APPENDIX G

PLANT NUCLEAR SAFETY OPERATIONAL ANALYSIS

This appendix delineates the analytical methods which were used to derive the BFNP Technical Specifications. This appendix is retained for historical purposes.

G.1 ANALYTICAL OBJECTIVE

The objective of the nuclear safety operational analysis is to systematically identify the requirements for and limitations on plant operation necessary to satisfy nuclear safety operational criteria.

Definitions of key terms used in this appendix are given in Subsection 1.2, "Definitions."

G.2 BASIS FOR SELECTING OPERATIONAL REQUIREMENTS

An operational requirement is a requirement or restriction on either the value of a process 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. 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 selected for one of two basic reasons:

1. A requirement is considered essential if the requirement is necessary to assure that some specified condition (unacceptable result) is avoided during or following some specified plant event.

2. A requirement is considered essential if the requirement is necessary to avoid some specified condition (unacceptable result) in spite of a single failure during or following some specified plant event.

A systematic method is used to identify operational requirements based on these two reasons.

G.2.1 Unacceptable Safety Results

The following listed conditions are the unacceptable safety results used as the major reasons for selecting system operational requirements. The different groups of unacceptable safety results are associated with different categories. Several of the unacceptable safety results are superior; in importance to the others; these superior, unacceptable safety results are marked with an asterisk.

The unacceptable safety results have been associated with the different categories of plant operation and events to facilitate the systematic selection of operational requirements. All the criteria must be satisfied at all times.

Plant Event Category	Unacceptable Safety Result	
1. Normal Operation	*1-1.	The release of radioactive material to the environs to such an extent that the limits of 10 CFR 20 are exceeded.
	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 10 CFR 20 would be exceeded.
	1-3.	Nuclear system stress in excess of that allowed for planned operation by applicable industry code.
	1-4.	The existence of a plant condition not considered by plant safety analysis.

Plant Event Category		Unacceptable Safety Result
2. Abnormal Operational Transients	2-1.	The release of radioactive material to the environs to such an extent that the that the limits of 10 CFR 20 are exceeded.
	2-2.	Any fuel failure calculated as a result of the transient.
	2-3.	Nuclear system stress in excess of that allowed for transients by applicable industry codes.
3. Accidents	*3-1.	Radioactive material release to such an extent that the guideline values of 10 CFR 100 would be exceeded.
	3-2.	Fuel cladding temperature in excess of 2200°F or peak fuel enthalpy greater than 280 cal/g.
	3-3.	Nuclear system stresses in excess of that allowed for accidents by applicable industry codes.
	3-4.	Containment stresses in excess of that allowed for accidents by applicable industry codes when containment is required.
	3-5.	Overexposure to radiation of plant operations personnel in the control room.

Plant Event Category		Unacceptable Safety Result
4. Special Event--Loss of habitability of the control room	4-1.	The inability to bring the reactor to the cold shutdown condition by manipulation of the local controls and equipment which are available outside the control room.
	4-2.	The inability to bring the reactor to the cold shutdown condition from outside the control room.
5. Special Event--Inability to shut down reactor with control rods.	5-1.	The inability to shut down the reactor independent of control rods.

G.2.2 Nuclear Safety Operational Criteria

The following nuclear safety operational criteria are used to select operational requirements:

Applicability	Criteria Identification	Nuclear Safety Operational Criteria
General	G	The plant shall be operated in such a manner that the unacceptable safety results are avoided.
Abnormal Operational Transients and Accidents	SF	The plant shall be operated in such a manner 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 frequent testing of a redundant system.

G.2.3 Origin of the Unacceptable Safety Results and Criteria

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 hardware design is required by design criteria to offer a specified degree of protection for a radioactive material barrier under certain circumstances, actual plant operation is required by operational criteria to offer the same degree of protection under the same circumstances.

The unacceptable temperature limit of 2200°F for accidents is a result of experiments with highly oxidized Zircaloy. It has been determined that at high temperatures this material may fragment as it is cooled. If the maximum cladding temperature is maintained below 2200°F, no cladding fragmentation will occur and no impediment to core cooling will result from changes in core geometry.

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 for which safety analysis has been performed. In a case where a system has not been shown to be nonessential to some safety action, the system would be considered essential under this criterion until proven otherwise. Thus, definitive safety analysis is a prerequisite to a finding of nonessentiality for a system or system action.

G.3 BASIS FOR SELECTION OF SURVEILLANCE TEST FREQUENCIES FOR NUCLEAR SAFETY SYSTEMS AND ENGINEERED SAFEGUARDS

G.3.1 Normal Surveillance Test Frequencies

After the essential nuclear safety systems and engineered safeguards have been identified through the application of the nuclear safety operational criteria, surveillance requirements are selected for these systems. In the course of selecting surveillance test frequencies, the various systems are considered in terms of relative availability, test capability, plant conditions necessary for testing, and engineering experience with the system type. The surveillance test frequency selected represents the application of engineering judgment integrating all of these considerations. However, the surveillance frequencies selected are conservative with respect to the surveillance requirements actually needed to maintain the reliability of the system as provided by the basic system design.

G.3.2 Allowable Repair Times

Allowable repair times are determined through engineering judgment. These times are conservative in comparison to those computed using availability analysis methods[1] for redundant, standby systems. The resulting maximum average allowable repair times assure that a system's long-term availability, including allowance for repair, is not reduced below the availability that would be achieved if repairs could be made in zero time.

G.3.3 Repair Time Rule

Repair of a safety system may be carried out while the reactor is in operation for a time equal to the maximum allowable average repair time. If repair is not complete when the allowable repair time expires, the reactor plant must be placed in its safest mode for potential radiological releases (with respect to the protection lost).

To maintain the validity of the assumptions used to establish the above repair time rule, the following restrictions must be observed.

1. Routine maintenance on shared systems, which are always needed, should be conducted to keep the equipment out of service for as short a time as possible, but never longer than the allowable repair time. Routine maintenance and testing should be scheduled where possible when the equipment is not needed.

2. Once the need for repair of a failed device is discovered, repair should proceed as quickly as possible consistent with good craftsmanship.

G.4 METHOD OF ANALYSIS

The nuclear safety operational analysis is performed after the plant detailed design has been established. The end products of the analysis are the operational nuclear safety requirements, restrictions, and limits on plant hardware and its operation, which must be observed to satisfy the nuclear safety operational criteria. The key steps in this analysis are as follows.

1. Identify and define the physical states (operating states) in which the BWR core may operate (exist).

2. For each operating state, identify the types of operations (planned) and events (transients, accidents, and special events) that the plant must accommodate within the nuclear safety operational criteria.

---

[1] Jacobs, I. M. "Guidelines for Determining Safe Test Intervals and Repair Times for Engineered Safeguards," General Electric Company, Atomic Power Equipment Department, April 1969 (APED 5726).

3. For each operating state, identify the safety actions essential to accommodating each applicable type of operation and event within the nuclear safety operational criteria.

4. For each operating state, identify the systems or variables (to be limited) that are essential to achieving each required safety action. Systems that are needed for the achievement of a safety action with a specified degree of redundancy are considered essential to the safety action. Limitations on process variables should be associated with the applicable unacceptable result and the related plant system originating the need for the limit.

5. For each system identified in step 4, identify the specified system functional requirements and restrictions that must be observed within each operating state. For each key process variable identified in step 4, establish the limits which must be observed in each operating state.

6. Identify the minimum amount of system hardware that must be operable (or restricted from operation) to accomplish the functional requirements (and restrictions) identified in step 5.

7. For each system, identify the conditions (operability, numbers of components, out-of-service times, inspection, and test frequencies) that must be met to accomplish (with an acceptable level of redundancy and availability) the system functional requirements (and restrictions) identified in step 5.

The results of steps 1, 2, 3, and 4 are presented in this appendix. The results of steps 5, 6, and 7 for each system and variable identified in step 4 are presented in the subsections of the safety analysis report that describe the system.

Together, the plant design and the observation of the operational nuclear safety requirements derived in this analysis assure that the nuclear safety operational criteria are satisfied. When an operational nuclear safety requirement for a system is combined with the action to be taken if the requirement cannot be met, a technical specification is formed. Figure G.0-1 shows in block form the process by which technical specifications are derived. Appendix B lists the Technical Specifications for the Browns Ferry Nuclear Plant.

G.5 ANALYSIS AND RESULTS

G.5.1 Identification of BWR Operating States

Six BWR operating states are identified and defined in Matrix 1. Some states, such as pressurized with the reactor vessel head removed, are eliminated by virtue of their impossibility. But the main objective in the selection of operating states is to

divide the BWR operating spectrum into a few major conditions to facilitate the considerations of various events in each state. The operating states identified include all the conditions in which the core can exist.

It is recognized that each of the identified operating states includes a wide spectrum of values for important plant parameters. Within each operating 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 the safety analysis report where the systems originating the requirement for the parameter limit are described. The plant parameters to be considered in this manner include the following:

Reactor coolant temperature,
Reactor vessel water level,
Reactor vessel pressure,
Reactor vessel water quality (chemical and radioactivity),
Reactor coolant forced circulation flow rate,
Reactor power level (thermal and neutron flux),
Core neutron flux distribution, and
Feedwater temperature.

G.5.2 Identification of Types of Operation and Events Applicable in Each BWR Operating State

G.5.2.1 Identification Method

Matrix 2 identifies the planned operations, abnormal operational transients, accidents, and special events that are to be considered in determining plant operational nuclear safety requirements and restrictions. Planned operations are to be considered without regard to the need for anticipating abnormal operational transients, accidents, or special events because these events are considered separately. The abnormal operational transients and accidents listed on the matrix were selected and categorized by the same methods as those described in Chapter 14.0, "Plant Safety Analysis." In each case, the events listed cause the most severe demand for protective action of any events of a similar nature.

The planned operations are defined as follows.

1. Planned Operation--Planned operation is normal plant operation under planned conditions in absence of significant abnormalities. Operations subsequent to an incident (transient, accident, or special event) are not considered planned operations until the actions taken in the plant are identical to those that would be used had the incident not occurred. The established planned operations can be considered as chronological: refueling outage,

achieving criticality, heatup, power operation, achieving shutdown, cooldown, refueling outage.

2. Refueling Outage--Refueling outage includes all of the planned operations associated with a normal refueling outage:

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

   (2) Refueling test operations, and

   (3) Planned maintenance.

3. Achieving Criticality--Achieving criticality includes all the plant actions that are normally 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.

4. Heatup--Heatup begins where achieving criticality ends and includes all plant actions that are 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.

5. Power Operation--Power operation begins where heatup ends and includes continued operation of the plant at power levels in excess of heatup power.

6. Achieving Shutdown--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.

7. Cooldown--Cooldown begins where achieving shutdown ends and includes all plant actions normally accomplished in the continued removal of decay heat and the reduction of nuclear system temperature and pressure.

The entries in Matrix 2 indicating the applicability of the planned operations are based on the definitions of the planned operations. The Matrix 2 entries indicating the applicability of an event (transient, accident, or special event) to each state are based on whether the event can occur starting from any of the initial conditions represented by the set of planned operation or event applicable in the corresponding BWR operating state.

It should be noted that, even though a given operation or event is not applicable while the reactor is in a certain operating state, operational restrictions on certain plant systems may be necessary to ensure that the given operation or event remains inapplicable. The needs for such restrictions are identified in later matrices.

G.5.2.2 Detailed Explanations of Matrix 2 Entries

The explanations for the entries made in Matrix 2 are given item-by-item in the following paragraphs.

G.5.2.2.1 Planned Operation

The entries for the planned operations all follow directly from the definitions of the planned operation and the definitions of the BWR operating states.

G.5.2.2.2 Abnormal Operational Transients

The abnormal operational transients listed as Events 12 through 36 are the same ones selected by the methods described in Section 14.0, "Plant Safety Analysis." The following paragraphs explain why certain events are applicable in certain operating states but not in others.

Events 12 and 13 - Generator and Turbine Trips

A turbine or generator trip can occur in operating states D (during heatup) or F (during power operation).

Events 14 and 15 - Main Steam Line Isolation

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

Event 16 - Loss of Vacuum (Turbine Trip Without Bypass)

Because the main condenser is normally used for the removal of decay heat under any condition in which steam is being generated, this event is applicable in operating states C, D, E, and F. The more significant cases are in operating state F, when the condenser is used during power operations.

Event 17 - (not used)

Event 18 - Loss of Feedwater Heating

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

Event 19 - Shutdown Cooling (RHRS) Malfunction

A shutdown cooling malfunction, causing a moderator temperature decrease, must be considered in operating states A, B, C, and D. This event is not considered in operating states E and F, because nuclear system pressure is too high to permit shutdown cooling (RHRS) operation.

Event 20 - Inadvertent Pump Start (Temperature Decrease)

The addition of cold water via an inadvertent start of a pumping system must be considered in all operating states because this event can potentially occur under any operating condition.

Event 21 - Control Rod Withdrawal Error

The results of adding positive reactivity via a control rod withdrawal error must be considered in all operating states. A rod withdrawal error can potentially occur under any operating condition.

Events 22 and 23 - Removal of Control Rod and Fuel Assembly Insertion

An inadvertent positive reactivity insertion can result from erroneous control rod removal, or fuel assembly insertion. Because these actions can occur only when the reactor vessel head is removed and manipulation of the refueling equipment over the reactor core is possible, operating state A is the only state in which these events must be considered.

Event 24 - (not used)

Event 25 - Pressure Regulator Failure

A pressure regulator failure, causing a coolant inventory decrease, is applicable only in operating states C, D, E, and F, because in none of the other states is the reactor pressurized.

Event 26 - Inadvertent Opening of Main Steam Relief Valves

The inadvertent opening of a main steam relief valve is possible in any operating state.

Event 27 - Loss of Feedwater Flow

Because continuous feedwater flow is neither required nor provided in operating states A and B, a loss of feedwater flow need only be considered in operating states C, D, E, and F.

Event 28 - Total Loss of Offsite Power

The effects of a loss of auxiliary power must be considered in each operating state.

Events 29, 30, 31, and 32 - Core Coolant Flow Decreases

Because forced coolant circulation would be present as a planned operation only in operating states C, D, E, and F, events causing loss of forced circulation flow need be considered only in these states.

Event 33 - Recirculation Flow Control Failure Increasing Flow

Because a recirculation flow control failure, causing an increased coolant flow through the core, can occur only when a recirculation pump is initially operating during planned operation, this event is applicable only in operating states C, D, E, and F.

Event 34 - Startup of Idle Recirculation Pump

A startup of an idle recirculation pump can potentially occur in any operating state.

Event 35 - Loss of Shutdown Cooling

Malfunctions causing loss of RHR shutdown cooling are considered in operating states A, B, C, and D, because only in these states would the RHR shutdown cooling system be in use as part of one of the planned operations.

Event 36 - Feedwater Controller Failure - Maximum Demand

A feedwater controller failure, causing an excess coolant inventory in the reactor vessel, must be considered in operating states C, D, E, and F because only in these states can the feedwater controller be in operation as part of the planned operations.

G.5.2.2.3 Accidents

The accidents listed in Matrix 2 as Items 38 through 41 are the same ones selected by the methods described in Section 14.0, "Plant Safety Analysis." The following paragraphs explain why certain accidents are applicable in certain operating states but not in others.

Event 38 - Control Rod Drop Accident

The control rod drop accident is applicable in operating states C, D, E, and F. 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 states C and E, where the plant is shut down by more than one rod prior to the accident.

Event 39 - Pipe Breaks Inside Primary Containment

A pipe break inside the primary containment is not applicable to operating states A and B, because the nuclear system is not significantly pressurized in these two states.

Event 40 - 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.

Event 41 - Pipe Breaks Outside Primary Containment

A pipe break outside the primary containment is not applicable to operating states A and B because the nuclear system is not significantly pressurized in these two states.

G.5.2.2.4 Special Event- Loss of Habitability of the Control Room (Event 44)

A loss of habitability of the control room is a special event investigated to evaluate the capability of the plant to be controlled from outside the control room. Special criteria apply to this event; these criteria are given in Section 14.0, "Plant Safety Analysis." A loss of habitability of the control room is applicable to any operating state.

G.5.2.2.5 Special Event - Ability to Shut Down the Reactor Without Control Rods (Event 45)

The inability to shut down the reactor with control rods is a special event postulated to evaluate the capabilities of the Standby Liquid Control System. The criteria for evaluating this event are given in Subsection 3.8, "Standby Liquid Control System." Because this event can occur only when the reactor is initially not shut down, it is applicable only to operating states B, D, and F.

G.5.3 Identification of Safety Actions and Systems Essential to Satisfying the Nuclear Safety Operational Criteria

G.5.3.1 Introduction

To fully identify and establish the proper 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 operational criteria. This relationship is displayed in a series of block diagrams and matrices.

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 block diagrams 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. Thus, the 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. The types of operations or events that are possible within the operating state,

3. The relationships of certain safety actions to the unacceptable results and to specific types of operation and events,

4. The relationships of the actions of certain systems to the safety actions and to specific types of operation and events,

5. The supporting or auxiliary systems essential to the operation of the front-line safety systems, and

6. The 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 Matrix 3 encompasses so many safety aspects of the plant design and operation, the matrices are necessarily large and utilize a number of codes and symbols. The major point is that it is impossible to rationally set operational requirements on a given component without systematically considering each of the just-noted six aspects of the BWR on a plantwide basis. Matrix 3 and the block diagrams for the events together provide a vehicle for such a systematic analysis. Through the use of Matrix 3 and the block diagrams, any operational requirement can be traced to the unacceptable result, criterion, or safety action originating its need.

All of the indications in Matrix 3 represent 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. A finding of essentiality is made by conducting an analysis in which the safety action, system, or limit under consideration 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 disregard of a safety action, system, or limit results in violation of 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.

There is a difference between classification analyses, which provide bases for findings of essentiality, and the analyses of Chapter 14.0, "Plant Safety Analysis." Although the events analyzed are the same, the analyses of Section 14.0 represent a real response of the plant under certain limiting assumptions, whereas a classification analysis strips away all nonessential actions and systems in the effort to determine essentiality. A classification analysis represents essential plant response. The analyses of Section 14.0 emphasize "worst cases" with regard to the fuel thermal-hydraulic conditions, nuclear system pressure, or radioactivity release. The classification analyses emphasize "protection sequences."

G.5.3.2 Presentation of Information in Matrix 3

Figure G.0-2 presents the concept used for presenting information in Matrix 3. The right-hand end of each matrix relates hardware (systems) requirements to safety actions and specific events. The left side of each matrix is used to relate safety actions to the unacceptable results and specific events. Each matrix applies only to one BWR operating state. A safety action, which is essential to avoiding one or more unacceptable results for a given event, is identified by placing the identification number of the appropriate unacceptable result inside the matrix block corresponding to the safety action and the event. In Figure G.0-2, the example shows that for a turbine trip the scram safety action is essential to avoid unacceptable results 2-2 and 2-3; and the pressure relief safety action is essential to avoid unacceptable result 2-3. By referring to the lists of unacceptable results given earlier, the reasons why scram and pressure relief are needed can be precisely determined.

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. Other symbols are placed in the system matrix blocks to indicate various requirements of the system as follows.

Number	Indicates that the system is essential to a safety action with that column number, or that the system is an auxiliary (support system) to the system with that column number.

SF (single failure)	The system is required so that an essential safety failure action will meet the single-failure criterion as stated by the nuclear safety operational criteria.
S (shared)	This symbol is used following one of the previous three symbols to indicate that the system shares with another system the obligation to perform an action, meet the single-failure criterion, or meet the availability requirements. The column number of the system with which the obligation is shared is written inside parentheses with the S.
R (restricted)	One or more of the system's functions must either not be acting or not be capable of acting in order to satisfy operational nuclear safety criteria while the reactor is in the designated operating state.
L (limit)	One or more of the key process parameters must be limited to satisfy nuclear safety operational criteria while the reactor is in the designated operating state.
P (personnel action)	Credit is taken for personnel action (manual control) of the corresponding system.
Blank	None of the system's functions is required or needs to be restricted to satisfy nuclear safety operational criteria while the reactor is in the designated operating state.
Dark Frame Around Block	The framed block represents the most significant or demanding condition from which an operational nuclear safety requirement for the system is derived.
Auxiliary	This symbol identifies those systems which function as auxiliaries to the front-line safety systems.

Figure G.0-2 shows a number of examples of the use of the symbols in the system side of Matrix 3. The examples on Figure G.0-2 are interpreted on Table G.0-1.

G.5.3.3 Rules Followed in Constructing Block Diagrams and Filling in Matrices

The block diagrams and the entries made in Matrix 3 represent the consistent application of a set of rules. These rules are as follows.

1. Entries are made only when an action, limit, or system is essential to satisfying the nuclear safety operational criteria and to avoiding the unacceptable safety

results. Entries are not made simply because a system does operate or a limit is observed.

2. Entries are made for all actions, limits, and systems essential for the event through the full range of initial conditions within an operating state. Thus, consideration is not limited to worst cases only; lesser cases sometimes require actions or systems different from the worst case.

3. For planned operations, entries are 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). In this respect, 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.

4. Limits are indicated on the matrix only for those essential parameters that are continuously monitored by the operator. 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 continuously monitored parameters are called "envelope limits," and limits on periodically monitored parameters are called "operability limits." Only the envelope limits and the associated indicators for the envelope limits are indicated on the matrix; 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.

5. For transients, accidents, and special events, entries are made for the entire duration of the event and aftermath until planned operation is resumed. Planned operation is considered resumed when the procedures being followed are identical to those used during any one of the planned operations.

6. The initial conditions for transients, accidents, and special events are limited to conditions that would exist during the planned operations applicable within the operating state.

7. 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 on a case basis, depending upon the conditions that would exist at the time operator action would be required. Credit for operator action is taken only when the operator can be reasonably expected to accomplish the required action under the existing conditions. When credit for operator action is taken, a "P" is entered in the appropriate matrix block.

8. Matrix entries for transients, accidents, and special events are made only for those actions, limits, and systems for which there arises a unique requirement as a result of the event. For instance, if a system that was in operation 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. Where an operational nuclear safety requirement for a system is based on a certain event, the corresponding matrix block is framed with dark lines.

G.5.3.4 Meaning of Matrix 3

The entries corresponding to a given event (horizontally across the entire width of Matrix 3) form a comprehensive statement of the safety actions and plant systems which must be the subject 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 the entire height of a Matrix 3) form a comprehensive statement of the needs for or restrictions against the system's actions in the designated operating state. It should be noted that requirements for indications refer to either direct or indirect indications of the listed process variable.

With the information presented in Matrix 3, it is possible to determine for each system the detailed functional requirements and the detailed conditions to be observed regarding system hardware in each operating state. The detailed conditions to be observed regarding system hardware include such operational nuclear safety requirements as number of components that must be operable and test frequencies.

G.5.3.5 Detailed Explanation of Matrix 3 Entries

The following paragraphs and the associated block diagrams describe the various events from a functional and system level viewpoint. A more detailed analysis of the transients, accidents, and special events is presented in Section 14.0 to give the event results in terms of key plant parameters.

The block diagrams of the protection sequences show only the front-line systems that must perform in a protection sequence. Systems that act as auxiliaries to the front-line safety systems are identified in the block diagrams of safety system auxiliaries given in Figures G.0-3 through G.0-22. Safety system auxiliaries are shown as required on Matrix 3 for any event for which the front-line safety system is required. The notation used on Matrix 3 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, the notation

60-65SF in Column 89 of a matrix would indicate that the DC power system (Column 89) must be single-failure proof relative to the system pair consisting of the RCICS (Column 60) and the HPCIS (Column 65). In this manner, Matrix 3 reflects 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 matrix. Auxiliaries are not shown for indications or for systems needed only for planned operations.

The treatment on the matrix of the offsite AC power system versus the standby AC power system (diesel generator) is worthy of special note. Most of the transients and accidents do not necessarily involve loss of the offsite AC power supply; however, the standby AC power system is by itself capable of accommodating the various 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 very similar to the sequence for Event 28, loss of all offsite AC power. To reveal the characteristic differences in the protection sequences, offsite AC power is assumed available for all transients except for Event 28, even though offsite power is not absolutely essential to satisfying the nuclear safety operational criteria. Should offsite AC power not be available, these transients become lesser cases of Event 28. For those transients in which the use of offsite power dictates the protection sequence, appropriate matrix entries are made in Column 96 (offsite AC power), but the single-failure criterion is not applied because, without offsite power, a lesser case of Event 28 results. For accidents, the protection sequences shown are those that assume the use only of the standby AC power system.

The conventions used on the protection sequence diagrams associated with each event are illustrated in Figure G.0-23. A separate protection sequence diagram is shown for each essential safety action requiring the operation of two or more systems.

G.5.3.5.1 Planned Operations

The requirements for the planned operations normally involve the use of limits on certain key process variables. Matrix 3 generally displays the process variable limits, associates the limits with the system for which the limit is essential, and shows the indications that are necessary for the plant operator to comply with the limits.

Event 1 - Refueling Outage

Refueling Outage operations include all planned operations pertaining to the nuclear core that are normally accomplished whenever the reactor vessel head is removed.

These operations are applicable to operating states A and B only. The essential safety actions for state A are as follows.

Safety Action	Reason Safety Action Required
Radioactive Material Release Control	To limit radioactive material release (10 CFR 20).
Core Power Level Control	To remain within the envelope of conditions considered by the plant safety analysis.

Safety Action	Reason Safety Action Required
Nuclear System Water Quality Control	To remain within the envelope of conditions considered by the plant safety analysis.
Core Reactivity Control	To remain within the envelope of conditions considered by the plant safety analysis.
Refueling Restrictions	To remain within the envelope of conditions considered by the plant safety analysis.
Stored Fuel Shielding, Cooling and Reactivity Control	To prevent excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.
Control Bay Environmental Control	To maintain control bay environment (temperature, humidity) within limits for personnel and equipment so that the plant is maintained within the envelope of conditions considered by plant safety analysis.

The limits that are associated with these safety actions are, in most cases, obvious. The power level control needed for this state refers to a minimum neutron source level. This minimum must exist prior to withdrawing control rods for a reactor startup. Possible refueling restriction sequences are indicated on Figure G.0-24. This figure shows that either the procedural restrictions or the refueling interlocks

can maintain core alteration conditions to within the envelope of conditions considered by the plant safety analysis.

State B considerations include those described for state A, but because the reactor is critical or subcritical by less than the reactivity worth of any one control rod, additional requirements must be observed. The additional safety actions for state B are as follows.

Safety Action	Reason Safety Action Required
Rod Worth Control	To assure that rod worth remains within the limits considered by the plant safety analysis.

As shown by Figure G.0-25, adequate rod worth control can be achieved either by operator control of rod position via the control rod position indications or by the action of the rod worth minimizer program of the process computer. In state B, power level control requires both a minimum and a maximum bound on core power level.

Event 2 - Achieving Criticality

Through the definition of achieving criticality, this operation is applicable to all operating states. States A, C, and E each consist of that part of "achieving criticality" in which the reactor is shut down (more than one rod subcritical). States B, D, and F each consist of that part of "achieving criticality" in which the reactor is not shut down. For states B, D, and F, the actual condition of criticality (k_{eff}=1) may or may not exist at any instant of time. For example, in operating state F, it is possible to be not shut down, yet still be in the latter stages of achieving criticality (k_{eff} <1). Note that the condition of shutdown for these analyses is a nuclear definition only.

Operating state F is the condition under which the nuclear system may be subject to its greatest loads. Because operating states A through E may be considered to be an approach to state F for this operation, the number of safety action requirements in state F is equal to or greater than the requirements in other states. The following listing relates the essential safety actions for this most demanding state (state F) with a justification for the action.

Safety Action	Reason Safety Action Required
Radioactive Material Release Control	To limit radioactive material release(10 CFR 20).
Core Power Level Control	To remain within the envelope of conditions considered by the plant safety analysis.
Reactor Vessel Pressure Control	To limit excessive pressure stresses and to remain within the envelope of conditions considered by the plant safety analysis.
Reactor Vessel Water Level Control	To prevent excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.
Nuclear System Temperature Control	To limit excessive thermal stresses on the nuclear system.
Nuclear System Water Quality Control	To remain within the envelope of conditions considered by the plant safety analysis.
Nuclear System Leakage Control	To limit crack propagation of the reactor vessel, to remain within the envelope of conditions considered by the plant safety analysis, and to limit radioactive material release (10 CFR 20).
Core Reactivity Control	To remain within the envelope of conditions considered by the plant safety analysis.
Rod Worth Control	To remain within the envelope of conditions considered by the plant safety analysis.
Primary Containment Pressure and Temperature Control	To remain within the envelope of conditions considered by the plant safety analysis.

Safety Action	Reason Safety Action Required

Control Bay Environmental Control	To maintain control bay environment (temperature, humidity) within limits for personnel and equipment so that the plant is maintained within the envelope of conditions considered by the plant safety analysis.
Stored Fuel Shielding, Cooling and Reactivity Control	To avoid excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.

To achieve these safety actions for this operation, it is essential that certain plant systems be operating or available to operate in state F. An example of a system requirement is the entry in block F2-46, which is "5." This entry means that the core power level indications must be operating to satisfy safety action 5, core power level control. This system requirement is self-explanatory in that the operator must have some indication of power level to control it. Similarly, to satisfy the essential safety action of rod worth control, the process computer and the control rod position indications share this function. That is, to have rod worth control, the operator must either have the process computer operating, or he must have some indication of control rod positions (see Figure G.0-25).

It is essential that limits be placed on certain parameters due to various systems (symbol "L" on Matrix 3). For example, limits are placed on pressure, water quality, and leakage due to reactor vessel design limitations (entries 8L, 10L, and 11L on matrix). Also, a limit exists on the power level due to fuel design limitations (entry 5L on matrix). Similar reasoning for safety action limits is made for the remaining systems. These limits are discussed in the section describing each individual system. A restriction (symbol "R" on Matrix 3) is placed on the operation of the recirculation system to avoid the thermal stresses on the reactor vessel which might otherwise arise from the cold-loop startup of a recirculation pump.

Event 3 - Heatup

Heatup, which begins where achieving criticality ends and includes all plant actions that are normally accomplished in approaching nuclear system rated conditions, begins in state D and continues into state F. The following list relates the essential safety actions with the needs for the actions, which are the same in states D and F.

Safety Action	Reason Safety Action Required
Core Neutron Flux Distribution Control	To remain within the envelope of conditions considered by the plant safety analysis.
Radioactive Material Release Control	To limit and indicate release of radioactive material.
Core Power Control	To operate only in conditions considered by the plant safety analysis.
Reactor Vessel Water Level Control	To limit and indicate fuel failure and operate only in conditions considered by the plant safety analysis.
Reactor Vessel Pressure Control	To limit and indicate fuel failure and operate only in conditions considered by the plant safety analysis and so indicate.
Nuclear System Temperature Control	To indicate and limit nuclear system process barrier stresses.
Nuclear Systems Water Quality Control	To operate only under conditions considered by the plant safety analysis.
Nuclear System Leakage Control	To indicate and limit nuclear system process barrier stresses, to operate only in conditions considered by the plant safety analysis and so indicate, and to limit and indicate release of radioactive material.
Core Reactivity Control	To operate so the reactor can be shut down with the control rods.
Rod Worth Control	To operate only in conditions considered by plant safety analysis and so indicate.
Primary Containment Pressure and Temperature Control	To remain within the envelope of conditions considered by the plant safety analysis.

Safety Action Reason Safety Action Required

Stored Fuel Shielding, Cooling and Reactivity Control	To avoid excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.
Control Bay Environmental Control	To maintain control bay environment (temperature, humidity) within limits for personnel and equipment so that the plant is maintained within the envelope of conditions considered by the plant safety analysis.

Most of the systems required to be operable to accomplish these safety actions are obvious. Limits (L) are placed on several process variables due to certain systems. For example, there is a limit on the core power level due to the fuel (5L in block F3-53).

For some systems requirements, two or more systems share the safety action responsibility. In particular, the safety action for core neutron flux distribution control is accomplished through operator observation of either the core flux distribution indications and the Neutron Monitoring System, which drives the indicators, or the control rod position indications. Also, the rod worth control safety action is accomplished through either automatic operation of the process computer or operator observation of the control rod position indications. (See Figure G.0-25.)

Event 4 - Power Operation

Operating state F is the only state in which the reactor can be under normal plant operation in excess of heatup power; therefore, states A, B, C, D, and E are not applicable to this event. The following listing relates the essential safety actions for this state with a justification for that action.

Safety Action	Reason Safety Action Required
Radioactive Material Release Control	To limit radioactive material release (10 CFR 20).
Core Power Level Control	To remain within the envelope of conditions considered by the plant safety analysis.

Safety Action	Reason Safety Action Required
Core Coolant Flow Rate Control	To avoid excessive fuel damage and to remain within the envelop of conditions considered by the plant safety analysis.

Control Bay Environmental Control	To maintain control bay environment (temperature, humidity) within limits for personnel and equipment so that the plant is maintained within the envelope of conditions considered by the plant safety analysis.
Core Neutron Flux Distribution Control	To remain within the envelope of conditions considered by the plant safety analysis.
Reactor Vessel Water Level Control	To prevent excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.
Reactor Vessel Pressure Control	To limit excessive pressure stresses and to remain within the envelope of conditions considered by the plant safety analysis.
Nuclear System Temperature Control	To limit excessive thermal stresses on the nuclear system.
Nuclear System Leakage Control	To limit radioactive material release (10 CFR 20), to remain within the envelope of conditions considered by the plant safety analysis, and to prevent crack propagation of the reactor vessel.
Nuclear System Water Quality Control	To remain within the envelope of conditions considered by the plant safety analysis.
Core Reactivity Control	To remain within the envelope of conditions considered by the plant safety analysis.

Safety Action	Reason Safety Action Required
Rod Worth Control	To remain within the envelope of conditions considered by the plant safety analysis.
Primary Containment Pressure and Temperature Control	To remain within the envelope of conditions considered by the plant safety analysis.

Stored Fuel Shielding, Cooling and Reactivity Control	To avoid excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.

To achieve certain of these safety actions for this operation, several plant systems are indicated in Matrix 3 as essential to safe operation. Of these actions, the core neutron flux distribution control (safety action 6) is accomplished by the reactor operator observing either the control rod position indications (system 52) or the core neutron flux distribution indications (system 47); these flux indications are driven by system 74, the Neutron Monitoring System. These systems are required to be continuously operating. Similarly, the control rod position indications (system 52) and the process computer (system 81) are shown to share rod worth control (action 13). Other system requirements are more obvious.

Certain parameters are limited due to an individual system. For example, there is a limit on pressure (pressure control, safety action 8) due to the reactor vessel. Similarly, there are limits on temperature and leakage due to the reactor vessel. The imposed limits are discussed in the section on each individual system.

A restriction (symbol "R" in Matrix 3) is placed on the operation of the recirculation system for this event to avoid the thermal stresses that may arise on the reactor vessel from the cold-loop startup of a recirculation pump.

Event 5 - Achieving Shutdown

The planned operation of achieving shutdown is applicable in states B, D, and F. In states A, C, and E, the reactor is in the shutdown condition by definition. The essential safety actions for achieving shutdown include the following.

Safety Action	Reason Safety Action Required
Radioactive Material Release Safety Action	To limit the release of radioactive material to the requirements of Reason Safety Action Required
Control	10 CFR 20 (includes indications essential to control such releases).
Core Coolant Flow Rate Control, Core Power Level Control, and Core Neutron Flux Distribution	To operate the plant only within the envelope of conditions considered by plant safety analysis employing those indications essential to maintain conditions within those limits.

Control

Control Bay Environmental Control	To maintain control bay environment (temperature, humidity) within limits for personnel and equipment so that the plant is maintained within the envelope of conditions considered by the plant safety analysis.
Reactor Vessel Water Level Control	To limit fuel failure to fission product release rates within the limits of 10 CFR 20, and to operate the plant only within the envelope of conditions considered by the plant safety analysis, including essential indications.
Reactor Vessel Pressure Control	To prevent stresses to the nuclear system process barrier in excess of that allowed by design for planned operation, including indications essential for control, and to limit plant operation to conditions considered by the plant safety analysis, including essential indications.
Nuclear System Temperature Control	To limit stresses to the nuclear system process barrier to that allowed by design for planned operation, including indications essential for control.
Nuclear System Water Quality Control	To remain within the envelope of conditions considered by the plant safety analysis.
<u>Safety Action</u>	<u>Reason Safety Action Required</u>
Nuclear System Leakage Control	To prevent stresses to the nuclear system process barrier from exceeding that allowed by design, to limit plant operation conditions to those considered by the plant safety analysis, and to restrict the release of radioactive material to limits designated by 10 CFR 20. These requirements shall include indications essential to their control.
Core Reactivity Control	To remain within the envelope of conditions within which the reactor can be shut down with control rods.

Rod Worth Control	To limit plant operation to conditions considered by the plant safety analysis, including essential indications.
Primary Containment Pressure and Temperature Control	To limit plant operation to conditions considered by the plant safety analysis, including essential indications.
Stored Fuel Shielding, Cooling and Reactivity Control	To avoid excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.

The above safety actions are required for operation in state F. In operating state D, the vessel pressure is less than 850 psig, resulting in minor modifications in safety actions and system requirements. In operating state B, vessel head is removed. In this state, there is no requirement for reactor vessel pressure control or core neutron flux distribution control.

In states F and D, shared (S) functions are noted in several instances. The core neutron flux distribution indications share with the control rod position indications the function of controlling through operator observation the core neutron flux distributions to avoid unacceptable result 1-4. This requires that essential indications be utilized to assure that operation remains within the envelope of conditions considered by the plant safety analysis. (See F-5-47, F-5-52, and F-5-74 entries.) Similarly, control rod position indications and the process computer share (S) the function of rod worth control to assure operation within the envelope of the plant safety analysis.

Event 6 - Cooldown

Since cooldown begins where achieving shutdown ends; by definition, cooldown is applicable in states A, C, and E, in which the reactor has achieved shutdown. The essential safety actions for cooldown include the following.

Safety Action	Reason Safety Action Required
Radioactive Material Release Control	To limit the release of radioactive material to 10 CFR 20 requirements (includes essential indications).
Reactor Vessel Water Level	To limit fuel failure to that which results in fission product release rates within 10 CFR 20 limits, and

Control	to limit plant operation to conditions considered by the plant safety analysis, including essential indications.
Reactor Vessel Pressure Control	To limit stresses to the nuclear system process barrier in excess of design allowances for planned operation, including essential indications, and to limit plant operation to conditions considered by the plant safety analysis, including essential indications.
Nuclear System Temperature Control	To limit stresses to the nuclear system process barrier in excess of design allowances for planned operation, including essential indications.
Nuclear System Water Quality Control	To remain within the envelope of conditions considered by the plant safety analysis.
Nuclear System Leakage Control	To limit stresses to the nuclear system process barrier in excess of design allowances for planned operation, to limit plant operation to the envelope of conditions considered by the plant safety analysis, and to restrict the release of radioactive material to the limits designated by 10 CFR 20. These requirements include indications essential to their control.

Safety Action	Reason Safety Action Required
Primary Containment Pressure and Temperature Control	To remain within the envelope of conditions considered by the plant safety analysis.
Stored Fuel Shielding, Cooling and Reactivity Control	To avoid excessive fuel damage and to remain within the envelope of conditions considered by the plant safety analysis.
Control Bay Environment Control	To maintain control bay environment (temperature, humidity) within limits for personnel and equipment so that the plant is maintained within the envelope of conditions considered by the plant safety analysis.

The requirements for limits and parameter indications for the safety actions essential to this planned operation are essentially identical to the requirements for these same safety actions for other planned operations, except that there is a unique temperature limit on rate-of-change during cooldown. This is indicated as a limit for temperature control on the reactor vessel and a requirement for temperature indications.

Events 7-11 - (Numbers Not Used)

G.5.3.5.2 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. Upon transferring the information in the sequence diagrams to Matrix 3, the auxiliaries for the front-line safety systems are accounted for on the matrix.

Events 12 and 13 - Generator Trip and Turbine Trip

Generator trip and turbine trip (with bypass) are similar, abnormal operational transients. The required safety actions and the systems required to fulfill the safety actions are the same for both transients. The state D turbine trip is an insignificant event due to the low initial power level.

Two safety actions are required to satisfy the nuclear safety operational criteria. Scram is required to prevent excessive fuel damage and to prevent overpressurization of the nuclear system. Pressure relief is required to prevent overpressurization of the nuclear system.

Figures G.0-26 and G.0-27 illustrate the different protection sequences pertinent to producing the scram and pressure-relief safety actions. Scram is accomplished through operation of the Reactor Protection System and the Control Rod Drive System. Pressure relief is accomplished through operation of the Nuclear System Pressure Relief System. As Figures G.0-26 and G.0-27 indicate, all of the systems involved with scram and pressure relief must individually meet the single-failure criterion.

Event 14 - Isolation of All Main Steam Lines

Isolation of all main steam lines is most severe and rapid in operating state F during power operation. In other states, steam line isolation becomes a lesser case of the state F sequence. The following listing relates the essential safety actions for the worst case with the needs for the actions.

Safety Action	Reason Safety Action Required
Scram	To prevent excessive fuel damage and to limit nuclear system pressure rise.
Pressure Relief	To prevent excessive nuclear system pressure rise.
Core Cooling	To prevent excessive fuel damage after the reactor vessel is isolated. Feedwater flow (normal cooling) is assumed lost.

As shown in Figure G.0-28a, scram is accomplished through the actions of the Reactor Protection System and the Control Rod Drive System. The Nuclear System Pressure Relief System provides pressure relief.

After the reactor is isolated and feedwater flow has been lost, decay heat may cause an increase in nuclear system pressure, eventually lifting main steam relief valves and allowing reactor vessel water level to decrease. The core cooling sequence shown in Figure G.0-28b shows both the short-term and long-term sequences necessary to achieve adequate cooling in spite of any single failure. This same sequence could be used in any situation in which the main heat sink and normal feedwater flow are lost. In this sequence, either the RCICS or HPCIS maintain water level in the reactor vessel as steam is relieved via the main steam relief valves to the torus. The RHRS torus cooling mode can be used to remove the heat received by the torus water. When the torus water temperature reaches 120°F, a controlled depressurization (100°F/hr) must be started by operating the main steam relief valves through remote manual control (considered part of the Automatic Depressurization System). Starting the depressurization when the torus water

reaches 120°F assures that the torus water retains its capability to suppress a full blowdown of the nuclear system within the bounds of the experimental data observed in actual pressure suppression tests. Depending upon nuclear system pressure, the RCICS, HPCIS, LPCI, or Core Spray Systems can be used to maintain reactor vessel water level until the shutdown cooling system can be placed into operation (planned operation).

Event 15 - Isolation of One Main Steam Line

The only condition under which isolation of one main steam line causes a significant transient is in state F during high power operation. Scram is the only unique action required in response to the event to avoid excessive fuel damage and nuclear system overpressurization. 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.0-29, the scram safety action is accomplished through the combined actions of the Neutron Monitoring System, Reactor Protection System, and Control Rod Drive System.

Event 16 - Loss of Condenser Vacuum

A loss of vacuum in the turbine-generator condenser can occur at any time steam pressure is available and is therefore applicable to operating states C, D, E, and F. This nuclear system pressure increase transient is the most severe of the pressure increase transients and is similar in analysis to the Event 14, "Isolation of All Main Steam Lines." However, as this transient becomes a lesser case in the operating states in which the reactor is more than one control rod subcritical, there is no need for scram protection in states C and E.

In operating state D, at more than 1055 psig, and in state F, scram is initiated to prevent excessive fuel damage and is accomplished with the actions of the Reactor Protection System and Control Rod Drive System. Figure G.0-30a shows the sequence. As shown in Figure G.0-30b, in operating states C, D, E, and F, the following additional actions are required. The Nuclear System Pressure Relief System provides pressure relief. After the reactor is isolated and feedwater flow has been lost, decay heat may cause an increase in nuclear system pressure, eventually lifting main steam relief valves and allowing reactor vessel water level to decrease. The core cooling sequence in this case is shown in Figure G.0-30b.

Event 17 - (Number Not Used)

Event 18 - Loss of Feedwater Heating

Significant feedwater heating occurs only in operating state F.

A loss of feedwater heating causes such a mild transient that no protective actions are required to accommodate the event when the reactor is on automatic recirculation flow control. If the reactor is on manual flow control, however, the neutron flux increase associated with this event will reach the scram setting. As shown in Figure G.0-31, the scram safety action is accomplished through the combined actions of the Neutron Monitoring System, Reactor Protection System, and Control Rod Drive System.

Event 19 - Shutdown Cooling (RHRS) Malfunction (Temperature Decrease)

No unique safety actions are required to avoid the unacceptable safety results for transients as a result of a reactor coolant temperature decrease induced by misoperation of the shutdown cooling heat exchangers. In states B and D, where the reactor is critical or near critical, the very slow power increase resulting from the moderator temperature decrease would be controlled by the operator in the same manner as is normally used to control power in the source or intermediate power ranges.

Event 20 - Inadvertent Pump Start (Temperature Decrease)

An inadvertent pump start (temperature decrease) is defined as an unintentional start of any nuclear system pump which adds sufficient cold water to the reactor coolant inventory to cause a measurable moderator temperature decrease.

While all the safety criteria apply, there are no unique safety actions required to control the adverse effects of such a pump start; that is, pressure increase and temperature decrease in states A, C, and E. In these operating states, the safety criteria are met through the basic design of the plant systems, and no safety action is specified. In states B, D, and F, where the reactor is not shut down, the plant operator can control any power changes by the normal manner for controlling power.

Event 21 - Control Rod Withdrawal Error

No unique safety actions are required in operating states A, C, and E because the core is more than one rod subcritical and could not achieve criticality with the full withdrawal of any one control rod.

During high power operation (state F), an uninhibited, erroneous rod withdrawal does not result in fuel damage since the rod block monitor stops the rod withdrawal. However, during plant operation in the intermediate range (achieving criticality, heatup, achieving shutdown, states B, D, and F), a high flux scram is required to terminate the increase in power level. As shown by Figure G.0-32, the required

scram is accomplished by the Neutron Monitoring, Reactor Protection, and Control Rod Drive Systems.

Events 22 and 23 - Fuel Assembly Insertion and Control Rod Removal

An inadvertent positive reactivity insertion can result from the erroneous physical operations pertaining to fuel assembly insertion, or control rod removal, and is possible only when the reactor vessel head is removed.

Because during core alterations the mode switch is in the REFUEL position, which allows the refueling equipment to be positioned over the core and also inhibits control rod withdrawal, this transient is applicable to operating state A only. No unique safety actions are required because the total worth (positive reactivity) of either one fuel assembly or one control rod is inadequate to cause a criticality.

In addition, the mechanical designs of the control rod assembly physically prevent its removal without the simultaneous or prior removal of the adjacent fuel assemblies.

Event 24 - (Number Not Used)

Event 25 - Pressure Regulator Failure

A pressure regulator failure is most severe and rapid in operating state F during power operation. In state E, pressure regulator failure becomes a milder case of the state F sequence. In states C and D, this transient is even less severe, because reactor vessel pressure is at less than 825 psia initially.

The following listing relates the essential safety actions for the worst case with a justification for the actions.

Safety Action	Reason Safety Action Required
Scram	To prevent excessive fuel damage and to limit nuclear system pressure rise following reactor vessel isolation.
Pressure Relief	To prevent excessive nuclear system pressure rise following reactor vessel isolation.

Safety Action	Reason Safety Action Required
Core Cooling	To prevent excessive fuel damage after the reactor vessel is isolated and feedwater flow (normal cooling) has been lost.

Reactor Vessel Isolation	To prevent damage to the fuel barrier by limiting the loss of reactor coolant.

The various protection sequences giving the safety actions are shown in Figure G.0-33. Depending on the plant conditions existing prior to the event, scram will be either on high flux (IRM range) or on main steam line isolation. The sequence resulting in reactor vessel isolation is also dependent upon initial conditions. In state F 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. Core cooling following isolation can be provided by either the RCICS or HPCIS.

Event 26 - Inadvertent Opening of a Main Steam Relief Valve

An inadvertent opening of a main steam relief valve is assumed in any state. In states A and B, the water level cannot be lowered so far as to threaten any fuel damage; therefore, no safety actions are required in states A and B. If the event occurs when the feedwater system and main condenser are in operation, the plant continues to operate in the normal manner, the feedwater system providing the additional water to maintain reactor vessel water level. The only situation requiring unique safety actions is when the event occurs at a time when the nuclear system is pressurized but the feedwater system is not in operation. The opening of a main steam relief valve in this case results in a reactor vessel low water level. The following safety actions are needed for this situation.

Safety Action	Reason Safety Action Required
Scram	To prevent excessive fuel damage.
Core Cooling	To prevent excessive fuel damage.

Reactor vessel isolation is not required because the vessel is already isolated in the situation under which any safety action is required.

The protection sequences for scram and core cooling are shown in Figure G.0-34. Reactor vessel low water level initiates both the scram and core cooling safety actions.

Event 27 - 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 may occur in states C, D, E, and F. The proper responses to this transient include a reactor scram on low water level and maintenance of reactor vessel water level. The following listing relates the essential safety actions for state F, with the need for the actions.

Safety Action	Reason Safety Action Required
Scram	To prevent excessive fuel damage.
Pressure Relief	To prevent excessive nuclear system pressure rise after the reactor vessel has been isolated.
Core Cooling	To prevent excessive fuel damage after the reactor vessel is isolated and feedwater flow (normal cooling) lost.
Reactor Vessel Isolation	To prevent damage to the fuel barrier by limiting the loss of reactor coolant.

As shown in Figures G.0-35a and b, the Reactor Protection System and Control Rod Drive System effect a scram on low water level. The 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 main steam relief valve setting. Pressure relief is accomplished by the Nuclear System Pressure Relief System. Core cooling is necessary to restore and maintain water level. Either the HPCIS or the RCICS can maintain adequate water level; as a pair, the HPCIS and RCICS satisfy the single-failure criterion for core cooling.

The requirements for operating state D are the same as for state F. The requirements for operating states C and E are the same as for states D and F, except that the scram action is not required.

Event 28 - Total Loss of Offsite Power

This is a variety of combinations of possible offsite power losses and initial plant conditions. Figures G.0-36a, b, c, d, and e show the various electrical sequences considered by this analysis. The sequences are selected by applying the abnormal operational transient selection criteria given in Subsection 14.4. Depending upon the specific case under consideration, the following safety actions are required.

Safety Action	Reason Safety Action Required
Scram	To prevent excessive fuel damage and to limit nuclear system pressure rise.
Pressure Relief	To prevent excessive nuclear system pressure rise after the reactor vessel has been isolated.

Core Cooling	To prevent excessive fuel damage after the feedwater flow (normal cooling) has been lost.
Restore AC Power	To prevent excessive fuel damage by providing AC power for various systems required for other safety actions.

The protection sequences shown in Figures G.0-36a, b, c, d, and e, encompass all of the sequences ever required to accommodate the event under any initial condition. For core cooling in states A and B, only the lower portion of the sequence shown in Figure G.0-36e is required.

Event 29 - Recirculation Flow Control Failure (Decreasing Flow)

This recirculation flow control malfunction causes a decrease in core coolant flow. Such a decrease can be accommodated within the operational nuclear safety criteria without the action of any protection systems. Thus, no unique operational nuclear safety requirements arise from this event. This event is not applicable to states A and B, because the reactor vessel head is off and the recirculation pumps would normally not be in use. The trip could occur in states C through F; however, the absence of matrix entries signifies the reactor's ability to accommodate the transient with no unique safety action requirement.

Event 30 - Trip of One Recirculation Pump

The trip of one recirculation pump produces a milder transient than the simultaneous trip of two recirculation pumps (see Event 31). No unique safety actions are required in response to this transient. This event is not applicable to states A and B, because the reactor vessel head is off and the recirculation pumps would normally not be in use. The trip could occur in states C through F; however, the absence of matrix entries signifies the reactor's ability to accommodate the transient with no unique safety action requirement.

Event 31 - Trip of Two Recirculation Pumps

The transient resulting from this two-loop trip is not severe enough to require any unique safety action in response to the event. The transient is compensated for by the inherent stability of the reactor. However, a manual scram may be required if evidence of thermal-hydraulic instability is observed. This event is not applicable to states A and B, because the reactor vessel head is off and the recirculation pumps would normally not be in use. The trip could occur in states C through F, however, the absence of matrix entries signifies the reactor's ability to accommodate the transient with no unique safety action requirement.

Event 32 - Recirculation Pump Seizure*

A recirculation pump seizure considers the instantaneous stoppage of the pump motor shaft of one recirculation pump. The case involving operation at design power in state F is described in Subsection 14.5. While all the safety criteria apply, there are no required safety actions to control the adverse effects of recirculation pump seizure. MCPR is maintained above 1.0 and no damage occurs to the fuel barrier. No scram is required, and no unique safety action is necessary to control temperature and pressure. The safety criteria are met through the basic design of the plant systems. This event is not applicable to states A and B, because the reactor vessel head is off and the recirculation pumps would normally not be in use. The trip could occur in states C through F, however, the absence of matrix entries signifies the reactor's ability to accommodate the transient with no unique safety action requirement. *(This event has been reclassified as an accident see NEDE-24011-P-A-US.)

Event 33 - Recirculation Flow Control Failure (Increasing Flow)

A recirculation flow control failure causing increased flow is applicable in states C, D, E, and F. In state F, the accompanying increase in power level is accommodated through a reactor scram. As shown in Figure G.0-37, the scram safety action is accomplished through the combined actions of the Neutron Monitoring System, Reactor Protection System, and Control Rod Drive System.

Event 34 - Startup of Idle Recirculation Pump

The cold-loop startup of an idle recirculation pump is most severe and rapid for those operating states in which the reactor may be critical (states B, D, and F). When the transient occurs in the range of 10 to 60 percent power operation, no safety actions are required in response to the event. Reactor power in this case would be limited to approximately 60 percent design power due to core flow limitations, while using one working recirculation loop. Above 60 percent power, a high neutron flux scram is initiated. Should the event occur when the reactor is not at power operation, but critical (<10 percent), the resulting transient may produce a high level neutron flux scram of the intermediate range monitors (IRM).

As shown in Figure G.0-38, the scram action is accomplished through the combined actions of the Neutron Monitoring System, Reactor Protection System, and Control Rod Drive System. At power operation (10-60 percent), the high level IRM scram is not initiated because the core flux monitoring has been shifted to the average power range monitors (APRM).

Event 35 - 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. At this time, the RHR system is operating in the shutdown cooling mode, which occurs only in states A, B, C, and D.

As shown in Figure G.0-39, 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 reestablished 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, either half of the RHRS-LPCI mode can be used to maintain water level. In states C and D, in which the reactor vessel head is on and the system can be pressurized, the low-pressure cooling system, main steam relief valves (manually operated), and RHRS-torus cooling mode can be used to maintain water level and remove decay heat.

Event 36 - Feedwater Controller Failure (Maximum Demand)

A feedwater controller failure (maximum demand) leads to an excess of coolant inventory in states C, D, E, and F. The following listing relates the essential safety actions with the need for the actions.

Safety Action		Reason Safety Action Required
Scram	°	To prevent excessive fuel damage and to limit nuclear system pressure rise.
Pressure Relief		To prevent excessive nuclear system pressure rise.

In operating state F, any adverse responses of the reactor due to cooling of the moderator can be accomplished by a scram. As shown in Figure G.0-40, the scram safety action is accomplished through the combined actions of the Neutron Monitoring System, Reactor Protection System, and the Control Rod Drive System. Pressure relief is required in states C, D, E, and F and is achieved through the operation of the Nuclear System Pressure Relief System.

G.5.3.5.3 Accidents

Event 37 - (Number Not Used)

Event 38 - Control Rod Drop Accident

The control rod drop accident is the result of an assumed failure of the rod-to-drive coupling after the rod becomes stuck in its fully-inserted position. The assumption is made that the control rod drive is fully withdrawn before the stuck rod falls out of the

core at a maximum velocity (determined by experimental data to be 3.11 ft/sec). The control rod velocity limiter, an engineered safeguard, limits the rod drop velocity to less than this value. The resultant radioactive material release is maintained below the requirements of 10 CFR 100. This accident is analyzed in Subsection 14.6.

Although the control rod drop accident is applicable in all operating states except states A and B, where special precautions are taken to ensure coupling integrity, no safety action is required in states C and E, where the plant is shut down by more than one rod prior to the accident. In states D and F, where fission product release may occur, the essential safety actions required include the following.

Safety Action	Reason Safety Action Required
Scram	To limit radiological effects to the guideline values of 10 CFR 100, and to limit peak fuel enthalpy.
Reactor Vessel Isolation	To limit radiological effects to the guideline values of 10 CFR 100.

Safety Action	Reason Safety Action Required
Establish Primary Containment	To limit radiological effects to the guideline values of 10 CFR 100.
Establish Secondary Containment	To limit radiological effects to the values of 10 CFR 100.
Core Cooling	To prevent fuel cladding temperatures in excess of 2200°F.
Containment Cooling	To limit containment stresses to acceptable values.
Limit Reactivity Insertion Rate	To prevent peak fuel enthalpy in excess of 280 cal/g and excessive nuclear system stresses.
Pressure Relief	To limit nuclear system pressure to that allowed for accidents by applicable industry codes.
Control Bay Environmental Control	To limit the radiation dose received by operations personnel who must remain in the control room to control the plant after accident.

Figures G.0-41a, b, and c show the different protection sequences for the control rod drop accident. These Figures show the safety actions required for operating states D and F.

Event 39 - Pipe Break Inside Primary Containment

Pipe breaks inside the primary containment are considered only when the nuclear system is significantly pressurized and result in the release of steam and/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 (DBA) for the loss of coolant from a pipe break inside the primary containment.

As shown in Figures G.0-42a and b, in operating states C and E (reactor shut down, but pressurized), a pipe break accident up to the DBA can be accommodated within the operational nuclear safety criteria through the various operations of the Main Steam Line Isolation Valves, Core Standby Cooling Systems (HPCIS, Automatic Depressurization System, LPCI and Core Spray System), Primary Containment and Reactor Vessel Isolation Control System, Primary Containment, Secondary Containment, Standby Gas Treatment System, Control Room Isolation System and the Incident Detection Circuitry. In operating states D and F (reactor not shut down, but pressurized), the same equipment is required as in states C and E; but, in addition, the Reactor Protection System and the Control Rod Drive System must operate to scram the reactor. The limiting items, upon which the operation of the above equipment is based, are the allowable fuel temperature and the primary containment pressure capability.

The control rod drive 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).

After completion of the automatic actions of the above equipment, manual operation of the RHRS (torus cooling mode) is required to maintain primary containment pressure and fuel temperature within limits during long-term cooldown following the accident.

Event 40 - Fuel Handling Accident

This unlikely accident, described in Subsection 14.6 as the drop of one fuel assembly from the refueling equipment during fuel handling operation, is possible in any state whenever fuel handling operations are in progress.

Because in state A the mode switch is in the REFUEL position, which allows the refueling equipment to be positioned over the core and also inhibits control rod withdrawal, the design basis accident is applicable to operating state A only.

Accident considerations include mechanical fuel damage due to impact and a subsequent release of fission products.

The following safety actions are required for response to the fuel handling accident.

Safety Action	Reason Safety Action Required
Establish Secondary Containment	To limit the radiological effects to the guideline values of 10 CFR 100.
Control Bay Environmental Control System	To prevent excessive radiation dose to operations personnel in the control room.

The protection sequences pertinent to this accident are shown in Figure G.0-43.

Event 41 - 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, D, E, and F). This accident is most severe when operating at high power (state F). In the other states (C, D, and E), this accident becomes a lesser case of the state F sequence. The following list relates the essential safety actions for the worst case, with the needs for the actions.

Safety Action	Reason Safety Action Required
Scram	To prevent fuel clad temperature in excess of 2200°F.
Reactor Vessel Isolation	To limit radiological effect so as not to exceed the guideline values of 10 CFR 100.
Core Cooling	To prevent fuel cladding temperatures in excess of 2200°F.
Restrict Loss of Reactor Coolant (passive)	To prevent fuel cladding temperatures in excess of 2200°F.
Pressure Relief	To limit nuclear system stresses so as not to exceed stresses allowed for accidents by applicable industry codes.
Control Bay Environ-	To prevent overexposure to radiation

mental Control of control room personnel.

The protection sequences for the various possible pipe breaks outside the primary containment are shown in Figures G.0-44a, b, and c. As shown in Figures G.0-44a and b, special consideration must be given to the HPCIS steam line breaks, because this system is otherwise used in response to the other pipe break accidents. The sequences 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.0-44b).

Scram is accomplished through operation of the Reactor Protection System and the Control Rod Drive System. Reactor vessel isolation is accomplished through operation of the main steam line isolation valves and the Primary Containment and Reactor Vessel Isolation Control System.

Core cooling is accomplished by the HPCIS or manual blowdown for a break in a main steam line. For the break of a HPCIS steam line (smaller steam line break accident) manual initiation of the Automatic Depressurization System is required after some time has elapsed. After the vessel has depressurized, core cooling is accomplished by either the Core Spray System or the LPCI mode of the RHRS in combination with RHRS torus cooling. Operation of the incident detection circuitry is required for operation of the HPCI, LPCI, and Core Spray Systems. Restricting the loss of reactor coolant for the main steam line break is accomplished by the flow restrictors. Pressure relief is accomplished through the action of the Nuclear System Pressure Relief System.

As shown on Figure G.0-44a, the most restrictive cooling requirements demand that the HPCIS and manual blowdown satisfy the single-failure criterion as a pair. The Core Spray System and the LPCIS are also required to satisfy the single-failure criterion as a pair.

Events 42 and 43 - (Numbers Not Used)

G.5.3.5.4 Special Event 44 - Loss of Habitability of the Control Room

This event is displayed to demonstrate the ability to safely shut down the reactor and subsequently to cool the reactor to the cold shutdown state, accomplished entirely from outside the control room.

Figure G.0-45 shows the protection sequences for this event in each operating state. In state A, no sequence is shown, because the reactor is already in the condition finally required for the event.

A scram from outside the control room can be achieved by opening the AC supply breakers for the Reactor Protection System. If the nuclear system becomes isolated

from the turbine, decay heat is transferred from the reactor to the torus water via the main steam relief valves. The RCICS is used to maintain reactor vessel water level, and the RHRS torus cooling mode is used to remove the decay heat from the torus water. When reactor pressure falls to 100 psig, the RHRS shutdown cooling mode is started.

G.5.3.5.5 Special Event 45 - Inability to Shut Down Reactor with Control Rods

The inability to shut down the reactor with control rods is a special event devised to evaluate the Standby Liquid Control System. By definition, this event can occur only when the reactor is not already shut down. Therefore, this event is considered only in operating states B, D, and F. Only the Standby Liquid Control System must operate to avoid unacceptable result 5-1. The design basis for the Standby Liquid Control System results from these operating criteria when applied under the most severe conditions (operating state F at rated power). As indicated on Figure G.0-46 and the matrices for states B, D, and F, the Standby Liquid Control System is manually initiated and controlled.

G.5.4 Remainder of the Nuclear Safety Operational Analysis

With the information presented in the protection sequence block diagrams and in Matrix 3, it is possible to determine on a system-by-system basis the functional and hardware requirements for each system.

G.6 CONCLUSION

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.