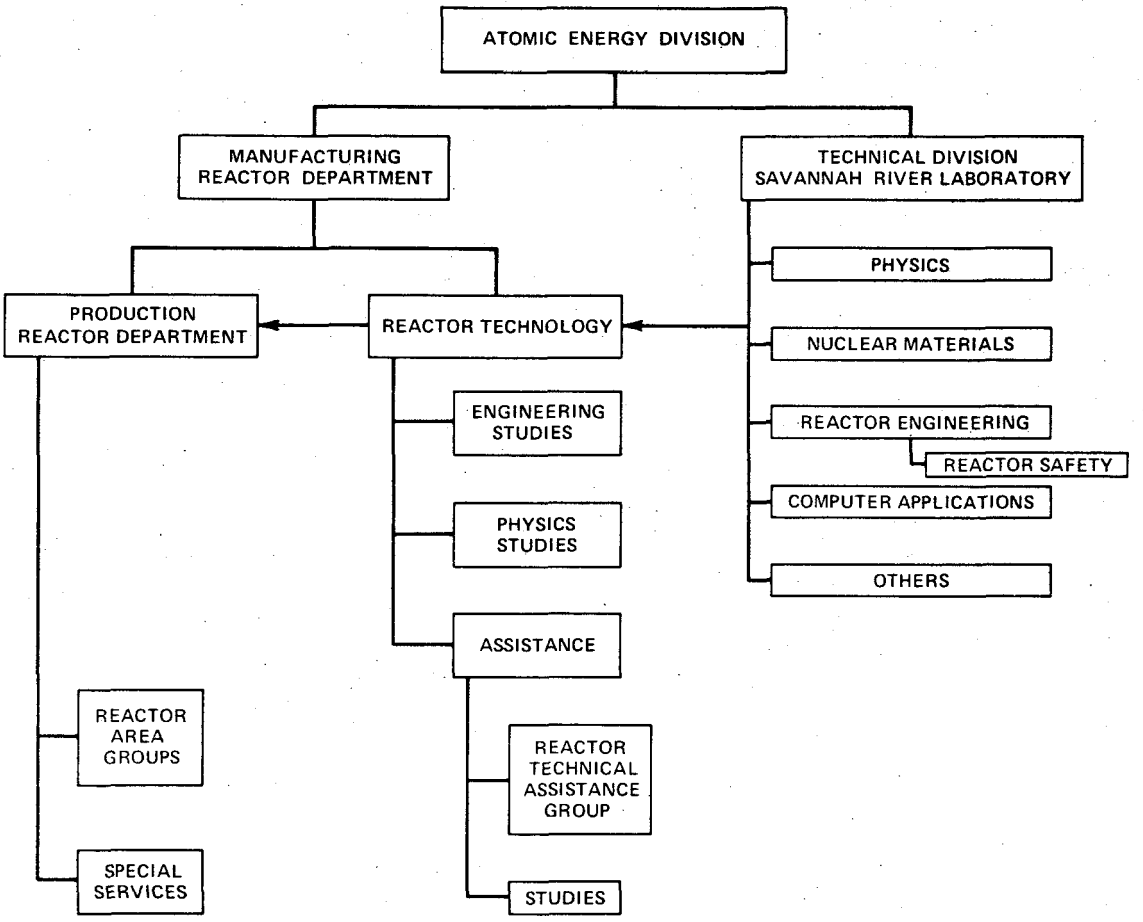
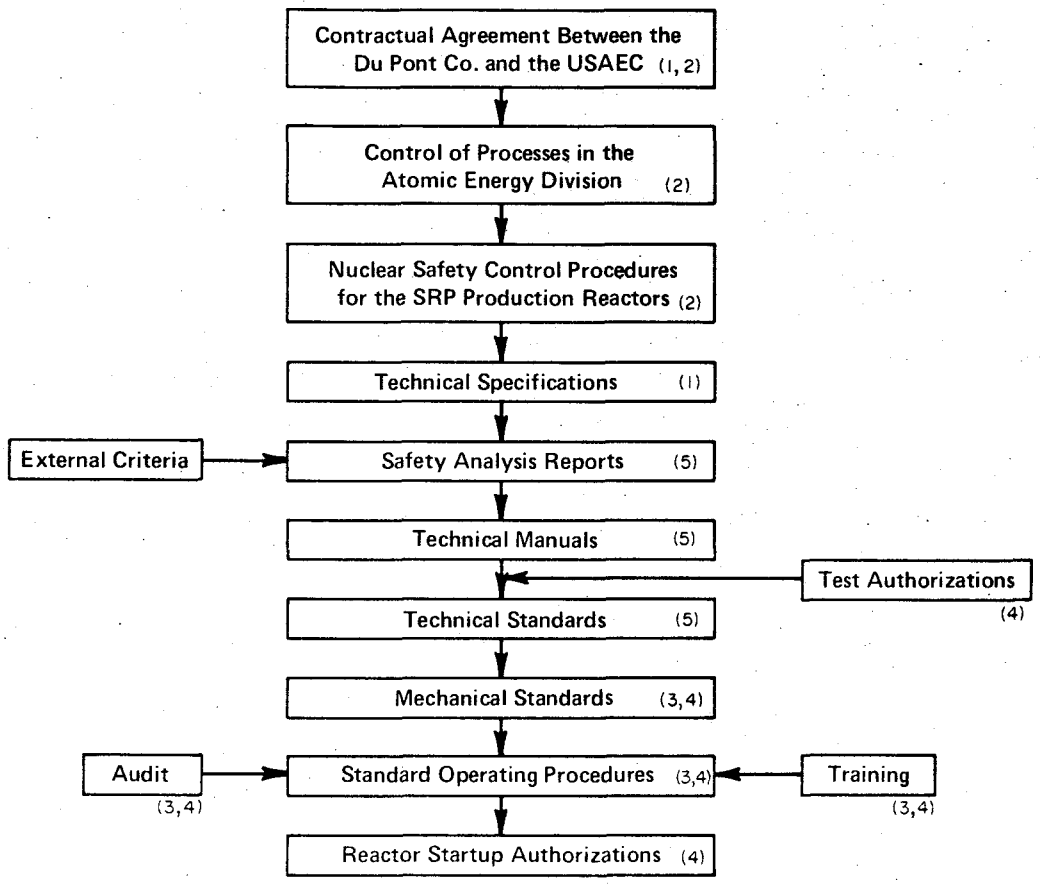


FIGURE 5 Flow of Technical Information



Prepared by:

(1) U. S. Atomic Energy Commission
(2) Du Pont Co.- Atomic Energy Division
(3) Reactor Department
(4) Reactor Technology Section
(5) Technical Division

FIGURE 6 Relationships Among Administrative Controls

As shown in Figure 6, part of the administrative control includes provision for audit of the operations. Auditing is carried out by the Reactor Department and the Reactor Technology Section. The Reactor Department audit includes observation of the operations to determine the degree of compliance with, and the adequacy of, the procedures. Written reports and recommendations are forwarded for action. As previously indicated, Reactor Technology audits operations carried out by the Reactor Department on a day-to-day basis, collects and analyzes operating data, and reviews operating logs. Special surveillance is provided for unusual operations where the chances of error or the consequence of error will be hazardous. Additional audit of the operations is conducted within the Technical Division through review of daily reports and Incident Reports to confirm that process variations and recommendations are within process bounds.

SAFETY LIMITS

Limits on critical operating variables are designed to protect against consequences for three operating situations: normal operations, incidents that are terminated by safety circuit response, and incidents in which safety rods fail to function.

For a particular critical variable the safety limits are established on the basis of analyses to determine the extreme value of the variable that will not yield actual damage -- or what range of values has a low probability of damage.

For a given operating mode, the condition of the reactor at any time is described by values of measured or calculated variables that characterize the performance of fuel assemblies and of the entire reactor. These variables include such quantities as temperatures, coolant flows, heat fluxes, radiation fields, and thermal and mechanical stresses on the reactor structure. Analyses of operating characteristics and experimental data establish the values of the critical operating variables at which actual damage or other undesirable consequences would occur in the reactor.

The principal safety limits are associated with the thermal hydraulic operations and are the Technical Limit, Transient-Protection Limit, Confinement Protection Limit, and the Operating Limit. The objectives of these limits are defined in the following sections.

Technical Limits

Technical Limits are specified to protect primary and secondary barriers, i.e., fuel and target, cladding, and the reactor structure during normal continuous operations so that the probability of harmful consequence is acceptably low. Technical Limits are established for effluent temperatures from each assembly and from the reactor to protect against:

- o bulk boiling of coolant
- o film boiling burnout
- o pump cavitation

Transient Protection Limits

Transient Protection Limits are specified to protect against significant damage to the reactor complex or against fission product releases as a result of certain designated incidents. The transient limits protect against the consequences of postulated power increases, flow changes, or pressure reductions that have a significant probability. The acceptable consequences for operation at the Transient Protection Limits are defined for specific incidents and on the basis that primary and/or backup scram circuits are operable. Generally, Transient Protection Limits are more restrictive than the Technical Limits.

Confinement Protection Limits

The intent of Confinement Protection Limits is to guard against the unlikely possibility that specified reactor transients not terminated by safety rod action may generate sufficient steam to impair the operability of the confinement system. For example, the confinement system pressure is controlled by regulating the incipient loss of coolant and/or the rate of removal of absorbing material which would add reactivity.

Operating Limits

Operating Limits are the highest level of continuous operation authorized by the Manufacturing Division. These limits provide margins from Transient Protection Limits to allow for normal process fluctuations and other operating unknowns. If the Confinement Protection Limit is less than an Operating Limit determined from a Transient Protection Limit, then the Confinement

Protection Limit is considered to be the Operating Limit. The relative relationship between these limits and indications of possible consequences associated with operation at each of these limits is indicated schematically in Figure 7.

ENGINEERED SAFETY SYSTEMS

Engineered safety systems are provided in the SRP reactor facilities to enhance the safety provided by the original design. These systems are analyzed, designed, and operated according to recognized safety guides on such subjects as a single active component failure, common mode failure, and separation of protection and control.

All engineered safety systems are designed and built to be readily tested and to provide high functional reliability. The three major systems (shutdown systems, emergency cooling system, and activity confinement system) are discussed below.

Shutdown Systems

Each Savannah River reactor is equipped with a set of safety rods which can shut down the reactor from full power (scram system). This set of rods is independent of the rod system used to control normal reactor power. Reactor power is significantly reduced within one second after actuation of this scram system. For each of the major incidents analyzed, at least two independent sensor systems must be capable of releasing the safety rods.

In addition, two other shutdown systems are available if the primary system should fail to function, or if unexpected reactivity transients should occur after the primary system has been utilized. One supplementary safety system is provided to inject soluble poison into the reactor. The other, the reactivity control system (control rods used for normal operation), is capable of reactor shutdown if the safety rods fail to function. Insertion of control rods and safety rods is started by the same signal. Control rod insertion is effective first and causes a small reduction in power before the safety rods enter the core. Neither supplementary system can terminate a transient as fast as the primary safety rod system.

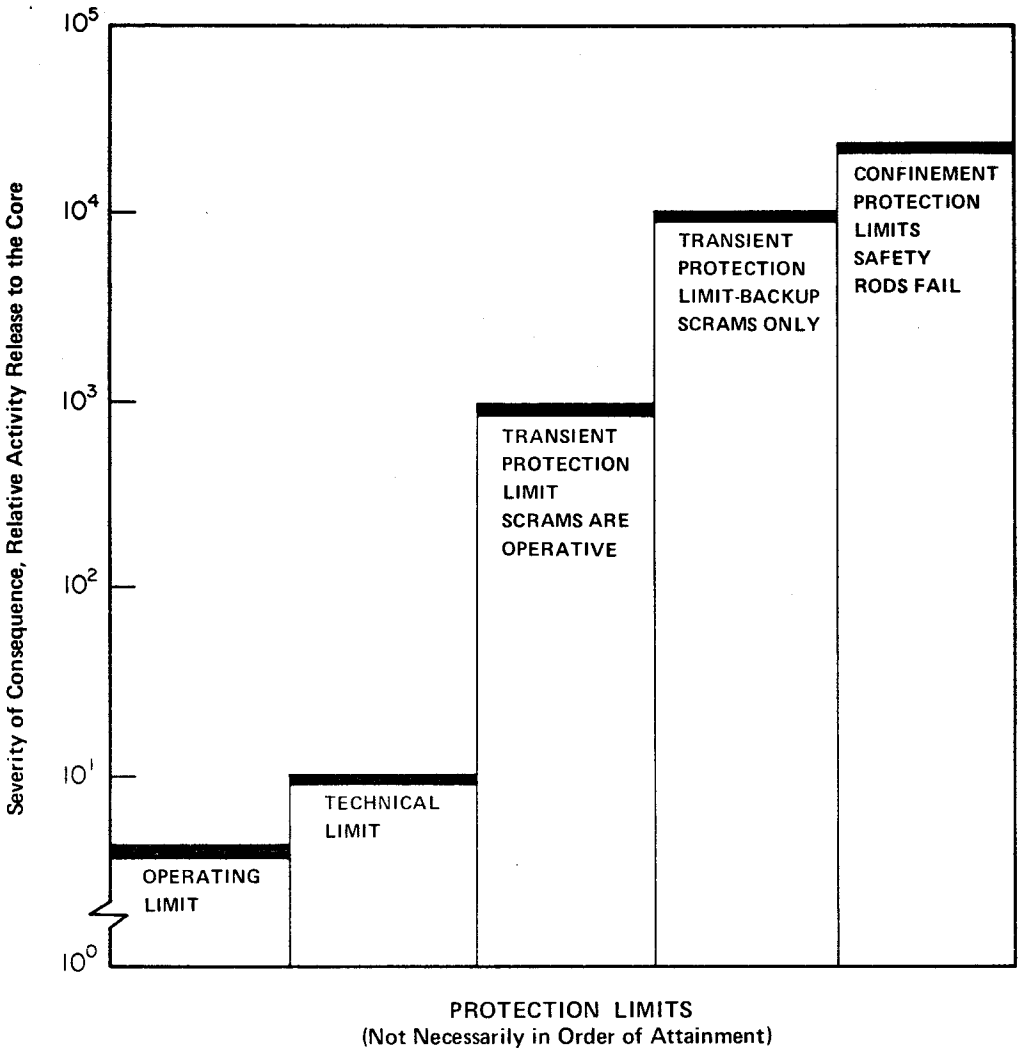


FIGURE 7 Relationship Between Protective Limits

Emergency Cooling System

The emergency cooling system is a combination of H_2O addition and partial recirculation with the primary D_2O pumps. If D_2O is lost because of a pipe rupture, the emergency cooling system provides for direct addition of H_2O to the reactor core. Four sources of H_2O supply are available to this system.

Activity Confinement System

An activity confinement system is provided to restrict the airborne release of radioactivity following any accident that breaches the other barriers to fission product release. The ventilation filter system is operated on-line continuously during reactor operation. This system is capable of removing a large fraction of particulate and halogen activity. Noble gas activity released from the core would not be confined. However, because of the large plant site (distance to nearest plant boundary is 8 km), offsite doses from such releases would not exceed federal guidelines under adverse meteorological conditions for all but the most unlikely and extreme assumptions of core melting.

CONTINUING SAFETY PROGRAM

Since startup, an aggressive and continuing safety effort has been maintained at Savannah River to keep the risks as low as practicable.

A continuing analysis to gain understanding of response to abnormal conditions has resulted in provisions for reducing the probability of occurrence and for mitigating the consequences, e.g.,

- improved procedures
- operating limits for protection against postulated transients
- new safety equipment, e.g., on-line computers
- new engineered safety features

MAJOR IMPROVEMENTS

To illustrate the benefits of such a continuing safety program, some of the major improvements incorporated since startup are discussed in summary form in the following sections.

Activity Confinement System

An activity confinement system consisting of mist eliminators and particulate and halogen filters in series was developed and installed in each of the reactor exhaust systems to prevent discharge of fission products, except for noble gases, in the event of accidental release. The objective here was to limit the consequence of accidents regardless of their probability.

Emergency Cooling Systems

The emergency cooling systems were further improved to include provision for diesel-driven pumps and remote control of critical equipment. The supply and distribution of coolant were further increased and improved. Extensive in-reactor tests were carried out to demonstrate the capability of the coolant pumps to circulate emergency coolant under starved-suction conditions.

Radial Power Monitor

Methods, instrumentation, and procedures for controlling neutron flux and power distribution in the reactors were developed. The features included alarms and scram sensors designed to provide automatic protection against flux distortions determined from measured temperatures throughout the reactor core. This system (called the radial power monitor) reduced the vulnerability to localized damage to clusters of fuel elements.

Meteorology Studies

Meteorology data were collected and techniques were developed for calculating potential dose to the public for hypothetical releases of radioactivity. This technology permitted a quantitative assessment of the dose risk to the public zone. It is now possible to appraise quantitatively the effect on potential dose of system modifications that influence the amount and nature of radioactive releases.

Burnout Protection Limits

A system based on frequency of occurrence of nonidealities on heat transfer surfaces was developed for establishing critical limits for primary reactor variables that govern proximity to film boiling burnout conditions in fuel elements. This work provided a basis for setting safety limits and for specifying alarm and scram

settings to protect fuel elements from unacceptable damage both during normal operation and during selected reactor excursions that would be terminated by scrams.

Xenon Control

The problems of controlling space-time power distributions that arise in the reactors from the influence of xenon were investigated experimentally and theoretically. The objective of this work was to develop procedures for minimizing the power distortions caused by xenon effects and thereby to lower the frequency of signals to the instruments that protect against such distortions. Controlled tests with the SRP production reactors provided information also of interest to the AEC's regulatory staff and to the nuclear industry.

Full-Core Meltdown

The expected course of full-core meltdown was calculated including the effects that such an event would have on consequence-limiting engineered safety features.

Reactor Shutdown Systems

SRP reactor protection systems and engineered safety features were evaluated against guidance criteria recently developed for designing thermal power reactors. SRP reactors conformed in most areas of applicable criteria. However, as a result of the study, some further changes in the systems are being made, and others are being considered, primarily with the objective of reducing the vulnerability of some of the consequence-limiters to "single component failures."

On-Line Computer

An on-line computer was applied to reactor operation, first, for surveillance and information processing and, later, for automatic reactor control.[2] Safety was improved by more rapid and complete processing of sensor information, by back-up surveillance of critical parameters, by computer-controlled alarms and rod reversals, and, in automatic control, by freeing the operator to follow the status of the reactor more broadly. In general, the objective was to reduce the probability of events that could lead to undesired consequences.

Operator Guidance

Operator guidance by the on-line computer is provided through programs that display control parameters and assess power distributions in the reactor in the form needed by the operator to make control decisions. Reactor operating procedures utilize the computer data where possible. In some instances, the more comprehensive data analyses by the computer have resulted in improved operating techniques.

A printed record of operating data can be supplied by the computer on demand and this is done routinely. Such printouts are retained for a specified period of time and provide a valuable history of reactor operation.

Limits and Systems Monitoring

The computer is programed to monitor the proximity to Operating Limits and to print alarm messages to identify any exceeded limit. If assembly coolant temperature limits are exceeded by more than 1°C, even with the reactor under manual control, the computer initiates control rod insertion to lower power until the temperature is below the Operating Limit. The high-speed calculational capability is especially useful in monitoring operation at the burnout heat flux limit.

The computer also monitors safety circuits to detect instruments not indicating in the proper range or bypass switches improperly set when the reactor is under computer control. Circuits have been designed to isolate the computer from safety instruments to prevent interactions. To date there have been no known occurrences of computer interference with protective functions.

The computer also monitors other miscellaneous signals such as operating parameters for the primary D_2O pump motors.

Closed-Loop Control

A system for closed-loop computer control of the Savannah River reactors during power ascension and level power operation is in use to improve both safety and efficiency of operation. Equipment and programing features include:

- o Stepping motor drives for rod-positioning synchronous motors to achieve accurate and repeatable rod positioning.
- o Provisions to disable the computer control functions (at any time) and return control to the operator.
- o Improved operator-computer communications to indicate the control status at all times.
- o A control algorithm that minimizes cyclic actions, avoids end-point overshoot, and can function even with small external process upsets.
- o Control of both full rods and partial rods so that gross power optimization (flattened flux patterns) is an integral part of the operation.
- o A testing system to evaluate the actual programs, and digital drive equipment before on-line use at each reactor.
- o An instantaneous visual display of procedural steps associated with the control actions in progress.
- o Effective separation of control and safety circuit functions.

STUDIES IN PROGRESS

Reactor Transients Not Terminated by Scrams

Protection against the consequences of loss-of-absorber incidents is provided by limiting specified pre-incident parameters of reactor charges, called Confinement Protection Limits, such that maximum pressures in the confinement system are calculated to be less than predetermined values.

A computer code to analyze reactor transients is used to calculate pressures in the radioactivity confinement system during loss-of-absorber incidents. The computer code calculates the sequence of the accident starting from normal steady-state operation, and includes the amount of core damage, the reactivity change in the core, and the rate of steam formation. In the unlikely event of an incident involving loss of absorber with inoperable safety rods, the incident can be terminated by the addition of sufficient negative reactivity to the reactor core from core disruption, negative temperature coefficients, or supplemental shutdown systems.

Although the computer code is in use it is recognized that part of the models included are rudimentary. Work continues to improve the models and the reliability of the calculations.

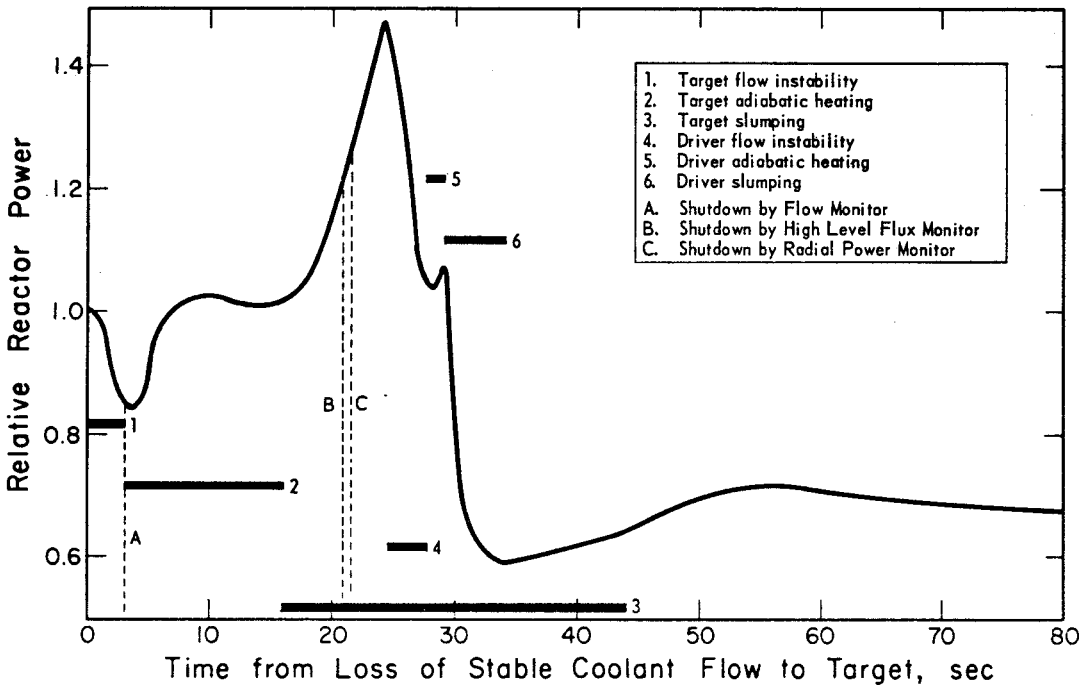


FIGURE 8 Calculated Consequences of Flow Instability in a One-Target Assembly in a Reactor Production Charge

An example of the consequence of a loss-of-absorber incident in a typical full-core production charge without safety rod action is illustrated in Figure 8. In this calculation the accident is terminated by loss of reactivity from melting of several driver assemblies. Calculated pressure surges would not damage the reactor confinement system.

Full-Core Meltdown Studies

Studies have been made to describe and understand the course of a full-core meltdown. Additional safety features are being evaluated to determine if additional protection is necessary to mitigate the consequences of this extremely unlikely accident. Studies show that if the exhaust air is cooled to offset the heating by molten debris from the reactor, the effectiveness of the present confinement would be enhanced. The need to supply additional means to cool the air beyond that now available under these accident conditions is being evaluated.

CONCLUSIONS

Defense-in-depth safety in all phases of reactor operation is an effective method for reducing the probability and consequences of incidents. The defense-in-depth concept covers all phases of reactor operation, including the organization, administrative controls, safety limits, and engineered safety features.

Continuous technical support to understand more fully the mechanisms of response of the reactor processes to abnormal conditions is a vital part of this defense. This technical support continues to identify areas for further improvements in procedures, safety limit analyses, new safety equipment, and protective systems so that the risk of reactor operation is maintained as low as practicable.

REFERENCES

1. A. A. Johnson. "Post-Startup Reactor Safety." *Reactor Safety and Hazards Evaluation Techniques, Vol. 1-62.* International Atomic Energy Agency, Vienna, 145-65 (1962).

2. K. L. Gimmy. "Closed-Loop Computer Control of Savannah River Reactors." *Trans. Amer. Nucl. Soc. 14 (Supplement 2),* 31-2 (1971).

ACKNOWLEDGMENT

Although a single author is indicated for this paper, the safety philosophy and the improvements described are the results of the efforts of many people, too numerous to mention. All branches of the organization are involved starting with the management and including many people in the Reactor Department and the Reactor Technology Section of the Manufacturing Division and many others in the Technical Division.