

APPENDIX G - PLANT NUCLEAR SAFETY OPERATIONAL ANALYSIS

The material presented in Appendix G is historical and describes information relevant to the original Technical Specifications. Information may be used for understanding accidents, transients, and special events. For accurate information regarding the details of committed equipment for mitigation of these accidents, The Improved Technical Specifications (ITS), Chapter 14 of the UFSAR, or reload licensing documents may be used. |

G.1 ANALYTICAL OBJECTIVE

The objective of the plant nuclear safety operational analysis is to systematically identify the systems essential to nuclear safety and the functional requirements which must be met on such systems in order to assure nuclear safety.

Key terms used in this appendix are defined in Section 1.0, "Introduction and Summary."

The material presented in Appendix G is historical and describes information relevant to the original Technical Specifications. Information may be used for understanding accidents, transients, and special events. For accurate information regarding the details of committed equipment for mitigation of these accidents, The Improved Technical Specifications (ITS), Chapter 14 of the UFSAR, or reload licensing documents may be used. |

G.2 INTRODUCTION

The operational analyses identify all essential protection sequences and identify the detailed hardware conditions essential to satisfying the nuclear safety operational criteria. The main objective of the analyses of Section 14.0, "Plant Safety Analysis," is to provide a detailed analysis of the "worst cases."

Thus, Section 14.0 is consequence oriented and Appendix G is protection sequence oriented. The sequences analyzed as "worst cases" in Section 14.0 correspond to one sequence for each event in Appendix G.

An objective of this analysis is to be comprehensive. This means that the analysis must be sufficiently broad in method that (1) all plant hardware is considered and (2) the full range of plant operating conditions is considered. It is recognized that there is a fallacy in preoccupation with "worst cases." Worst cases are those that give the most severe consequences, but the protection sequences essential to lesser cases may be different from those for the worst case sequence. To assure that operational requirements are found for all equipment essential to attaining acceptable consequences, all essential protection sequences must be identified. In this way a comprehensive level of safety is attained. Thus, the nuclear safety operational analysis is protection sequence oriented to achieve comprehensiveness.

An operational requirement is a requirement or restriction on either the value of a plant variable or the operability of a plant system. Such requirements must be observed during all modes of plant operation (not just at power) to assure that the plant is operated safely (to avoid the unacceptable safety results). There are two kinds of operational requirements for plant hardware:

1. Limiting condition for operation: the required condition for a system while the reactor is operating in a specified condition.
2. Surveillance requirements: the nature and frequency of tests required to assure that the system is capable of performing its essential functions.

Operational requirements are systematically selected for one of two basic reasons:

1. To assure that the unacceptable results are avoided following specified plant events.
2. To assure the existence of a single failure proof success path to acceptable consequences should a transient or accident occur.

The operational requirements that emerge from the nuclear safety operational analysis are frequently complex hardware requirements applicable only under certain carefully specified plant conditions. Although these complex operational requirements are the true safety requirements, they are too complicated for use as technical specifications. The complex operational requirements must be simplified to obtain a practical set of technical specifications.

G.2.1 Nuclear Safety Operational Criteria

The following nuclear safety operational criteria are used to select operational requirements and must be satisfied at all times.

Applicability

Nuclear Safety Operational Criteria

Planned operation, abnormal operational transients, accidents, and special events

The plant shall be operated so as to avoid unacceptable safety results.

Abnormal operational transients and accidents

The plant shall be operated in such a way that no single active component failure can prevent the safety actions essential to avoiding the unacceptable safety results associated with abnormal operational transients and accidents. This requirement is not applicable during system repair if the availability of the safety action is maintained either by restricting the allowable repair time or by more frequently testing a redundant system.

G.2.2 Unacceptable Safety Results

The following specified measures of safety are the unacceptable safety results used as the major bases for identifying system operational requirements. The unacceptable safety results are associated with different event categories. Those unacceptable safety results that are superior in importance to the others are marked with an asterisk.

Plant Event Category

Unacceptable Safety Result

1. Planned Operation

*1-1. Release of radioactive material to the environs that exceeds the limits of 10CFR20.

- 1-2. Fuel failure to such an extent that were the freed fission products released to the environs via the normal discharge paths for radioactive material, the limits of 10CFR20 would be exceeded.
 - 1-3. Nuclear system stress in excess of that allowed for planned operation by applicable ASME and ANSI codes.
 - 1-4. Existence of a plant condition not considered by plant safety analyses.
2. Abnormal Operational Transients
- *2-1. Release of radioactive material to the environs that exceeds the limits of 10CFR20.
 - 2-2. Any fuel failure calculated as a direct result of the transient analyses.
 - 2-3. Nuclear system stress exceeding that allowed for transients by applicable ASME and ANSI codes.
3. Accidents
- *3-1. Radioactive material release exceeding the guideline values of 10CFR100.
 - 3-2. Catastrophic failure of the fuel barrier as a result of exceeding mechanical or thermal limits.
- | <u>Plant Event Category</u> | <u>Unacceptable Safety Result</u> |
|-----------------------------|---|
| | 3-3. Nuclear system stresses exceeding those allowed for accidents by applicable ASME and ANSI codes. |
| | 3-4. Containment stresses exceeding those allowed for accidents by applicable ASME and ANSI codes when containment is required. |
| | 3-5. Overexposure to radiation of station personnel in the control room. |
| 4. Special Events | 4-1. Inability to shut down reactor by manipulating controls and equipment outside the control room. |

- 4-2. Inability to perform emergency procedures to bring the reactor to the cold shutdown condition from outside the control room.
- 4-3. Inability to shut down the reactor independent of control rods.
- 4-4. Inability to safely maintain plant in shutdown condition upon loss of the normal heat sink.

Most of the unacceptable safety results and nuclear safety operational criteria represent an extension of the general intent of plant hardware design criteria to plant operations. Thus, where design criteria require that hardware design offer a specified degree of protection for a radioactive material barrier under certain circumstances, so operational criteria require that actual plant operation offer the same degree of protection under the same circumstances.

Unacceptable safety result 1-4 differs in origin from the other criteria. This criterion requires, in effect, that the plant be operated only under conditions (pressure, power, water level, etc) for which safety analysis has been performed.

The material presented in Appendix G is historical and describes information relevant to the original Technical Specifications. Information may be used for understanding accidents, transients, and special events. For accurate information regarding the details of committed equipment for mitigation of these accidents, The Improved Technical Specifications (ITS), Chapter 14 of the UFSAR, or reload licensing documents may be used. |

G.3 METHOD OF ANALYSIS

The following inputs are required for the analysis of specific plant events:

1. Applicable nuclear safety operation criteria (paragraph G.2.1).
2. Applicable unacceptable safety results (paragraph G.2.2).
3. Definition of BWR operating states (paragraph G.3.1).
4. Event selection criteria (paragraph G.3.2).
5. Rules for event analysis (paragraph G.3.4).

With this information, each selected event can be evaluated to determine systematically the actions, systems, and limits essential to avoiding the unacceptable results. The plant components and limits so identified are then considered subject to operational nuclear safety requirements and technical specifications.

G.3.1 Boiling Water Reactor Operating States

Four BWR operating states in which the reactor can exist are defined in Table G.3.1. The main objective in selecting operating states is to divide the BWR operating spectrum into a few major conditions to facilitate consideration of various events in each state.

Each operating state includes a wide spectrum of values for important plant parameters. Within each state these parameters are considered over their entire range to determine the limits on their values necessary to satisfy the operational nuclear safety criteria. Such limitations are presented in the subsections of this Final Safety Analysis Report that describe the systems associated with the parameter limit.

G.3.2 Selection of Events for Analysis

G.3.2.1 Planned Operations

Planned operation refers to plant operation under planned conditions in the absence of significant abnormalities. Operations subsequent to an incident (transient, accident, or special event) are not considered planned operations until the actions taken or equipment used in the plant are identical to those that would have been used had the incident not occurred. As defined, the planned operations can be considered as a chronological sequence of events: refueling --> achieving criticality --> heatup --> power operation --> achieving shutdown --> cooldown --> refueling. These are further discussed in paragraph G.5.2.

Together, the BWR operating states and the planned operations define the full spectrum of conditions from which transients, accidents, and special events are initiated. The BWR operating states define only the physical condition (pressure, temperature, etc.) of the reactor; the planned operations define what the plant is doing. The separation of physical conditions from the operation being performed is deliberate and facilitates careful consideration of all possible initial conditions from which incidents may occur.

G.3.2.2 Abnormal Operational Transients and Accidents

The abnormal operational transients and accidents examined are those transients and accidents selected on the bases described in paragraphs 14.4.2 and 14.4.3 of Section 14.0, "Plant Safety Analysis."

The following transients analyzed in Section 14.0 were examined (Table G.3.2) and determined to require no unique safety responses, and thus are not further discussed in this appendix, but are entered in Table G.3.2 and Matrices A through D for completeness:

1. Inadvertent pump start (temperature decrease).
2. Shutdown cooling (RHRS) malfunction (temperature decrease).
3. Control rod removal error during refueling.
4. Fuel assembly insertion error during refueling.
5. Recirculation flow control failure - decreasing flow.

6. Trip of one recirculation pump.
7. Trip of two recirculation M-G set drive motors.
8. Recirculation pump seizure.

G.3.2.3 Special Events

Three special events are evaluated to demonstrate plant capabilities required by specially selected nuclear safety criteria. The capability to perform a safe shutdown from outside the control room is demonstrated by evaluating the event "shut down from outside the control room." The adequacy of the redundant reactivity control system is demonstrated by evaluating the event "shut down without control rods." The capability to perform a safe shutdown with an emergency heat sink in the event of a loss of Conowingo Pond is demonstrated by evaluating the event, "loss of normal heat sink."

G.3.3 Rules for Event Analysis

The following functional rules are followed in performing operational analyses for the various plant events:

1. An action, system, or limit shall be considered essential only if it is essential to satisfying the nuclear safety operational criteria (paragraph G.2.1).
2. The full range of initial conditions shall be considered for each event analyzed, so that all essential protection sequences are identified. Consideration is not limited to "worst cases," because lesser cases sometimes require actions or systems different from the "worst case."
3. The initial conditions for transients, accidents, and special events shall be limited to the conditions that would exist during the planned operations in the applicable operating state.
4. For planned operations, consideration shall be made only for actions, limits, and systems essential to avoiding the unacceptable results during operation in that state (as opposed to transients, accidents, and special events, which are followed through to completion). Planned operations are treated differently from other events because the transfer from one state to another during planned operations is deliberate.

For events other than planned operations the transfer from one state to another may be unavoidable.

5. Only for those essential parameters that are continuously monitored by the operator shall limits be derived for display on the operations matrices, Matrices A through D. Parameter limits associated with the required performance of an essential system are considered to be included in the requirement for the operability of the system. Limits on frequently monitored process parameters are called "envelope limits," and limits on parameters associated with the operability of a safety system are called "operability limits." "Envelope limits" define the envelope of planned operating conditions. Systems associated with the control of the envelope parameters are considered nonessential as long as it is possible to place the plant in a safe condition without using the system in question.
6. For transients, accidents, and special events, consideration shall be made for the entire duration of the event and aftermath until some planned operation is resumed. Planned operation is considered resumed when the procedures being followed are identical to those used during any one of the defined planned operations.
7. Credit for operator action shall be taken on a case basis, depending on the conditions that would exist at the time operator action is required. Because transients, accidents, and special events are considered through the entire duration of the event until planned operation is resumed, manual operation of certain systems is sometimes required following the more rapid portions of the event. Credit for operator action is taken only when the operator can reasonably be expected to accomplish the required action under the existing conditions.
8. For transients, accidents, and special events, only those actions, limits, and systems shall be considered essential for which there arises a unique requirement as a result of the event. For instance, if a system that was operating prior to the event (during planned operation) is to be employed in the same manner following the event and if the event did not affect the operation of the system, then no matrix entries for the system would be made.

9. The operational analyses shall identify all the support or auxiliary systems essential to the functioning, of the front-line safety systems.

Safety systems auxiliaries whose failure results in safe failure of the front-line safety systems shall be considered nonessential.

10. A system or action that actually functions in response to a transient, accident, or special event shall be considered essential unless the effects of the system or action are not included in the detailed analysis for the event.
11. For pipe breaks inside and outside the primary containment, a concurrent loss of off-site power was further assumed.

G.3.4 Steps in an Operational Analysis

The procedure followed in performing an operational analysis for a given event (selected according to the event selection criteria) is as follows:

1. Determine the BWR operating states in which the event is applicable (Table G.3.1). An incident is considered applicable within an operating state if the incident can occur from the initial conditions within the operating state.
2. Identify all the essential protection sequences (safety actions and front-line safety systems) for the event in each applicable operating state (Figures G.5.1 through G.5.22 and G.5.24 through G.5.26).
3. Identify all the safety system auxiliaries essential to the functioning of the front-line safety systems (Figures G.5.23a and G.5.23b).

TABLE G.3.1

BOILING WATER REACTOR OPERATING STATES

<u>Condition</u>	<u>States</u>			
	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>
Reactor vessel head off*	X	X		
Reactor vessel head on			X	X
Shutdown	X		X	
Not shutdown		X		X

Definition

Shutdown: K_{eff} sufficiently less than 1.0 that the full withdrawal of any one control rod could not produce criticality under the most restrictive potential conditions of temperature, pressure, core age, and fission product concentrations.

* Because the reactor vessel head is off in states A and B, pressure is atmospheric pressure.

TABLE G.3.2

EVENTS APPLICABLE IN EACH BOILING WATER REACTOR OPERATING STATE

<u>Types of Operation and Events</u>	<u>BWR Operating States</u>			
	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>
PLANNED OPERATION				
1. Refueling	X			
2. Achieving Criticality		X		X
3. Heatup				X
4. Power Operation				X
5. Achieving Shutdown		X		X
6. Cooldown	X		X	
ABNORMAL OPERATIONAL TRANSIENTS				
<u>Nuclear System Pressure Increase</u>				
8. (not used)				
9. Electrical load rejection (turbine trip with bypass)				X
10. Turbine trip without bypass				X
11. Isolation of all main steam lines			X	X
12. Isolation of one main steam line			X	X
<u>Moderator Temperature Decrease</u>				
13. (not used)				
14. Feedwater controller failure - maximum demand			X	X
15. Loss of feedwater heating				X

TABLE G.3.2 (Continued)

<u>Types of Operation and Events</u>	<u>BWR Operating States</u>			
	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>
Shutdown cooling (RHRS) malfunction (temperature decrease)	X	X	X	X
<u>Reactivity Insertion</u>				
16. Control rod withdrawal error	X	X	X	X
Control rod removal	X			
Fuel assembly insertion	X			
<u>Loss of Coolant Inventory</u>				
17. Pressure regulator failure			X	X
18. Inadvertent opening of a relief or safety valve	X	X	X	X
19. Loss of feedwater flow			X	X
20. Loss of auxiliary power	X	X	X	X
<u>Core Coolant Flow Decrease</u>				
Recirculation flow control failure-decreasing flow			X	X
Trip of one recirculation pump			X	X
Trip of two recirculation M-G set drive motors			X	X
Recirculation pump seizure			X	X
21. Loss of shutdown cooling	X	X	X	X
<u>Core Coolant Flow Increase</u>				
22. Recirculation flow control failure-(increasing flow)			X	X

TABLE G.3.2 (Continued)

<u>Types of Operation and Events</u>	<u>BWR Operating States</u>			
	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>
23. Startup of idle recirculation pump	X	X	X	X
ACCIDENTS				
24. Control rod drop accident			X	X
25. Pipe breaks inside primary containment			X	X
26. Fuel handling accident	X	X	X	X
27. Pipe breaks outside primary containment			X	X
28. (Not used)				
SPECIAL EVENTS				
29. Shutdown from outside control room	X	X	X	X
30. Shutdown without control rods		X		X
31. Loss of normal heat sink	X	X	X	X

The material presented in Appendix G is historical and describes information relevant to the original Technical Specifications. Information may be used for understanding accidents, transients, and special events. For accurate information regarding the details of committed equipment for mitigation of these accidents, The Improved Technical Specifications (ITS), Chapter 14 of the UFSAR, or reload licensing documents may be used. |

G.4 DISPLAY OF OPERATIONAL ANALYSIS RESULTS

To fully identify and establish the requirements, restrictions, and limitations that must be observed during plant operation, plant systems and components must be related to the needs for their actions in satisfying the nuclear safety operations criteria. This appendix displays these relationships in a series of block diagrams and matrices.

First, Table G.3.2 indicates in which operating states each event is applicable. Then, for each event, a block diagram is presented showing the conditions and systems essential to achieving each essential safety action. The block diagrams show only that equipment necessary to provide the safety actions in such a way that the nuclear safety operational criteria are satisfied. The total plant capability to provide a safety action is not shown, only the minimum capability essential to satisfying the operational criteria. The diagrams also show the essential protection sequences for each event. Once all of the protection sequences are identified in block diagram form, the equipment requirements are superimposed on the operational matrices (Matrices A through D). Thus, these matrices display the most restrictive requirements from all of the essential protection sequences for any one event. Each matrix of the series considers the following conceptual aspects:

1. The BWR operating state.
2. Types of operations or events that are possible within the operating state.
3. Relationships of certain safety actions to the unacceptable results and to specific types of operations and events.
4. Relationships of the actions of certain systems to safety actions and to specific types of operations and events.
5. Supporting or auxiliary systems essential to the operation of the frontline safety systems.
6. Considerations necessary to achieve a minimum level of functional redundancy (the single failure criterion applied functionally at the safety action level).

Because the scope of information presented on Matrices A through D encompasses so many safety aspects of the plant design and operation, the matrices are necessarily large and utilize many codes and symbols. It is difficult to rationally set operational

requirements on a given component without systematically considering each of the just-noted six aspects of the BWR on a plant-wide basis.

Matrices A through D and the block diagrams for the events combine to provide a vehicle for such a systematic analysis. Through the use of Matrices A through D and the block diagrams, any operational requirement can be traced to the unacceptable result, criterion, or safety action originating its need.

Each indication in Matrices A through D represents a finding of essentiality for the safety action, system, or limit under consideration. Essentiality in this context means that the safety action, system, or limit is essential to satisfying the nuclear safety operational criteria. Essentiality is found through an analysis in which the safety action, system, or limit being considered is completely disregarded in the analyses of the applicable operations or events. If the nuclear safety operational criteria are satisfied without the safety action, system, or limit, then the safety action, system, or limit is not essential, and no operational nuclear safety requirement would be indicated. When disregarding a safety action, system, or limit results in violating one or more nuclear safety operational criteria, the safety action, system, or limit is considered essential, and the resulting operational nuclear safety requirements can be related to specific criteria and unacceptable results.

G.4.1 Protection Sequence and Safety System Auxiliary Diagrams

Block diagrams illustrate the essential protection sequences for each event requiring unique safety actions. These protection sequence diagrams show only the required front-line safety systems. The conventions used on these diagrams are shown in Figure G.4.1.

The auxiliary systems essential to the correct functioning of the front-line safety systems are shown on safety system auxiliary diagrams. The conventions used on these diagrams are shown in Figure G.4.2.

G.4.2 Operational Matrices (Matrices A through D)

Figure G.4.3 shows the concept used for presenting information in Matrices A through D. The "Plant Systems" columns of each matrix relate hardware (systems) requirements to safety actions and specific events. The "Safety Actions" columns relate safety actions to the unacceptable results for each specific event. Each matrix applies only to one BWR operating state. A safety action

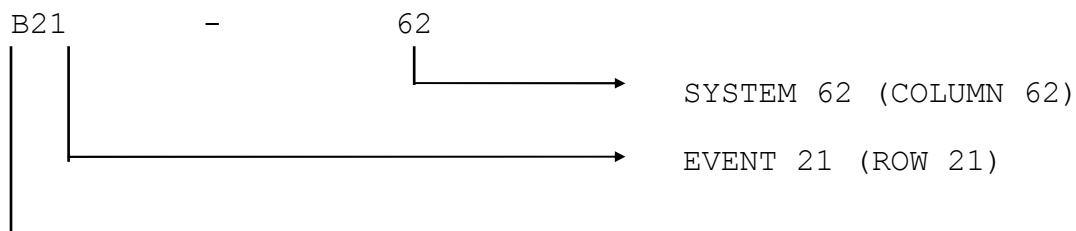
that is essential to avoiding one or more unacceptable results for a given event is identified with the number of the appropriate unacceptable result in the matrix block corresponding to the safety action and the event. The example shows that for a turbine trip the scram safety action is essential to avoiding unacceptable results 2-2 and 2-3, and the pressure relief safety action is essential to avoiding unacceptable result 2-3. Paragraph G.5.3, "Abnormal Operational Transients," lists the reasons why scram and pressure relief are needed.

A system that is essential to carrying out a safety action for a given event is identified by placing the column number of the safety action in the matrix block corresponding to the system and event. This number also can indicate that the system is an auxiliary (support system) to the system with that column number. Other symbols used in the system matrix blocks are explained in the notes to Figure G.4.3.

Safety system auxiliaries are shown as required on Matrices A through D for any event for which the front-line safety system is required. The notation used on Matrices A through D for safety system auxiliaries reflects the need, when applicable, to ensure that a safety system auxiliary is single-failure proof relative to some combination of front-line safety systems. Thus (Figure G.4.3) the notation (63-64) SF in column 83 of a matrix would indicate that the Standby ac Power System (column 83) must be single-failure proof (SF) relative to the system pair consisting of the Core Spray System (column 63) and the LPCI (column 64). Thus Matrices A through D reflect an in-depth analysis of the auxiliaries that support more than one front-line safety system.

If a front-line safety system fails safe following failure of an auxiliary system, the auxiliary system is considered nonessential and is not indicated on the block diagrams or the matrices.

Where an operational nuclear safety requirement for a system is based on a certain event, the corresponding matrix block is framed with dark lines. Operational nuclear safety requirements for a system are given in the Final Safety Analysis Report subsection describing the system, and each requirement is referenced to the most significant block on Matrices A through D. The references are given as coordinates on a Matrix as follows:



—————→ OPERATING STATE B
(MATRIX B)

The treatment on the matrices of the off-site ac power system versus the standby ac power system (on-site diesel-generators) is worth noting. Most of the transients and accidents do not necessarily involve loss of the off-site ac power supply; however, the standby ac power system is by itself capable of accommodating the events within the nuclear safety operational criteria. But the protection sequences resulting from considering only the use of the standby ac power system are all similar to the sequence for event 20, loss of auxiliary power. To reveal the characteristic differences in the protection sequences, off-site ac power is assumed available for all transients except event 20. For those transients in which the use of off-site power dictates the protection sequence, appropriate symbols are entered in column 82 (off-site ac power), but the single-failure criterion is not applied because, with off-site power, a lesser case of event 20 results. For accidents involving pipe breaks, the protection sequences shown are those that assume the use of the standby ac power system.

The entries corresponding to a given event (horizontally across the entire width of each matrix) form a comprehensive statement of the safety actions and plant systems that must be the subjects of operational nuclear safety requirements to satisfy the nuclear safety operational criteria. System requirements and safety actions are related to the criteria for which they are essential. The entries corresponding to a given system (vertically down each matrix) form a comprehensive statement of the needs for, or restrictions against, the system's actions in the designated operating state.

The material presented in Appendix G is historical and describes information relevant to the original Technical Specifications. Information may be used for understanding accidents, transients, and special events. For accurate information regarding the details of committed equipment for mitigation of these accidents, The Improved Technical Specifications (ITS), Chapter 14 of the UFSAR, or reload licensing documents may be used. |

G.5 OPERATIONAL ANALYSES FOR PEACH BOTTOM ATOMIC POWER STATION

The results of the operational analyses for Peach Bottom Atomic Power Station events are discussed in the following paragraphs and displayed in Figures G.5.1 through G.5.26. Table G.3.2 indicates the BWR operating states in which each event is applicable, and the series of Matrices A through D superimposes all the protection sequence requirements for each event.

G.5.1 Special Considerations of Particular Systems for Sequence Diagram Format

G.5.1.1 Primary Containment and Reactor Vessel Isolation and Control System (System 72)

Subsection 7.3, "Primary Containment and Reactor Vessel Isolation Control System," describes in detail the initiating signals and the valves actuated from various sensors to achieve the desired isolation actions.

G.5.1.2 Residual Heat Removal System - Low-Pressure Coolant Injection Mode (System 63) and Core Spray (System 64)

The various combinations of LPCI and core spray systems which are considered in this analysis are discussed in Section 6.0, "Core Standby Cooling Systems."

G.5.1.3 Mode Switch Positions

The various positions of the mode switch are defined in subsection 1.2, and its effects, which must be considered for several transients, are discussed in subsections 7.2, "Reactor Protection System"; 7.5, "Neutron Monitoring System", 7.6, "Refueling Interlocks"; and 7.7, "Reactor Manual Control System".

G.5.2 Planned Operations

The planned operations are defined below.

Event 1 - Refueling

Includes all the planned operations associated with a normal refueling outage except those tests in which the reactor is taken out of and returned to the shutdown (more than one rod subcritical) condition. The following planned operations are included in refueling:

1. Planned, physical movements of core components (fuel, control rods, etc).

2. Refueling test operations (except criticality and shutdown margin tests).
3. Planned maintenance.

Event 2 - Achieving Criticality

The planned operation accomplished in bringing the plant from a condition in which all control rods are fully inserted to a condition in which nuclear criticality is achieved and maintained.

Event 3 - Heatup

Begins where achieving criticality ends and includes all plant actions normally accomplished in approaching nuclear system rated temperature and pressure by using nuclear power (reactor critical). Heatup extends through warmup and synchronization of the turbine-generator.

Event 4 - Power Operation

Begins where heatup ends and includes continued plant operation at power levels in excess of heatup power.

Event 5 - Achieving Shutdown

Begins where power operation ends and includes all plant actions normally accomplished in achieving nuclear shutdown (more than one rod subcritical) following power operation.

Event 6 - Cooldown

Begins where achieving shutdown ends and includes all normal plant operations for achieving and maintaining the desired conditions of nuclear system temperature and pressure.

It may be noticed that the exact point at which some of the planned operations (events) end and others begin cannot be precisely determined. It will be seen later that such precision is not required, for the protection requirements are adequately defined in passing from one state to the next. The dependence of several of the planned operations on the one rod subcritical condition provides an exact point on either side of which protection (especially scram) requirements differ. Thus, where a precise boundary between planned operations is needed, the definitions provide the needed precision.

The requirements for the planned operations normally involve using limits on certain key process variables and restrictions on certain plant equipment. The control block diagrams for each

operating state (Figures G.5.1 through G.5.4) show only those controls necessary to avoid unacceptable safety results 1-1 through 1-4.

Following is a description of the planned operations (Events 1 through 6), as they pertain to each of the four operating states. The description of each operating state contains a definition of that state, a list of the planned operations that apply to that state, and a list of the safety actions and their corresponding column numbers that are required to avoid the unacceptable safety results.

State A

In State A the reactor is in a shutdown condition, the vessel head is off, and the vessel is at atmospheric pressure. The applicable events for planned operations are refueling and cooldown (Events 1 and 6 respectively).

Figure G.5.1 shows a diagram of the necessary safety actions for planned operations, the corresponding plant systems, and the event for which these actions are necessary. As indicated in the diagram the required safety actions are as follows:

Matrix
Column

Safety Action

3	Radioactive material release control
7	Reactor vessel water level control
9	Nuclear system temperature control
10	Nuclear system water quality control
12	Core reactivity control
14	Refueling restrictions
16	Stored fuel shielding, cooling, and reactivity control

State B

In State B the reactor vessel head is off, the reactor is not shut down, and the vessel is at atmospheric pressure. Applicable planned operations are achieving criticality and achieving shutdown (Events 2 and 5 respectively).

Figure G.5.2 shows a diagram relating the necessary safety actions for planned operations, the plant systems, and the event for which the safety actions are necessary. The required safety actions for planned operation in State B are as follows:

<u>Matrix Column</u>	<u>Safety Action</u>
3	Radioactive material release control
5	Core power level control
7	Reactor vessel water level control
9	Nuclear system temperature control
10	Nuclear system water quality control
12	Core reactivity control
13	Rod worth control
16	Stored fuel shielding, cooling, and reactivity control

State C

In State C the reactor vessel head is on and the reactor is shut down. The applicable planned operation is cooldown (Event 6). Sequence diagrams relating essential safety actions for planned operations, the plant systems, and the applicable events are shown in Figure G.5.3. The required safety actions for planned operation in State C are as follows:

Matrix
Column

Safety Action

3	Radioactive material release control
7	Reactor vessel water level control
8	Reactor vessel pressure control
9	Nuclear system temperature control
10	Nuclear system water quality control
11	Nuclear system leakage control
12	Core reactivity control
15	Primary containment pressure and temperature control
16	Stored fuel shielding, cooling, and reactivity control

State D

In State D the reactor vessel head is on and the reactor is not shut down. Applicable planned operations are achieving criticality, heatup, power operation, and shutdown (Events 2, 3, 4, and 5 respectively).

Figure G.5.4 is a diagram that relates essential safety actions for planned operations, the corresponding plant systems, and the event for which the safety actions are necessary. The required safety actions for planned operation in State D are as follows:

Matrix
Column

Safety Action

3	Radioactive material release control
4	Core coolant flow rate control
5	Core power level control
6	Core neutron flux distribution control
7	Reactor vessel water level control
8	Reactor vessel pressure control

- 9 Nuclear system temperature control
- 10 Nuclear system water quality control
- 11 Nuclear system leakage control
- 12 Core reactivity control
- 13 Rod worth control
- 15 Primary containment pressure and temperature control
- 16 Stored fuel shielding, cooling, and reactivity control

The following list relates the safety actions for planned operation with the unacceptable results for planned operation:

<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Radioactive Material Release Control	1-1	To maintain radioactive material release within 10CFR20.
Core Coolant Flow Rate Control	1-2 1-4	To limit fuel failure and to remain within the envelope of conditions considered by the plant safety analysis.
Core Power Level Control	1-2 1-4	To limit fuel failure and to remain within the envelope of conditions considered by the plant safety analysis.
Core Neutron Flux Distribution Control	1-2 1-4	To limit fuel failure and to remain within the envelope of conditions considered by plant safety analysis.

<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Reactor Vessel Water Level Control	1-2 1-4	To limit fuel failure and operate only in conditions considered by plant safety analysis.
Reactor Vessel Pressure Control	1-3 1-4	To limit nuclear process barrier stress and operate only in conditions considered by plant safety analysis and so indicate.
Nuclear System Temperature Control	1-3	To limit nuclear system process barrier stresses.
Nuclear System Water Quality Control	1-4	To remain within the conditions considered by plant safety analysis.
Nuclear System Leakage Control	1-1 1-3 1-4	To limit nuclear system process barrier stresses, to operate only in conditions considered by plant safety analysis, and to limit release of radioactive material.
Core Reactivity Control	1-4	To operate within the conditions considered by plant safety analysis.
Rod Worth Control	1-4	To operate only in conditions considered by plant safety analysis.
Refueling Restrictions	1-4	To remain within the envelope of conditions considered by plant safety analysis.

<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Primary Containment Pressure, Temperature and Atmosphere Control	1-4	To remain within the envelope of conditions considered by plant safety analysis.
Stored Fuel Shielding, Cooling, and Reactivity Control	1-2 1-4	To limit fuel failure, to provide adequate shielding of station personnel, and to maintain stored fuel to within the envelope of conditions considered by the plant safety analysis.

The following paragraphs describe the safety actions for planned operations. Each description includes a selection of the operating states that apply to the safety action, the plant system affected by limits or restrictions, and the unacceptable safety result that is avoided. The four operating states are shown in Table G.3.1.

Safety Action 3 - Radioactive Material Release Control

Radioactive materials may be released to the environs in any operating state; therefore, radioactive material release control is required in all operating states. Because of the significance of preventing excessive release of radioactive materials to the environs, this is the only safety action for which monitoring systems are explicitly shown. The stack radiation monitoring systems provide indication for gaseous release through the stack. Gaseous releases through all other vents are monitored by the reactor building ventilation monitoring system. The process liquid radiation monitors are not required, because all liquid wastes are monitored by batch sampling before release, and other potential discharge paths for the release of radioactive liquids are monitored by grab sampling. Limits are expressed on the reactor building heating and ventilating system, liquid radwaste system, and solid radwaste system so that the planned releases of radioactive materials comply with the limits given in 10CFR20 and 10CFR71 (related unacceptable safety result 1-1).

Safety Action 4 - Core Coolant Flow Rate Control

In State D, when above 12 percent rated power, the core coolant flow rate must be maintained above certain minimums (i.e., limited) to maintain the integrity of the fuel cladding (1-2) and assure the validity of the plant safety analysis (1-4).

Safety Action 5 - Core Power Level Control

The plant safety analyses pertaining to accidental positive reactivity additions have assumed as an initial condition that the neutron source level is above a specified minimum. Because a significant positive reactivity addition can only occur when the reactor is less than one rod subcritical, the assumed minimum source level need be observed only in States B and D. The minimum source level assumed in the analyses has been related to the counts per second readings on the wide range neutron monitor (WRNM); thus, this minimum power level limit on the fuel is expressed as a required WRNM count level. Observation of the limit assures the validity of the plant safety analysis (1-4). Maximum core power limits are also expressed for operating States B and D, to maintain fuel integrity (1-2) and remain below the maximum power levels assumed in the plant safety analysis (1-4).

Safety Action 6 - Core Neutron Flux Distribution Control

Core neutron flux distribution must be limited in State D where core power peaking could, unless controlled, result in fuel failure (1-2). Additional limits are expressed in this state, because the core neutron flux distribution must be maintained within the envelope of conditions considered by plant safety analysis (1-4).

Safety Action 7 - Reactor Vessel Water Level Control

In any operating state the reactor vessel water level could, unless controlled, drop to a level that will not provide adequate core cooling; therefore, reactor vessel water level control applies to all operating states. Observation of the reactor vessel water level limits protects against fuel failure (1-2) and assures the validity of the plant safety analysis (1-4).

Safety Action 8 - Reactor Vessel Pressure Control

Reactor vessel pressure control is not needed in States A and B because vessel pressure cannot be increased above atmospheric pressure. In State C a limit is expressed on the reactor vessel to assure that it is not hydrostatically tested until the temperature is above the NDT temperature plus 60°F; this prevents

excessive stress (1-3). Also, in State C a limit is expressed on the RHRS to assure that it is not operated in the shutdown cooling mode when the reactor vessel pressure is greater than 75 psig; this prevents excessive stress (1-3). In State D the same limit is expressed on the RHRS for the same reason. In States C and D a limit on reactor vessel pressure is necessitated by plant safety analyses (1-4).

Safety Action 9 - Nuclear System Temperature Control

In States C and D a limit is expressed on the reactor vessel to prevent the reactor vessel head bolting studs from being under tension when the temperature is less than 70°F and, thus, avoid excessive stress (1-3). This limit does not apply in States A and B because the head will not be bolted in place during criticality tests or during refueling. In all operating states a limit is expressed on the reactor vessel to prevent an excessive rate of change of the reactor vessel temperature to avoid excessive stress (1-3). In States C and D the feedwater system is used and a limit is placed on the reactor fuel so that the feedwater temperature is maintained within the envelope of conditions considered by the plant safety analysis (1-4). For State D, the limit observed on the temperature difference between the recirculation system and the reactor vessel prohibits the starting of the recirculation pumps. This operating restriction and limit prevent excessive thermal stress in the reactor vessel (1-3).

Safety Action 10 - Nuclear System Water Quality Control

A limit is placed on reactor coolant quality (chemical) in all operating states. For operating states where the nuclear system is pressurized (States C and D), an additional limit is placed on reactor coolant activity to assure the validity of the analysis of the main steam line break accident (1-4).

Safety Action 11 - Nuclear System Leakage Control

Because excessive nuclear system leakage could only occur while the reactor vessel is pressurized, limits are applied only to the nuclear system in States C and D. Observing these limits prevents nuclear system damage due to excessive stress (1-3) and assures the validity of the plant safety analysis (1-4).

Safety Action 12 - Core Reactivity Control

In State A during refueling, a limit is specified on core loading (fuel) to assure that core reactivity is maintained within the envelope of conditions considered by the plant safety analysis (1-4). In all states, limits are imposed on the CRDS to assure adequate control of core reactivity so that core reactivity

remains within the envelope of conditions considered by the plant safety analysis (1-4).

Safety Action 13 - Rod Worth Control

Any time the reactor is not shut down and is generating less than 10 percent power (States B and D), a limit is imposed on the control rod pattern to assure that control rod worth is maintained within the envelope of conditions considered by the analysis of the rod drop accident (1-4).

Safety Action 14 - Refueling Restriction

By definition, planned operation 1, refueling, applies only to State A. Observing procedural restrictions on reactor fuel handling maintains plant conditions within that envelope considered by the plant safety analysis (1-4).

Safety Action 15 - Primary Containment Pressure, and Atmosphere Control

In all operating states limits are imposed on the primary containment and the suppression pool storage to maintain temperature and pressure within the envelope considered by plant safety analysis (1-4). These limits assure an environment in which instruments and equipment can operate reliably within the primary containment. Limits on the suppression pool storage apply to the water temperature to assure that it has the capability of absorbing the energy discharged during a blowdown. In State D, a limit on the containment atmosphere's oxygen content assures containment integrity in case of a metal-water reaction during a loss-of-coolant accident.

Safety Action 16 - Stored Fuel Shielding, Cooling, and Reactivity Control

Because both new and spent fuel will be stored during all operating states, stored fuel shielding, cooling, and reactivity control apply to all operating states. Limits are imposed on the spent fuel storage pool storage positions, water level, fuel handling procedures, and water temperature. Observing the limits on fuel storage positions assures that spent fuel reactivity remains within the envelope of conditions considered by the plant safety analysis (1-4). Observing the limits on water level assures shielding in order to maintain conditions within the envelope of conditions considered by the plant safety analysis (1-4). Observing the limit on water temperature and water level avoids excessive fuel pool stress and fuel damage (1-2). A limit is imposed on the new fuel storage arrangement to assure that the fuel storage geometry is maintained within the envelope of

reactivity conditions considered by the plant safety analysis (1-4).

G.5.3 Abnormal Operational Transients

The safety requirements and protection sequences for abnormal operational transients are described in the following paragraphs. The protection sequence block diagrams show only the sequence of front-line safety systems. On transferring the information in the sequence diagrams to Matrices A through D, the auxiliaries for the front-line safety systems are accounted for on the matrices.

The following list relates the safety actions for transients to the unacceptable safety results. Appropriate entries are made on Matrices A through D to indicate when a safety action is essential to avoiding an unacceptable result for a given transient.

<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Scram	2-2 2-3	To prevent fuel damage and to limit nuclear system pressure rise.
Pressure relief	2-3	To prevent excessive nuclear system pressure rise.
Core cooling	2-2	To prevent fuel damage in the event that normal cooling is interrupted.
<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Reactor vessel isolation	2-2	To prevent fuel damage by reducing the outflow of steam and water from the reactor vessel, thereby limiting the decrease in reactor vessel water level.
Restore ac power	2-2	To prevent fuel damage by restoring ac power to systems essential to other safety actions.

End-of-Cycle	2-2	To prevent fuel damage and
Recirculation Pump	2-3	limit nuclear system pressure
Trip		rise by reducing core flow
		and increasing void content.

Event 8 - (number not used)

Event 9 - Electrical Load Rejection (or Turbine Trip) With Bypass

An electrical load rejection can occur in operating State D (during power operation). This transient is initiated by a power load unbalance device for load rejections greater than about 45 percent. The power load unbalance device causes turbine control valve fast closure which results in scram and RPT. Opening the main generator breaker causes turbine trip and turbine stop valve closure resulting in scram and RPT. The required safety actions and the systems required to fulfill the safety actions are the same for both causes. These events are not as severe when the initial power level is low (less than 30 percent), thus minimizing the effects of the transient and allowing return to planned operations. See Figure G.5.5 for the protection sequences required for electrical load rejections.

Event 10 - Electrical Load Rejection (or Turbine Trip) Without Bypass

These are the most severe abnormal operational transients resulting directly in a nuclear system pressure increase. As described in Event 9, these events result from a load rejection greater than about 45% causing turbine control valve fast closure, or turbine trip and turbine stop valve closure, either event occurring with failure of the bypass valves to open. These transients can only occur in State D. Loss of condenser vacuum can occur in States C or D. Scram protection in State C is not required since the reactor is in the shutdown condition (by definition).

In operating State D at more than 30% reactor power, scram is initiated to prevent fuel damage and is accomplished with the actions of the RPS and CRDS. RPT occurs from turbine stop valve closure or turbine control valve fast closure above 30% reactor power. Figure G.5.6 shows the sequence. The nuclear system pressure relief system provides pressure relief. If feedwater flow ceases, decay heat causes a decrease in reactor water level which prompts initiation of core cooling. The ADS and the low pressure core cooling systems provide core cooling until a planned operation is achieved.

Event 11 - Isolation of All Main Steam Lines

Isolation of the main steam lines can result in a transient for which some degree of protection is required only in operating States C and D. In operating States A and B, the main steam lines are continuously isolated.

Isolation of all main steam lines is most severe and rapid in operating State D during power operation. In State C isolation becomes a lesser case of the State D sequence.

Figure G.5.7 shows how scram is accomplished when main steam lines are isolated by the actions of the RPS and the CRDS. The nuclear system pressure relief system provides pressure relief. Feedwater flow stops because the feedwater pump turbine steam supply is cut off. Pressure relief combined with loss of feedwater flow causes reactor vessel water level to fall. At high pressures, the HPCIS or RCICS supplies water to maintain reactor vessel water level and protect the core.

Event 12 - Isolation of One Main Steam Line

Isolation of one main steam line causes a significant transient only in State D during high power operation. Scram is the only unique action required to avoid fuel damage and nuclear system overpressure. Because the feedwater system and main condenser remain in operation following the event, no unique requirement arises for core cooling.

As shown in Figure G.5.8, the scram safety action is accomplished through the combined actions of the neutron monitoring system, RPS, and CRDS.

Event 13 - (number not used)

Event 14 - Feedwater Controller Failure - Maximum Demand

A feedwater controller failure causing an excess coolant inventory in the reactor vessel is possible in all operating states. Feedwater controller failures considered are those that would give failures of automatic flow control, manual flow control, or feedwater bypass valve control. In operating States A and B, no safety actions are required since the vessel head is removed and the moderator temperature is low. In operating State C, because the reactor is already shut down, there are no safety actions required and the failure only results in increasing water level. In operating State D, the water level increase in the reactor causes a high level scram and turbine stop valve closure. Any adverse responses by the reactor caused by cooling of the moderator can be mitigated by the scram. As shown in Figure

G.5.9, the accomplishment of the scram safety action is satisfied through the combined actions of the neutron monitoring system, RPS, and CRDS. RPT occurs due to turbine stop valve closure. Pressure relief is required in State D and is achieved through the operation of the nuclear system pressure relief system.

Event 15 - Loss of Feedwater Heating

A loss of feedwater heating must be considered with regard to the nuclear safety operational criteria only in operating State D because significant feedwater heating does not occur in any other operating state.

When the reactor is on manual recirc. flow control, the neutron flux increase associated with this event will reach the scram setting. As shown in Figure G.5.10, the scram safety action is accomplished through actions of the neutron monitoring system, RPS, and CRDS.

Event 16 - Control Rod Withdrawal Error

Because a rod withdrawal error resulting in an increase of positive reactivity can occur under any operating condition, it must be considered in all operating states.

No unique safety action is required in operating States A and C, because the core is more than one rod subcritical. During high power operation (State D) an uninhibited, erroneous rod withdrawal cannot result in a condition requiring a unique safety action; no fuel damage results. However, during plant operation in the intermediate range (achieving criticality, heatup, and achieving shutdown in States B and/or D), a high flux scram occurs and terminates the increase in power level. As shown in Figure G.5.11, the required scram is accomplished by the neutron monitoring system, RPS, and CRDS.

Event 17 - Pressure Regulator Failure

A pressure regulator failure causing the opening of a turbine control or bypass valve applies only in operating States C and D because in other states the pressure regulator is not operated.

A pressure regulator failure, causing opening of the turbine control valves or bypass valves, is most severe and rapid in operating State D during low power.

The various protection sequences giving the safety actions are shown in Figure G.5.12. Depending on the plant conditions existing prior to the event, scram will be initiated either on

main steam line isolation, turbine trip, reactor vessel high pressure, or reactor vessel low water level. The sequence resulting in reactor vessel isolation also depends on initial conditions. With the mode switch in RUN, isolation is initiated when main steam line pressure decreases to 850 psig. Under other conditions, isolation is initiated by reactor vessel low water level. After isolation is completed, decay heat will cause reactor vessel pressure to increase until limited by the operation of the relief valves. Core cooling following isolation can be provided by either the RCICS or HPCIS. Shortly after reactor vessel isolation, normal core cooling via the main condenser and feedwater system can be re-established.

Event 18 - Inadvertent Opening of a Relief or Safety Valve

The inadvertent opening of a relief or safety valve is possible in any operating state. The protection sequences are shown in Figure G.5.13. In States A and B the water level cannot be lowered far enough to threaten fuel damage; therefore, no safety actions are required.

If the event occurs when the feedwater system is not active or during manual feedwater flow control (States C and D), a loss in the coolant inventory results in a reactor vessel low water level signal. The low water level signal initiates reactor vessel isolation in States C and D, and scram in State D. The nuclear system pressure relief system provides pressure relief. Core cooling is preferably and most probably accomplished through the automatic initiation of the HPCIS by the incident detection circuitry. The ADS remains as a backup core cooling system if needed. If needed, its manual initiation is not required for some length of time. After the vessel has depressurized, the core may be cooled by the LPCI or core spray.

If the event occurs when the feedwater system is in automatic feedwater flow control (State D) the discharge of steam to the suppression pool will cause high drywell pressure after some length of time. The high drywell pressure signal initiates primary containment isolation and scram. Due to the large number of available monitors indicating the effects of steam discharge through a relief or safety valve and the length of time necessary to raise the drywell pressure, the operator would most probably initiate plant shutdown through manual action. The nuclear system pressure relief system provides pressure relief. The core cooling sequence is similar to that described above except that the HPCI is initiated automatically on high drywell pressure.

Event 19 - Loss of Feedwater Flow

A loss of feedwater flow results in a net decrease in the coolant inventory available for core cooling. A partial or complete loss of feedwater flow can occur in States C and D. Required safety actions for this transient include a reactor scram on low water level and maintenance of reactor vessel water level. As shown in Figure G.5.14, the RPS and CRDS effect a scram on low water level. The primary containment and reactor vessel isolation control system and the main steam line isolation valves act to isolate the reactor vessel. After the main steam line isolation valves close, decay heat slowly raises system pressure to the lowest relief valve setting. Pressure is relieved by the nuclear system pressure relief system. Core cooling is achieved by restoring and maintaining water level. Either the HPCIS or the RCICS can maintain adequate water level and, as a pair, these systems satisfy the single failure criterion for core cooling.

The requirements for operating State C are the same as for State D except that the scram action is not required.

Event 20 - Loss of Auxiliary Power

There is a variety of possible electrical failures of which loss of auxiliary power is the most severe. This event is postulated to occur either due to faults or trips within the auxiliary power distribution system without transfer to outside power sources or, due to complete loss of all external connections to the distribution grid. This event can occur in any state, but the most severe event occurs in State D during power operation. Figure G.5.15 shows the safety actions required for the loss of auxiliary power.

Event 21 - Loss of Shutdown Cooling

The loss of RHR shutdown cooling can occur only during the low pressure portion of a normal reactor shutdown and cooldown.

As shown in Figure G.5.16 for most single failures that could result in loss of shutdown cooling, no unique safety actions are required; in these cases shutdown cooling is simply re-established using other, normal shutdown cooling equipment. In the cases where the RHRS shutdown cooling suction line becomes inoperative, a unique requirement for cooling arises. In States A and B, in which the reactor vessel head is off, the LPCI, or core spray can be used to maintain water level. In States C and D, in which the reactor vessel head is on, the system can be pressurized, the ADS and RHRS suppression pool cooling mode (both manually operated) can be used to maintain water level and remove decay heat.

Event 22 - Recirculation Flow Control Failure (Increasing Flow)

A recirculation flow control failure causing increased flow is applicable in States C and D. In State D, the accompanying increase in power level is accommodated through a reactor scram. As shown in Figure G.5.17, the scram safety action is accomplished through the combined actions of the neutron monitoring system, RPS, and CRDS.

Event 23 - Startup of Idle Recirculation Pump

The cold loop startup of an idle recirculation pump event can occur in any state and is most severe and rapid for those operating states in which the reactor may be critical (States B and D). When the transient occurs at lower power levels no safety action (scram) is required, since the high neutron flux setpoint is not expected to be reached following an ILS event. If an ILS event were to be initiated from high power, a high neutron flux scram might occur. The maximum core flow allowed with only one recirculation pump in service is restricted by the plant Technical Specifications. This limits the maximum core power that can be achieved with one pump in service and reduces the likelihood that an ILS event will result in a high neutron flux scram. Should the event occur when the reactor is not at power operation, but critical, the resulting transient may produce a short period scram of the WRNM's.

As shown in Figure G.5.18, the scram action is accomplished through the combined actions of the neutron monitoring system, RPS, and CRDS. When operating at power (> 10% power) the WRNM period scram is not initiated, because the core flux monitoring has been shifted to the APRM's.

G.5.4 Accidents

The safety requirements and protection sequences for accidents are described in the following paragraphs. The protection sequence block diagrams show only the sequence of front-line safety systems. On transferring the information in the sequence diagram to Matrices A through D the auxiliaries for the front-line safety systems are accounted for on the matrices.

The following list relates the safety actions for accidents with the unacceptable safety results. Appropriate entries are made on Matrices A through D when a safety action is essential to avoiding an unacceptable result for a given accident.

<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Scram	3-2 3-3	To prevent catastrophic failure of the fuel barrier as a result of exceeding mechanical or thermal limits and to prevent excessive nuclear system pressures.
Pressure Relief	3-3	To prevent excessive nuclear system pressure.
Core Cooling	3-2	To prevent catastrophic failure of the fuel barrier as a result of exceeding mechanical or thermal limits.
Reactor Vessel Isolation	3-1	To limit radiological effects to not exceed the guideline values of 10CFR100.
Establish Primary Containment	3-1	To limit radiological effects to not exceed the guideline values of 10CFR100.

<u>Safety Action</u>	<u>Related Unacceptable Result</u>	<u>Reason Action Required</u>
Establish Secondary Containment	3-1	To limit radiological effects to not exceed the guideline values of 10CFR100.
Containment Cooling	3-4	To prevent excessive pressure in the primary containment when containment is required.
Stop Control Rod Ejection (Passive)	3-3	To prevent excessive nuclear system pressure.
Restrict Loss of Reactor Coolant (Passive)	3-2	To prevent catastrophic failure of the fuel barrier as a result of exceeding mechanical or thermal limits.
Control Room Environmental Control	3-5	To prevent overexposure to radiation of plant personnel in the control room.
Limit Reactivity Insertion Rate	3-2 3-3	To prevent catastrophic failure of the fuel barrier as a result of exceeding mechanical or thermal limits and to prevent excessive nuclear system pressure.

Event 24 - Control Rod Drop Accident

The control rod drop accident results from an assumed failure of the rod-to-drive coupling after the rod becomes stuck in its fully inserted position. It is assumed that the control rod drive is fully withdrawn before the stuck rod falls out of the core at a maximum velocity of 5 ft/sec. The control rod velocity limiter, an engineered safeguard, limits the rod drop velocity to less than this value. The resultant doses due to radioactive material release are maintained below the guideline values of 10CFR100.

The control rod drop accident is applicable in operating States C and D. The rod drop accident cannot occur in States A and B

because rod coupling integrity is checked on each rod to be withdrawn if more than one rod is to be withdrawn. No safety actions are required in State C where the plant is shut down by more than one rod.

Figure G.5.19 shows the different protection sequences for the control rod drop accident. As shown in Figure G.5.19, the reactor is scrammed and isolated. For all design basis cases, the neutron monitoring system, RPS, and CRDS will produce a high flux scram.

The main steam line radiation monitoring system causes the reactor vessel to isolate and provides indication to the operator to establish primary containment.

After the reactor has been scrammed and isolated, the pressure relief system allows the steam (produced by decay heat) to be directed to the suppression pool. Initial core cooling is accomplished by either the RCICS or the HPCIS. As indicated in Figure G.5.19, the operator initiates the RHRS containment cooling mode and depressurizes the vessel with the ADS. The LPCI, HPCIS, or core spray system maintains the vessel water level and accomplishes extended core cooling.

Event 25 - Pipe Breaks Inside Primary Containment

Pipe breaks inside the primary containment are considered only when the nuclear system is pressurized. The result is a release of steam or water into the primary containment. The most severe case is the circumferential break of the largest recirculation system pipe. This is called the design basis accident for the loss of coolant from a pipe break inside the primary containment.

As shown in Figure G.5.20, in operating State C (reactor shutdown, but pressurized) a pipe break accident up to the design basis accident can be accommodated within the operational nuclear safety criteria through the various operations of the applicable safety-related systems. For small pipe breaks inside the primary containment, pressure relief is effected by the nuclear system pressure relief system, which transfers decay heat to the suppression pool. For large breaks, depressurization takes place through the break itself. In operating State D (reactor not shut down, and pressurized) the same equipment is required as in State C but, in addition, the RPS and the CRDS must operate to scram the reactor.

The CRD housing supports are considered necessary whenever the system is pressurized to prevent excessive control rod movement through the bottom of the pressure vessel following the postulated rupture of one control rod drive housing (a lesser case of loss-of-coolant accident).

Manual operation of the RHRS containment cooling mode is required during long term cooldown following the accident.

Event 26 - Fuel Handling Accident

Because a fuel handling accident can potentially occur any time when fuel assemblies are being manipulated, either over the reactor core or in the spent fuel pool, this accident is considered in all operating states. Considerations include mechanical fuel damage caused by impact and a subsequent release of fission products. The protection sequences pertinent to this accident are shown in Figure G.5.21. Secondary containment isolation and the standby gas treatment system are automatically initiated by the reactor building ventilation radiation monitoring system.

Event 27 - Pipe Break Outside Primary Containment

Pipe break accidents outside the primary containment are assumed to occur any time the nuclear system is pressurized (States C and D). This accident is most severe during operations at high power (State D). In State C, this accident becomes a lesser case of the State D sequence.

The protection sequences for the various possible pipe breaks outside the primary containment are shown in Figure G.5.22. The sequences also show that for small breaks (breaks not requiring immediate action) the operator can use a large number of process indications to identify the break and isolate it (Figure G.5.22).

In operating State D scram is accomplished through operation of the RPS and the CRDS. Reactor vessel isolation is accomplished through operation of the main steam line isolation valves and the primary containment and reactor vessel isolation control system.

For a main steam line break, core cooling is initially accomplished by either the HPCIS or the ADS in conjunction with either the LPCI or core spray systems. These systems provide two parallel paths to effect initial core cooling, thereby satisfying the single failure criterion. Extended core cooling is accomplished by the single failure proof, parallel combination of core spray or LPCI. The ADS and the RHRS containment cooling mode (both manually operated) are required during long term cooldown following the accident.

Event 28 - (number not used)

G.5.5 Safety System Auxiliaries

Figures G.5.23a and G.5.23b show the safety system auxiliary essential to the functioning of each front-line safety system. When the associated front-line safety system appears in a protection sequence, appropriate entries are made on Matrices A through D to show that the safety system auxiliaries are also required.

The ac emergency auxiliary switchgear includes the emergency auxiliary buses, load centers, and motor control centers, including the supply breakers off the buses, load centers, and motor control centers, down to the breakers for the individual electrical loads. The standby ac power system includes the diesel-generators and associated and auxiliary equipment, including the diesel-generator breakers. The off-site ac power system includes all electrical power distribution equipment which is necessary to transmit off-site ac power to electrical loads and which is not included in the ac emergency auxiliary switchgear or the standby ac power system.

G.5.6 Special Events

Special events are postulated to demonstrate some special capability of the plant. As such, special events do not belong in any of the other event categories. The safety action listed on the matrices for the special events follows directly from the requirement to demonstrate the special plant capability.

Event 29 - Shutdown from Outside Control Room

Shutdown from outside the control room is a special event investigated to evaluate the capability of the plant to be safely shut down and maintained in the shutdown condition from outside the control room. Special criteria given in subsection 7.18, "Separate Shutdown Control Stations," apply to this event. The event is applicable to any operating state. Figure G.5.24 shows the protection sequences for this event in each operating state.

A scram and main steam line isolation valve closure is assumed initiated from the control room prior to abandonment, but could also be accomplished from outside the control room by opening the ac supply breakers for the RPS. De-energizing the RPS also causes main steam line isolation. Once the nuclear system becomes isolated from the reactor, decay heat is transferred from the reactor to the suppression pool via the relief valves. The incident detection circuitry initiates operation of the HPCIS on

low water level, and the RCICS is controlled from the separate shutdown control panels, maintaining reactor vessel water level. Relief valve actuation can also be initiated, as required, from the remote panels. If access to the control room cannot be regained for some indeterminate period, nothing in the design of the plants prevents the use of emergency procedures to bring the plants to the cold shutdown condition by methods described in subsection 7.18, "Separate Shutdown Control Panels."

Event 30 - Shutdown Without Control Rods

The plant has the capability to shut down the reactor independently of the CRDS by use of the standby liquid control system. This event is applicable in States B and D.

The standby liquid control system operates to avoid unacceptable result 4-3. The design bases for the standby liquid control system assume the most severe condition (State D at rated power). As indicated in Figure G.5.25 and the matrices for States B and D, the standby liquid control system is manually initiated and controlled.

Event 31 - Loss of Normal Heat Sink

Loss of normal heat sink is a special event associated with the capability to safely shut down the plants and maintain them shut down on a long term basis upon the loss of Conowingo Pond as the normal heat sink. Special criteria given in subsection 10.24, "Emergency Heat Sink," apply to this event. The event is applicable to any operating state. Figure G.5.26 shows the protection sequence for this event for all states.

If the normal heat sink (Conowingo Pond) is lost, the high-pressure and emergency service water systems can supply cooling water for decay heat removal from the on-site, 3.7 million-gal reservoir, with the return water being cooled by the emergency cooling tower, thus avoiding unacceptable safety result 4-4.

G.5.7 Other Events

To assess the capabilities of Peach Bottom Units 2 and 3 for plant shutdown through hot standby and cold conditions, a study of the equipment actuation sequence was made for the more restrictive, although extremely remote, case of simultaneous:

- (a) Loss of offsite power.
- (b) On-site power availability of 3 out of 4 emergency diesel generators.

- (c) Concurrent trip of the turbine-generator of each units, and
- (d) Loss of capability of all seismic Class II equipment and structures (including condensate storage tank).

The expected sequence of equipment actuation for the case described above is presented as Table 14.5.1. The sequence shows that required manual actuations only occur after ten minutes and can be easily accomplished by the operators in a controlled fashion.

A detailed equipment actuation sequence required to shut the plant down through hot standby to a cold condition is given in Appendix G and illustrated on Figure G.5.15. The only non-automatic parameters considered are the initiation of suppression pool cooling at approximately 10 minutes and the initiation of controlled reactor depressurization at a pool temperature of 130°F.

Further analysis of the loss of off-site power with concurrent trip of the turbine-generator has been described in paragraph 14.5.4.4 as the loss of auxiliary power by loss of all external connections to the grid.

Design conditions of 90°F river water temperature, 90°F torus water temperature, and 135°F drywell temperature were assumed as initial.

Analytical constraints imposed in the analyses to demonstrate the design capability were:

- a. Reactor depressurization will start before torus water exceeds 130°F (no heat loss from the torus is assumed).
- b. HPCI/RCIC pumps will be secured before torus water exceeds 140°F.
- c. Reactor cooldown to 300°F (for shutdown cooling mode) before torus water temperature exceeds 170°F. Analysis of the RHR pump NPSH requirement showed that, even assuming the torus pressure remains atmospheric (14.7 psia), adequate NPSH is available for a torus water temperature of 176°F. Therefore, this requirement further assures that adequate NPSH is available.
- d. Reactor depressurization shall be accomplished using one or more of the five ADS relief valves at a rate not to exceed a reactor cooldown of 100°F/hour.

- e. After 1 hour the diesel-generator loads must not exceed the 2,000 hour rating (3,000 kW).
- f. Drywell temperature should not exceed 281°F, the containment vessel design temperature.

Each unit will automatically restore reactor level using the HPCI and RCIC pumps in less than 10 minutes. Thereafter, the operator has the option of allowing automatic operation of HPCI or RCIC or manually controlling flow. At or before 10 minutes, the operator manually lines up one RHR pump, one RHR heat exchanger, and one HPSW pump in the suppression pool cooling mode for the unit with the lower (decay heat) power history (assume Unit 3). Two RHR pumps, two RHR heat exchangers and two HPSW pumps are placed in the other unit (Unit 2). At 10 minutes, the Unit 3 operator commences a controlled depressurization (reactor cooldown rate of 100°F/hour) by manually operating the relief valves. After 30 minutes an operator commences a similar cooldown of Unit 2. At approximately $t = 1$ hour - 40 minutes the Unit 3 torus temperature reaches 140°F and the HPCI/RCIC for that unit are secured.

At approximately 2-3/4 hours, Unit 3 has been cooled sufficiently to enable it to be lined up in the shutdown cooling mode (torus temperature = 163°F, drywell temperature = <200°F). At approximately 3 hours Unit 2 can be put in the shutdown cooling mode (torus temperature = 156°F, drywell temperature 205°F).

The analysis of the sequence of events showed that torus water (see Figure 14.5.16) and drywell (see Figure 14.5.17) temperature limits were not exceeded over the entire range, the reactor cooldown rate of 100°F/hr was not exceeded, and the electrical loading on the diesel generators did not exceed the diesel generator rating. Figure 14.5.17 was originally developed using an initial drywell average temperature of 135°F. Due to the margin in excess of 50°F between the drywell temperature response and the drywell temperature limit of 281°F, these conclusions are also valid for an initial drywell bulk average temperature of 145°F.

Relief valve operational capability was examined. The individual accumulators on the five ADS relief valves provide a minimum of five operations for each valve. The reactor cooldown rate of 100°F/hr was maintainable over the cooldown range within the number of valve operations available.

The temperatures of the compartments outside the torus compartment housing seismic Class I equipment will not exceed the design limits on equipment operation. These compartments have redundant

unit coolers supplied from the emergency buses. The cooling water is supplied from the emergency service water system.

Fuel pool cooling was also examined. With no cooling available other than evaporative cooling, the temperature of the pool would rise at a rate of approximately 3°F/hour, with a corresponding pool level decrease of approximately 1 inch/hour. Makeup is always available from the RHR system. The RHR system can provide cooling to the fuel pool when the reactor pressure decreases to 15 psig (250°F), and this will be achieved approximately 5-1/2 hours after initiating reactor shutdown cooling from a reactor water temperature of 300°F. Structurally the fuel pool can withstand a pool temperature of 212°F, although this will not be approached before cooling can be re-established using the RHR system. It was concluded that no unacceptable condition would exist.

Should four diesels be available the procedure would remain essentially the same, but with two RHR pumps, two RHR heat exchangers and two HPSW pumps lined up for suppression pool cooling on each unit at or before 10 minutes. The only difference would be the reduced torus temperature rate of rise and ultimate torus temperature for the first unit cooled down.

Should off-site power be available, but without seismic Class II systems, the procedure would remain the same as for the situation without off-site power but with four diesels.

For the case of no off-site power and only three diesels available, but with seismic Class II systems available, the cooldown of the unit with one RHR pump, one RHR heat exchanger and one HPSW pump could be delayed up to 30 minutes, and the second unit cooldown delayed up to 1 hour, and still remain within the imposed parameters. The use of the condensate storage tank as the suction source and cooling medium for the HPCI/RCIC pumps would ensure availability of the pumps down to a reactor pressure of approximately 100 psig since RCIC/HPCI pump operations are not restrained by 140°F limit. The resultant torus temperatures would be approximately the same as those for the case without the condensate storage tank available.

With off-site power and seismic Class II systems available, the initial torus water and drywell temperature would remain approximately the same over the cooldown period. No constraints would exist for the operator except to establish a cooldown rate at or less than the 100 F/hour using the main condenser as the heat sink and the condensate storage tank as the suction source and cooling medium for the HPCI/RCIC pump.

Thus, it is within the capability of Peach Bottom Units 2 and 3 to shutdown and cooldown both units simultaneously in a controlled and safe manner, even for the remotely possible degraded conditions examined. Unusual and critical procedural requirements are not imposed for the timeliness or method of operator actions. Normal operating limitations on equipment are not exceeded. Thus, the operator is provided with flexibility of action while maintaining margin to the equipment design limits should it become necessary or required by the situation.

Diesel generator "A" supplies power to the inboard shutdown cooling valve in both of the units. Consequently, the unavailability of that diesel generator would prevent using the RHR shutdown cooling mode.

Should the shutdown cooling mode of RHR not be available even for both reactors, the units can still be safely maintained in the shutdown condition. In this situation the relief valves will be left in the open condition to maintain reactor vessel pressure at approximately 50 psig while relieving decay heat to the torus via the relief valve discharge path. The RHR system will be used to provide make-up water to the reactors as well as to remove heat from the tori. Analysis has shown that by maintaining one RHR pump and heat exchanger in the suppression pool cooling mode on each unit and alternately running a second RHR pump and heat exchanger on one of the units for about one hour and then on the other unit for about an hour, the maximum suppression pool temperature will be approximately 175°F for the unit with the higher torus temperature (see Figure 14.5.18). Thus adequate NPSH for the RHR pumps will be maintained. For this unlikely condition drywell ambient temperature on both units will continue to rise and for Unit 2 will reach the containment vessel design temperature of 281°F at approximately 26 hours after the reactors scrammed (see Figure 14.5.19). If the analysis were performed at the initial drywell bulk average temperature of 145°F instead of 135°F, the temperature curves in Figure 14.5.19 would shift slightly to the left. The drywell temperature would reach 281°F at approximately 25 hours instead of 26 hours.

Assuming that containment spray is not initiated, drywell ambient temperatures could reach 300°F in both units at approximately 40 hours after the reactors have scrammed. The ambient temperature in the drywells will remain near 300°F until either the reactors are cooled down or drywell cooling is restored. Exceeding the containment design temperature by only about 20°F for the remotely possible conditions postulated is not expected to prejudice the integrity of the containment.

TABLE G.5.1

SEQUENCE OF EVENTS

Expected sequence of events for condition of loss of off-site power, loss of one diesel-generator, Class II systems unavailable (including condensate storage tanks), and turbine-generator trip on both units.

<u>Time</u>	<u>*Unit</u>	<u>Function</u>	<u>Event</u>
0 sec	2 & 3	Automatic (A)	Diesel logic initiated.
<1 sec	*2 & 3	A	Reactors scram.
3 sec	2 & 3	A	Diesels (3) start.
~10 sec	*2 & 3	A	Reactor water level reaches low level; PCIS and SGTS valve operation initiated.
<13 sec	2 & 3	A	Diesels up to operating speed and connected to emergency buses.
13 sec	2 & 3	A	RHR pumps start.
<16 sec	2 & 3	A	Diesels pick up 460-V loads; PCIS and SGTS actions go to completion
20 sec	2 & 3	A	Reactor water level reaches low-low (490 inches), HPCI and RCIC start logic initiated.
<49 sec	Common	A	ESW pump started.
5-6 min	2 & 3	A	Reactor water level at high level; HPCI and RCIC pumps trip off.

*Transient analysis for first 20 seconds after reactor scram for this sequence is presented in paragraph 14.5.4.4 and shown in Figure 14.5.11b.

TABLE G.5.1 (Continued)

<u>Time</u>	<u>*Unit</u>	<u>Function</u>	<u>Event</u>
10 min	2	Manual (M)	Align two RHR pumps and heat exchangers in the suppression pool cooling mode and two HPSW pumps on Unit 2.
	3	M	Start one RHR pump and heat exchanger in the suppression pool cooling mode and one HPSW pump on Unit 3.
	2 & 3	M	Reset RCIC turbines.
	3	M	Commence cooldown of Unit 3 at 100°F/hr.
	2 & 3	M	Secure standby gas treatment systems.
(10-100 min)	3	M	Maintain water level in reactors with RCIC manually controlling flow or starting and stopping the turbines as necessary to maintain water level above 490 inches.
(10-115 min)	3	A	
30 min	2	M	Commence cooldown of Unit 2 at 100°F/hr.
~62 min	3	A	Unit 3 satisfies low pressure permissive (500 psig); core spray pump starts, LPCI injection valve opens, CS valve opens.
	3	M	Restore equipment to cooldown lineup.
~82 min	2	A	Unit 2 satisfies low pressure permissive (500 psig); CS pump starts, LPCI injection valve opens, core spray valves open.

TABLE G.5.1 (Continued)

<u>Time</u>	<u>*Unit</u>	<u>Function</u>	<u>Event</u>
	2	M	Restore equipment to cooldown lineup.
~92 min	3	N/A	Unit 3 reaches shutoff head of RHR pump.
~100 min	3	M	Unit 3 suppression pool temperature approaches 140°F. Secure Unit 3 RCIC/HPCI turbines.
~112 min	2	N/A	Unit 2 reaches shutoff head of RHR pump.
~115 min	2	M	Unit 2 suppression pool temperature reaches 140°F; secure Unit 2 HPCI/RCIC turbines.
~165 min	3	M	Place Unit 3 in shutdown cooling mode, (reactor temperature reaches pressure <75 psig).
100-165 min	3	M	Maintain water level in Unit 3 reactor above 490 inches using the RHRS.
180 min	2	M	Place Unit 2 in the shutdown cooling mode, (reactor pressure <75 psig).
115-180 min	2	M	Maintain water level in Unit 2 reactor above 490 inches using the RHRS.

The material presented in Appendix G is historical and describes information relevant to the original Technical Specifications. Information may be used for understanding accidents, transients, and special events. For accurate information regarding the details of committed equipment for mitigation of these accidents, The Improved Technical Specifications (ITS), Chapter 14 of the UFSAR, or reload licensing documents may be used.

G.6 REMAINDER OF NUCLEAR SAFETY OPERATIONAL ANALYSIS

With the information presented in the protection sequence block diagrams and in Matrices A through D, it is possible to determine the exact functional and hardware requirements for each system. This is done by considering each entry in the matrix column for a system. This remaining part of the nuclear safety operational analysis is presented in those portions of the Final Safety Analysis Report where the subject system itself is described and evaluated. In each section on "Operational Nuclear Safety Requirements," the essential actions of the system are identified (using Matrices A through D as a guide). Then requirements and restrictions are established for system hardware to assure that the essential actions can be achieved within the redundancy goals set for the system or action.

To derive the operational requirements and technical specifications for the individual components of a system included in any essential protection sequence, the following steps are taken:

1. Identify all the essential actions within the system (intrasystem actions) necessary for the system to function to the degree necessary to avoid the unacceptable results:
2. Identify the minimum hardware conditions necessary for the system to accomplish the minimum intrasystem actions.
3. If the single failure criterion applies, identify the additional hardware conditions necessary to achieve the plant safety actions (scram, pressure relief, isolation, cooling, etc.) in spite of single failures. This step gives the operational nuclear safety requirements for the plant components so identified.
4. Identify surveillance requirements and allowable repair times for the essential plant hardware.

The action that must be taken (should an operational nuclear safety requirement not be met) can be determined by considering the associated unacceptable safety results.

5. The operational nuclear safety requirements derived using the above process may be complicated functions of operating states, parameter ranges, and hardware conditions. Simplify the operational requirements determined in steps 3 and 4 to obtain technical

specifications that encompass the true operational requirements and are easily used by plant operations and management personnel. The first four of the above five steps are accomplished in the subsections of the Final Safety Analysis Report where the subject system is described and evaluated. The fifth step is accomplished in the Technical Specifications, Appendix B.

It is concluded that the operational nuclear safety criteria are satisfied when the plant is operated in accordance with the operational nuclear safety requirements determined by the method presented in this appendix.