15A Plant Nuclear Safety Operational Analysis (NSOA)

15A.1 Objectives

The objectives of the Nuclear Safety Operational Analysis (NSOA) are cited below.

15A.1.1 Essential Protective Sequences

Identify and demonstrate that essential protection sequences needed to accommodate the plant normal operations, moderate frequency incidents (anticipated operational transients), infrequent incidents (abnormal operational transients), and limiting faults (design basis accidents) are available and adequate. In addition, each event considered in the plant safety analysis (Chapter 15) is further examined and analyzed. Specific essential protective sequences are identified. The appropriate sequence is discussed for all ABWR operating modes.

15A.1.2 Design Basis Adequacy

Identify and demonstrate that the safety design basis of the various structures, systems or components needed to satisfy the plant essential protection sequences are appropriate, available and adequate. Each protective sequence identifies the specific structures, systems or components performing safety or power generation functions. The interrelationships between primary and secondary (or auxiliary equipment) systems in providing these functions are shown. The individual design bases (identified throughout Tier 2 for each structure, system, or component) are brought together by the analysis in this section. In addition to the individual equipment design basis analysis, the plant-wide design bases are examined and presented here.

15A.1.3 System-Level/Qualitative—Type FMEA

Identify a system-level/qualitative-type Failure Modes and Effects Analysis (FMEA) of essential protective sequences to show compliance with the Single Active Component Failure (SACF)or Single Operator Error (SOE) criteria. Each protective sequence entry is evaluated relative to SACF or SOE criteria. Safety classification aspects and interrelationships between systems are also considered.

15A.1.4 NSOA Criteria Relative to Plant Safety Analysis

Identify the systems, equipment, or components' operational conditions and requirements essential to satisfy the nuclear safety operational criteria utilized in the Chapter 15 plant events.

15A.1.5 Technical Specification Operational Basis

Will establish limiting operating conditions, testing and surveillance bases relative to plant Technical Specifications.

15A.2 Approach to Operational Nuclear Safety

15A.2.1 General Philosophy

The specified measures of safety used in this analysis are referred to as "unacceptable consequences." They are analytically determinable limits on the consequences of different classifications of plant events. The NSOA is thus an "event-consequence" oriented evaluation. Refer to Figure 15A-1 for a description of the systematic process by which these unacceptable results are converted into safety requirements.

15A.2.2 Specific Philosophy

The following guidelines are utilized to develop the NSOA.

(1) Scope and Classification of Plant Events

(a) Normal (Planned)Operations

Normal Operations are planned conditions in the absence of significant abnormalities. Operations subsequent to an incident (transient, accident or special event) are not considered planned operations until the procedures being followed or equipment being used are identical to those used during any one of the defined planned operations. Specific events are presented in Table 15A-8.

(b) Moderate Frequency Incidents (Anticipated (Expected) Operational Transients)

Moderate Frequency Incidents are deviations from normal conditions which are expected to occur at a moderate frequency, and, as such, the design includes the capability to withstand the conditions without operational impairment. Included are incidents that result from a single operator error, control malfunction and others as presented in Table 15A-9.

(c) Infrequent Incidents (Abnormal (Unexpected) Operational Transients)

Infrequent Incidents are infrequent deviations from normal conditions. The design includes a capability to withstand these conditions without operational impairment. Table 15A-10 presents the events included within this classification.

(d) Limiting Faults (Design Basis (Postulated) Accidents)

Limiting Faults are hypothesized accidents the characteristics and consequences of which are utilized in the design of those systems and components pertinent to the preservation of radioactive material barriers and the restriction of radioactive material release from the barriers. The potential radiation exposures resulting from Limiting Faults may be greater than for any

similar accident postulated from the same general accident assumptions. Specific events are presented in Table 15A-11.

(e) Special (Hypothetical) Events

Special Events are postulated to demonstrate some special capability of the plant in accordance with NRC requirements. For analyzed events within this classification, see Table 15A-12.

(2) Safety and Power Generation Aspects

Matters identified with “safety” classification are governed by regulatory requirements. Safety functions include:

(a) The accommodation of moderate frequency incidents, infrequent incidents and limiting faults

(b) The maintenance of containment integrity

(c) The assurance of ECCS

(d) The continuance of reactor coolant pressure boundary (RCPB) integrity

Safety classified aspects are related to 10CFR100 dose limits, infrequent and low probability occurrences, SACF criteria, worst-case operating conditions and initials assumptions, automatic (30-min.) corrective actions, significant unacceptable dose and environmental effects, and the involvement of other coincident (mechanistic or non-mechanistic) plant and environmental situations.

Power generation classified considerations are related to continued plant power generation operation, equipment operational matters, component availability aspects and to long-term offsite public effects.

Some matters identified with “power generation” classification are also covered by regulatory guidelines. Power generation functions include:

(a) Accommodation of planned operations and moderate frequency incidents

(b) Minimization of radiological releases to appropriate levels

(c) Assurance of safe and orderly reactor shutdown, and/or return to power generation operations

(d) Continuance of plant equipment design conditions to ensure long-term reliable operation

Power generation is related to 10CFR20 and 10CFR50 Appendix I dose limits.

(3) Frequency of Events

Consideration of the frequency of the initial (or initiating) event is straightforward. Added considerations (e.g., further failures or operator errors) certainly influence the classification grouping. The events in this appendix are initially grouped per initiating frequency occurrence. The imposition of further failures necessitates further classification to a lower frequency category.

The introduction of SACF or SOE into the examination of planned operation, moderate frequency incidents or infrequent incidents evaluations has not been previously considered a design basis or evaluation prerequisite. It is provided and included here to demonstrate the plant's capability to accommodate the requirement.

(4) Conservative Analysis—Margins

The unacceptable consequences established in this appendix relative to the public health and safety are, in themselves, in strict and conservative conformance to regulatory requirements.

(5) Safety Function Definition

First, the essential protective sequences shown for an event in this appendix list the minimum structures and systems required to be available to satisfy the SACF or SOE evaluation aspects of the event. Other protective “success paths” exist in some cases than are shown with the event.

Second, not all the events involve the same natural, environmental or plant conditional assumptions. For example, loss-of-coolant accident (LOCA) and safe shutdown earthquake (SSE) mechanical loads are associated with Event 32. In Event 29, the control rod drop accident (CRDA) is not assumed to be associated with any SSE or operating basis earthquake (OBE) occurrence. Therefore, seismic safety function requirements are not considered for Event 29. Some of the safety function equipment associated with the Event 29 protective sequence is also capable of handling more limiting events, such as Event 32.

Third, containment may have a safety function for some event when uncontained radiological release would be unacceptable, but for other events it may not be applicable (e.g., during refueling). The requirement to maintain the containment in post-accident recovery is only needed to limit doses to less than 10CRF100. After radiological sources are depleted with time, further containment is unnecessary. Thus, the “time domain” and “need for” aspects of a function are taken into account and considered when evaluating the events in this appendix.

Fourth, the operation of engineered safety features (ESF) equipment, for normal operational events, should not be misunderstood to mean that ESF equipment requirements apply to this event category.

Likewise, the interpretation of the use of ESF-SACF capable systems for moderate frequency incidents protective sequences should not imply that these equipment requirements (seismic, redundancy, diversity, testable, IEEE, etc.) are required for moderate frequency incidents.

(6) Envelope and Actual Event Analysis

The event analysis presented in Chapter 15 does not include event frequency considerations, but does present an "envelope analysis" evaluation based on expected situations. Studies of the actual plant occurrences, their frequency and their actual impact are reflected in their categorization in this appendix. This places the plant safety evaluations and their impact into a better perspective by focusing attention on the "envelope analysis" with more appropriate understanding.

15A.2.2.1 Consistency of the Analysis

Figure 15A-2 illustrates three inconsistencies. Panel A shows the possible inconsistency resulting from operational requirements being placed on separate levels of protection for one event. If the second and sixth levels of protection are important enough to warrant operational requirements, then so are the third, fourth and fifth levels. Panel B shows the possible inconsistency resulting from operational requirements being arbitrarily placed on some action thought to be important to safety. In the case shown, scram represents different protection levels for two similar events in one category: if the fourth level of protection for Event B is important enough to warrant an operational requirement, then so is the fourth level for Event A. Thus, to simply place operational requirements on all equipment needed for some action (scram, isolation, etc.) could be inconsistent and unreasonable if different protection levels are represented. Panel C shows the possible inconsistency resulting from operational requirements being placed on some arbitrary level of protection for any and all postulated events. Here the inconsistency is not recognizing and accounting for different event categories based on cause or expected frequency of occurrence.

Inconsistencies of the types illustrated in Figure 15A-2 are avoided in the NSOA by directing the analysis to "event consequences" oriented aspects. Analytical inconsistencies are avoided by (1) treating all the events of a category under the same set of functional rules, (2) applying another set of functional rules to another category, and (3) having a consistent set of rules between categories. Thus, it is valid to compare the results of the analyses of the events in any one category and invalid to compare events of different categories, and thus different rules, to the other category. An example of this is the different rules (limits, assumptions, etc.) of accidents compared to the applicable anticipated transients.

15A.2.3 Comprehensiveness of the Analysis

The analysis must be sufficiently comprehensive in method that (1) all plant hardware is considered and (2) the full range of plant operating conditions is considered. The tendency to be preoccupied with "worst cases" (those that appear to give the most severe consequences) is

recognized; however, the protection sequences essential to lesser cases may be different (more or less restrictive) from the worst-case sequence. To assure that operational and design basis requirements are defined and appropriate for all equipment essential to attaining acceptable consequences, all essential protection sequences must be identified for each of the plant safety events examinations. Only in this way is a comprehensive level of safety attained. Thus, the NSOA is also "protection sequence" oriented to achieve comprehensiveness.

15A.2.4 Systematic Approach of the Analysis

In summary, the systematic method utilized in this analysis contributes to both the consistency and comprehensiveness of the analysis. The desired characteristics representative of a systematic approach to selecting BWR operational requirements are as follows:

(1) Specify measures of safety-unacceptable consequences

(2) Consider all normal operations

(3) Systematic event selection

(4) Common treatment analysis of all events of any one type

(5) Systematic identification of plant actions and systems essential to avoiding unacceptable consequences

(6) Emergency operational requirements and limits from system analysis

Figure 15A-1 illustrates the systematic process by which the operational and design basis nuclear safety requirements and technical specifications are derived. The process involves the evaluation of carefully selected plant events relative to the unacceptable consequences (specified measures of safety). Those limits, actions, systems and components found to be essential to achieving acceptable consequences are the subjects of operational requirements.

15A.2.5 Relationship of Nuclear Safety Operational Analysis to Safety Analyses of Chapter 15

One of the main objectives of the operational analysis is to identify all essential protection sequences and to establish the detailed equipment conditions essential to satisfying the nuclear safety operational criteria. The spectrum of events examined in Chapter 15 represents a complete set of plant safety considerations. The main objective of the earlier analyses of Chapter 15 is, of course, to provide detailed worst-case (limiting or envelope) analysis of the plant events. The worst cases are correspondingly analyzed and treated likewise in this appendix, but in light of frequency of occurrence, unacceptable consequences and assumption categories.

The detailed discussion relative to each of the events covered in Chapter 15 is not repeated in this appendix. Refer to the specific section in Chapter 15 as cross- correlated in Tables 15A-8

through 15A-12. These tables provide cross-correlation between the NSOA event, its protection sequence diagram and its safety evaluation in Chapter 15.

15A.2.6 Relationship Between NSOA and Operational Requirements, Technical Specifications, Design Basis, and SACF Aspects

By definition, "an operational requirement" is a requirement or restriction (limit) on either the value of a plant variable or the operability condition associated with a plant system. Such requirements must be observed during all modes of plant operation (not just at full power) to assure that the plant is operated safely (to avoid the unacceptable results). There are two kinds of operational requirements for plant hardware:

(1) Limiting Condition for Operation: the required condition for a system while the reactor is operating in a specified state

(2) Surveillance Requirements: the nature and frequency of tests required to assure that the system is capable of performing its essential functions

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

(1) To assure that unacceptable consequences are mitigated following specified plant events by examining and challenging the system design

(2) To assure the consequences of a transient or accident is acceptable with the existence of a SACF or SOE criteria

The individual structures and systems which perform a safety function are required to do so under design basis conditions, including environmental consideration and under single active component failure assumptions. The NSOA confirms the previous examination of the individual equipment (see the "Evaluations" subsection) requirement conformance analyses.

15A.2.7 Unacceptable Consequences Criteria

Tables 15A-1 through 15A-5 identify the unacceptable consequences and capability considerations associated with different event categories. To prevent or mitigate them, they are recognized as the major bases for identifying system operational requirements as well as the bases for all other safety analyses versus criteria throughout Tier 2.

15A.2.8 General Nuclear Safety Operational Criteria

The nuclear safety operational criteria used to select operational requirements are described in Table 15A-6.

The unacceptable consequences associated with the different categories of plant operations and events are dictated by:

(1) Probability of occurrence

(2) Allowable limits (per the probability) related to radiological, structural, environmental, etc., aspects

(3) Coincidence of other related or unrelated disturbances

(4) Time domain of event and consequences consideration

15A.3 Method of Analysis

15A.3.1 General Approach

The NSOA is performed on the plant as designed. The end products of the analysis are the nuclear safety operational requirements and the restrictions on plant hardware and its operation that must be observed (1) to satisfy the nuclear safety operational criteria and (2) to show compliance of the plant safety and power generation systems with plant wide requirements. Figure 15A-2 shows the process used in the analysis. The following inputs are required for the analysis of specific plant events:

(1) Unacceptable Consequences Criteria (Subsection 15A.2.7)

(2) General Nuclear Safety Operational Criteria (Subsection 15A.2.8)

(3) ABWR Operating States (Subsection 15A.3.2)

(4) Selection of Events for Analysis (Subsection 15A.3.3)

(5) Guidelines for Event Analysis (Subsection 15A.3.5)

With this information, each selected event can be evaluated to systematically determine the actions, systems and limits essential to avoiding the defined unacceptable consequences. The essential plant components and limits so identified are then considered to be in agreement with and subject to nuclear operational, design basis requirements and technical specification restrictions.

15A.3.2 BWR Operating States

Four ABWR operating states in which the reactor can exist are defined in Subsection 15A.6.2.4 and summarized in Table 15A-7. The main objective in selecting operating states is to divide the ABWR operating spectrum into sets of initial conditions to facilitate consideration of various events in each state.

Each operating state includes a wide spectrum of values for important plant parameters. Within each state, these parameters are considered over their entire range to determine the limits on their values necessary to satisfy the nuclear safety operational criteria. The plant parameters to be considered in this manner include the following:

(1) Reactor coolant temperature

(2) Reactor vessel water level

(3) Reactor vessel pressure

(4) Reactor vessel water quality

(5) Reactor coolant forced circulation flow rate

(6) Reactor power level (thermal and neutron flux)

(7) Core neutron flux distribution

(8) Feedwater temperature

(9) Containment temperature and pressure

(10) Suppression pool water temperature and level

(11) Spent fuel pool water temperature and level

15A.3.3 Selection of Events for Analysis

15A.3.3.1 Normal Operation

Operations subsequent to an incident (transient, accident or additional plant capability event) are not considered planned operations until the actions taken or equipment used in the plant are identical to those that would be used had the incident not occurred. As defined, the planned operations can be considered as a chronological sequence: refueling outage --> achieving criticality --> heatup --> power operation --> achieving shutdown --> cooldown --> refueling outage.

The normal operations are defined below.

(1) Refueling Outage: Includes all the planned operations associated with a normal refueling outage except those tests in which the reactor is taken critical and returned to the shutdown condition. The following planned operations are included in refueling outage:

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

(b) Refueling test operations (except criticality and shutdown margin tests)

(c) Planned maintenance

(d) Required inspection

(2) Achieving Criticality: Includes all the plant actions 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.

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

(4) Power Operation: Begins when heatup ends and includes continued plant operation at power levels in excess of heatup power.

(5) Achieving Shutdown: Begins when the main generator is unloaded and includes all plant actions normally accomplished in achieving nuclear shutdown (more than one rod subcritical) following power operation.

(6) Cooldown: Begins when achieving nuclear shutdown ends and includes all plant actions normal to the continued removal of decay heat and the reduction of RPV temperature and pressure.

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

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

15A.3.3.2 Moderate Frequency Incidents (Anticipated Operational Transients)

To select moderate frequency incidents (anticipated operational transients), eight nuclear system parameter variations are considered as potential initiating causes of threats to the fuel and the reactor coolant pressure boundary. The parameter variations are as follows:

(1) Reactor pressure vessel pressure increase

(2) Reactor pressure vessel water (moderator) temperature decrease

(3) Control rod withdrawal

(4) Reactor pressure vessel coolant inventory decrease

(5) Rector core coolant flow decrease

(6) Reactor core coolant flow increase

(7) Core coolant temperature increase

(8) Excess of coolant inventory

These parameter variations, if uncontrolled, could result in damage to the reactor fuel or reactor coolant pressure boundary, or both. A nuclear system pressure increase threatens to rupture the reactor coolant pressure boundary from internal pressure. A pressure increase also collapses voids in the moderator, causing an insertion of positive reactivity that threatens fuel damage as a result of overheating. A reactor vessel water (moderator) temperature decrease results in an insertion of positive reactivity as density increases. This could lead to fuel overheating. Positive reactivity insertions are possible from causes other than nuclear system pressure or moderator temperature changes. Such reactivity insertions threaten fuel damage caused by overheating. Both a reactor vessel coolant inventory decrease and a reduction in coolant flow through the core threatens the integrity of the fuel as the coolant becomes unable to adequately remove the heat generated in the core. An increase in coolant flow through the core reduces the void content of the moderator and results in an insertion of positive reactivity. Core coolant temperature increase threatens the integrity of the fuel; such a variation could be the result of a heat exchanger malfunction during operation in the shutdown cooling mode. An excess of coolant inventory could be the result of malfunctioning water level control equipment; such a malfunction can result in a turbine trip, which causes an expected increase in nuclear system pressure and power.

Moderate frequency incidents (anticipated operational transients) are defined as transients resulting from a SACF or SOE that can be reasonably expected (moderate probability of occurrence once per year to once in 20 years) during any mode of plant operation. Examples of single operation failures or operator errors in this range of probability are:

(1) Opening or closing any single valve (a check valve is not assumed to close against normal flow)

(2) Starting or stopping any single component

(3) Malfunction or maloperation of any single control device

(4) Any single electrical failure

(5) Any single operator error

An operator error is defined as an active deviation from nuclear plant standard operating practices. A single operator error is the set of actions that is a direct consequence of a single reasonably expected erroneous decision. The set of actions is limited as follows:

(1) Those actions that could be performed by only one person

(2) Those actions that would have constituted a correct procedure had the initial decision been correct

(3) Those actions that are subsequent to the initial operator error and that affect the designed operation of the plant, but are not necessarily directly related to the operator error

The various types of a single operator error or a single active component failure are applied to various plant systems with a consideration for a variety of plant conditions to discover events directly resulting in an undesired parameter variation. Once discovered, each event is evaluated for the threat it poses to the integrity of the radioactive material barriers.

15A.3.3.3 Infrequent Incidents (Abnormal Operational Transients)

To select infrequent incidents, eight nuclear system parameter variations are considered as potential initiating causes of gross core-wide fuel failures and threats of the reactor coolant pressure boundary. The parameter variations are as follows:

(1) Reactor pressure vessel pressure increase

(2) Reactor pressure vessel water (moderator) temperature decrease

(3) Control rod withdrawal

(4) Reactor vessel coolant inventory decrease

(5) Reactor core coolant flow decrease

(6) Reactor core coolant flow increase

(7) Core coolant temperature increase

(8) Excess of coolant inventory

The eight parameter variations listed above include all effects within the nuclear system caused by abnormal operational transients that threaten gross core-wide reactor fuel integrity or seriously affect reactor coolant pressure boundary. Variation of any one parameter may cause a change in another listed parameter; however, for analysis purposes, threats to barrier integrity are evaluated by groups according to the parameter variation originating the threat.

Infrequent incidents (abnormal operational transient) are defined as incidents resulting from single or multiple equipment failure and/or single or multiple operator errors that are not reasonably expected (less than one event in 20 years to one in 100 years) during any mode of plant operation. Examples of single or multiple operational failure and/or single or multiple operator errors are:

(1) Failure of major power generation equipment components

(2) Multiple electrical failures

(3) Multiple operator errors

(4) Combinations of equipment failure and an operator error

Operator error is defined as an active deviation from nuclear plant standard operating practices. A multiple operator error is the set of actions that is a direct consequence of several unexpected erroneous decisions.

The various types of a single errors and/or single malfunctions are applied to various plant systems with a consideration for a variety of plant conditions to discover events directly resulting in an undesired parameter variation. Once discovered, each event is evaluated for the threat it poses to the integrity of the various radioactive material barriers.

15A.3.3.4 Limiting Faults (Design Basis Accidents)

Limiting faults (accidents) are defined as hypothesized events that affect the radioactive material barriers and are not expected during plant operations. These are plant events, equipment failures, combinations of initial conditions which are of extremely low probability (once in 100 years or longer). The postulated accident types considered are as follows:

(1) Mechanical failure of a single component leading to the release of radioactive materials from one or more barriers. The components referred to here are not those that act as radioactive material barriers. Examples of mechanical failure are breakage of the coupling between a control rod drive and the control rod.

(2) Arbitrary rupture of any single pipe up to and including complete severance of the largest pipe in the reactor coolant pressure boundary. This kind of accident is considered only under conditions in which the nuclear system is pressurized.

For purposes of analysis, accidents are categorized as those events that result in releasing radioactive material:

(1) From the fuel with the reactor coolant pressure boundary, Reactor Building initially intact

(2) Directly to the containment

(3) Directly to the Reactor or Turbine Buildings with the containment initially intact

(4) Directly to the Reactor Building with the containment not intact

(5) Directly to the spent fuel containing facilities within the Reactor Building

(6) Directly to the Turbine Building

(7) Directly to the environs

The effects of various accident types are investigated, with consideration for the full spectrum of plant conditions, to examine events that result in the release of radioactive material.

15A.3.3.5 Special Events

A number of additional events are evaluated to demonstrate plant capabilities relative to special arbitrary nuclear safety criteria. These special events involve extremely low probability occurrence situations. As an example, the adequacy to the redundant reactivity control system is demonstrated by evaluating the special event: “reactor shutdown without control rods.” A similar example, the capability to perform a safe shutdown from outside the main control room, is demonstrated by evaluating the special event: “reactor shutdown from outside the main control room.”

15A.3.4 Applicability of Events to Operating States

The first step in performing an operational analysis for a given “incident” (transient, accident or special event) is to determine in which operating states the incident can occur. An incident is considered applicable within an operating state if the incident can be initiated from the physical conditions that characterize the operating state. Applicability of the “normal operations” to the operating states follows from the definitions of planned operations. A planned operation is considered applicable within an operating state if the planned operation can be conducted when the reactor exists under the physical conditions defining the operating state.

15A.3.5 Guidelines for Event Analysis

The following functional guidelines are followed in performing SACF, operational design basis analyses for the various plant events:

(1) An action, system, or limit shall be considered essential only if it is essential to avoiding an unacceptable result or satisfying the nuclear safety operational criteria.

(2) The full range of initial conditions (as defined in Subsection 15A.3.5(3)) shall be considered for each event analyzed so that all essential protection sequences are identified. Consideration is not limited to worst cases because lesser cases sometimes may require more restrictive actions or systems different from the worst cases.

(3) The initial conditions for transients, accidents and additional plant capability events shall be limited to conditions that would exist during planned operations in the applicable operating state.

(4) For normal operations, consideration shall be made only for actions, limits, and systems essential to avoiding the unacceptable consequences during operation in that state (as opposed to transients, accidents and additional plant capability events, which are followed through to completion). Normal operations are treated differently from other events because the transfer from one state to another during planned operations is deliberate. For events other than normal operations, the transfer from one state to another may be unavoidable.

(5) Limits shall be derived 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 frequently monitored process parameters are called "envelope limits," and limits on parameters associated with the operability of a safety system are called "operability limits." Systems associated with the control of the envelope parameters are considered nonessential if it is possible to place the plant in a safe condition without using the system in question.

(6) For transients, accidents and special events, consideration shall be made for the entire duration of the event and aftermath until some planned operation is resumed.

Normal operation is considered resumed when the procedures being followed or equipment being used are identical to those used during any one of the defined planned operations. Where "Extended Core Cooling" is an immediate integral part of the event, it will be included in the protection sequence. Where it may be an eventual part of the event, it will not be directly added but, of course, can be implied to be available.

(7) Credit for operator action shall be taken on a case-by-case basis, depending on the conditions that would exist at the time operator action would be required. Because transients, accidents and special events are considered through the entire duration of the event until normal operation is resumed, manual operation of certain systems is sometimes required following the more rapid or automatic portions of the event. Credit for operator action is taken only when the operator can reasonably be expected to accomplish the required action under the existing conditions.

(8) For transients, accidents and special events, only those actions, limits and systems shall be considered essential for which there arises a unique requirement as a result of the event. For instance, if a system that was operating prior to the event (during planned operation) is to be employed in the same manner following the event, and if the event did not affect the operation of the system, then the system would not appear on the protection sequence diagram.

(9) The operational analyses shall identify all the support of auxiliary systems essential to the functioning of the frontline safety systems. Safety system auxiliaries whose failure results in safe failure of the frontline safety systems shall be considered nonessential.

(10) A system or action that plays a unique role in the response to a transient, accident or special event shall be considered essential unless the effects of the system or action are not included in the detailed analysis of the event.

15A.3.6 Steps in an Operational Analysis

All information needed to perform an operational analysis for each plant event has been presented (Figure 15A-1). The procedure for performing an operational analysis for a given event (selected according to the event selection criteria) is as follows:

(1) Determine the ABWR operating states in which the event is applicable.

(2) Identify all the essential protection sequences (safety actions and frontline safety systems) for the event in each applicable operating state.

(3) Identify all the safety system auxiliaries essential to the functioning of the frontline safety systems.

These three steps are performed in Section 15A.6.

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

(1) Identify all the essential actions within the system (intrasystem actions) necessary for the system to function to the degree necessary to avoid the unacceptable consequences.

(2) Identify the minimum hardware conditions necessary for the system to accomplish the minimum intrasystem actions.

(3) If the single-failure criterion applies, identify the additional hardware conditions necessary to achieve the plant safety actions (e.g., scram, pressure relief, isolation, cooling) in spite of single failures. This step gives the nuclear safety operational requirements for the plant components so identified.

(4) Identify surveillance requirements and allowable repair times for the essential plant hardware (Subsection 15A.5.2).

(5) Simplify the operational requirements determined in steps (3) and (4) so that a technical specification may be obtained that encompass the true operational requirements and are easily used by plant operations and management personnel.

15A.4 Display of Operational Analysis Results

15A.4.1 General

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

Tables 15A-7 and 15A-8 through 15A-12 indicate which operating states each event is applicable. For each event, a block diagram is presented showing the conditions and systems required to achieve each essential safety action. The block diagrams show only those systems necessary to provide the safety actions such that the nuclear safety operational and design basis criteria are satisfied. The total plant capability to provide a safety action is generally not shown, only the minimum capability essential to satisfying the operational criteria. It is very important to understand that only enough protective equipment is cited in the diagram to provide the necessary action. Many events can utilize many more paths to success than are shown. These operational analyses involve the minimum equipment needed to prevent or avert an unacceptable consequence. Thus, the diagrams depict all essential protection sequences for each event with the least amount of protective equipment needed. Once all of these protection sequences are identified in block diagram form, system requirements are derived by considering all events in which the particular system is employed. The analysis considers the following conceptual aspects:

(1) The ABWR operating state

(2) Types of operations or events that are possible within the operating state

(3) Relationships of certain safety actions to the unacceptable consequences and to specific types of operations and events

(4) Relationships of certain systems to safety actions and to specific types of operations and events

(5) Supporting or auxiliary systems essential to the operation of the frontline safety systems

(6) Functional redundancy (the single-failure criterion applied at the safety action level; this is, in effect, a qualitative, system-level, FMEA-type analysis)

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

15A.4.2 Protection Sequence and Safety System Auxiliary Diagrams

Block diagrams illustrate essential protection sequences for each event requiring unique safety actions. These protection sequence diagrams show only the required frontline safety systems. The format and conventions used for these diagrams are shown in Figure 15A-3.

The auxiliary systems essential to the correct functioning of frontline safety systems are shown on safety system auxiliary diagrams. The format used for these diagrams is shown in Figure 15A-4. The diagram indicates that auxiliary systems A, B, and C are required for proper operations of frontline safety system X.

Total plant requirements for an auxiliary system or the relationships of a particular auxiliary system to all other safety systems (frontline and auxiliary) within an operating state are shown on the commonality of auxiliary diagrams. The format used for these diagrams is shown in Figure 15A-5. The convention employed in Figure 15A-5 indicates that auxiliary system A is required:

(1) To be single-failure proof relative to system γ in State A-events X, Y; State B-events X, Y; State C-events X, Y, Z; State D-events X, Y, Z.

(2) To be single-failure proof relative to the parallel combination of systems α and β in State A-events U, V, W; State B-events V, W; State C-events U, V, W, X; State D-events U, V, W, X.

(3) To be single-failure proof relative to the parallel combination of system π and ε in series with the parallel combination of systems Epsilon and Chi in State C-events Y, W; State D-events Y, W, Z. As noted, system ε is part of the combination but does not require auxiliary system A for its proper operation.

(4) For system δ in State B-events Q, R; State D-events Q, R, S.

With these three types of diagrams, it is possible to determine for each system the detailed functional requirements and conditions to be observed regarding system

hardware in each operating state. The detailed conditions to be observed regarding system hardware include such nuclear safety operational requirements as test frequencies and the number of components that must be operable.

15A.5 Bases for Selecting Surveillance Test Frequencies and Allowable Outage Times

15A.5.1 Normal Surveillance Test Frequencies

After the essential nuclear safety systems and engineered safeguards have been identified by applying the nuclear safety operational criteria, surveillance requirements are selected for these systems. In this selection process, the various systems are considered in terms of relative availability, test capability, plant conditions necessary for testing and engineering experience with the system type. Surveillance test frequencies are determined using models developed in the Probabilistic Risk Assessment (PRA).

15A.5.2 Allowable Outage Times

Allowable outage times are selected by computation using models developed in the PRA. The resulting maximum average allowable outage times assure that a system's long-term availability, including allowance for repair and test, is not reduced below a specified availability.

15A.5.3 Outage Time Rule

A safety system can be repaired or tested while the reactor is in operation if the repair and test time is equal to or less than the maximum allowable average outage time. If repair or test is not complete when the allowable outage time expires, the plant must be placed in its safest mode (with respect to the protection lost) in accordance with the Technical Specifications.

To maintain the validity of the assumptions used to establish the previously noted repair rule, the following restrictions must be observed:

(1) The allowable outage time is only used as needed to restore failed equipment to operation or to perform required surveillance tests, not for routine maintenance. Routine maintenance should be scheduled when the equipment is not needed.

(2) At the conclusion of the repair, the repaired component must be retested and placed in service.

(3) Once the need for repair of a failed component is discovered, repairs should proceed as quickly as possible consistent with good craftsmanship.

15A.6 Operational Analyses

Results of the operational analyses are discussed in the following paragraphs and displayed on Figures 15A-6 through 15A-70 and in Tables 15A-8 through 15A-12.

15A.6.1 Safety System Auxiliaries

Figures 15A-6 and 15A-7 show the safety system auxiliaries essential to the functioning of each frontline safety system. Commonality of auxiliary diagrams is shown in Figures 15A-65 through 15A-70.

15A.6.2 Normal Operations

15A.6.2.1 General

Requirements for the normal or planned operations normally involve limits (L) on certain key process variables and restrictions (R) on certain plant equipment. The control block diagrams for each operating state (Figures 15A-8 through 15A-11) show only those controls necessary to avoid unacceptable safety consequences (1-1 through 1-4 of Table 15A-1). Table 15A-8 summarizes additional information for Normal Operation.

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

15A.6.2.2 Event Definitions

Event 1—Refueling Outage

Refueling outage includes all the planned operations associated with a normal refueling outage except those tests in which the reactor is made critical and returned to the shutdown condition. The following planned operations are included in refueling outage:

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

(2) Refueling test operations (except for the criticality and the shutdown margin tests)

(3) Planned maintenance

(4) Required inspections

Event 2—Achieving Criticality

Achieving criticality includes all the plant actions 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.

Event 3—Reactor Heatup

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

Event 4—Power Operation—Electric Generation

Power operation begins where heatup ends and continued plant operation at power levels in excess of heatup power or steady-state operation. It also includes plant maneuvers such as:

(1) Daily electrical load reduction and recoveries

(2) Electrical grid frequency control adjustment

(3) Control rod movements

(4) Power generation surveillance testing involving:

(a) Turbine stop valve closing

(b) Turbine control valve adjustments

(c) Main Steam Isolating Valve (MSIV) exercising

Event 5—Achieving Reactor Shutdown

Achieving shutdown begins where the main generator is unloaded and includes all plant actions normally accomplished in achieving nuclear shutdown (more than one rod subcritical) after power operation.

Event 6—Reactor Cooldown

Cooldown begins where achieving shutdown ends and includes all plant actions normal to the continued removal of decay heat and the reduction of nuclear system temperature and pressure.

15A.6.2.3 Required Safety Actions/Related Unacceptable Consequences

The following paragraphs describe the safety actions for planned operations. Each description includes a selection of the operating states that apply to the safety action, the plant system affected by limits or restrictions and the unacceptable consequence that is avoided. The four operating states are defined in Table 15A-7. The unacceptable consequences criteria are tabulated in Table 15A-1.

15A.6.2.3.1 Radioactive Material Release Control

Radioactive materials may be released to the environs in any operating state; therefore, radioactive material release control is required in all operating states. Because of the significance of preventing excessive release of radioactive materials to the environs, this is the only safety action for which monitoring systems are explicitly shown. The offgas vent radiation monitoring system provides indication for gaseous release through the main vent. Gaseous releases through other vents are monitored by the ventilation monitoring system. The process liquid radiation monitors are not required because all liquid wastes are monitored by batch sampling before a controlled release. Limits are expressed on the offgas vent system, liquid radwaste system and solid radwaste system so that the planned release of radioactive materials

comply with the limits given in 10CFR20, 10CFR50, and 10CFR71 (related unacceptable safety result 1-1 Table 15A-1).

15A.6.2.3.2 Core Coolant Flow Rate Control

In State D, when above approximately 10% Nuclear Boiler (NB) rated power, the core coolant flow rate must be maintained above certain minimums (i.e., limited) to maintain the integrity of the fuel cladding (1-2) and assure the validity of the plant safety analysis (1-4).

15A.6.2.3.3 Core Power Level Control

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

15A.6.2.3.4 Core Neutron Flux Distribution Control

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

15A.6.2.3.5 Reactor Vessel Water Level Control

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

15A.6.2.3.6 Reactor Vessel Pressure Control

Reactor vessel pressure control is not needed in states A and B because vessel pressure cannot be increased above atmospheric pressure. In State C, a limit is expressed on the reactor vessel to assure that it is not hydrostatically tested until the temperature is above the NDT temperature plus 33.3°C; this prevents excessive stress (1-3). Also, in States C and D a limit is expressed on the Residual Heat Removal (RHR) System to assure that it is not operated in the shutdown cooling mode when the reactor vessel pressure is greater than approximately 0.689 MPaG

(0.932 MPaG limit); this prevents excessive stress (1-3). In States C and D, a limit on the reactor vessel pressure is necessitated by the plant safety analysis (1-4).

15A.6.2.3.7 Nuclear System Temperature Control

In operating States C and D, a limit is expressed on the reactor vessel to prevent the reactor vessel head bolting studs from being in tension when the temperature is less than 21°C to avoid excessive stress (1-3) on the reactor vessel flange. This limit does not apply in States A and B because the head will not be bolted in place during criticality tests or during refueling. In all operating states, a limit is expressed on the reactor vessel to prevent an excessive rate of change of the reactor vessel temperature to avoid excessive stress (1-3). In States C and D, where it is planned operation to use the Feedwater System, a limit is placed on the reactor fuel so that the feedwater temperature is maintained within the envelope of conditions considered by the plant safety analysis (1-4). For State D, a limit is observed on the temperature difference between the bottom head drain and the reactor vessel saturation to prevent the starting of the reactor internal pumps. This operating restriction and limit prevents excessive stress in the reactor vessel (1-3).

15A.6.2.3.8 Nuclear System Water Quality Control

In all operating states, water of improper chemical quality could produce excessive stress as a result of chemical corrosion (1-3). Therefore, a limit is placed on reactor coolant chemical quality in all operating states. For all operating states where the nuclear system can be pressurized (States C and D), an additional limit on reactor coolant activity assures the validity of the analysis of the main steamline break accident.

15A.6.2.3.9 Nuclear System Leakage Control

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

15A.6.2.3.10 Core Reactivity Control

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

15A.6.2.3.11 Control Rod Worth Control

Any time the reactor is not shut down and is generating less than 20% power (State D), a limit is imposed on the control rod pattern to assure that control rod worth is maintained within the envelope of conditions considered by the analysis of the rod withdrawal error (1-4).

15A.6.2.3.12 Refueling Restriction

By definition, planned operation event 1 (refueling outage) applies only to State A. Observing the restrictions on the reactor fuel and on the operation of the CRD System within the specified limit maintains plant conditions within the envelope considered by the plant safety analysis (1-4).

15A.6.2.3.13 Containment and Reactor Building Pressure and Temperature Control

In States C and D, limits are imposed on the suppression pool temperature to maintain containment pressure within the envelope considered by plant safety analysis (1-4). These limits assure an environment in which instruments and equipment can operate correctly within the containment. Limits on the pressure suppression pool apply to the water temperature and water level to assure that it has the capability of absorbing the energy discharged during a safety/relief valve blowdown.

15A.6.2.3.14 Stored Fuel Shielding, Cooling and Reactivity Control

Because both new and spent fuel will be stored during all operating states, stored fuel shielding, cooling and reactivity control apply to all operating states. Limits are imposed on the spent fuel pool storage positions, water level, fuel-handling procedures and water temperature. Observing the limits on fuel storage positions assures that spent fuel reactivity remains within the envelope of conditions considered by the plant safety analysis (1-4). Observing the limits on water level assures shielding in order to maintain conditions within the envelope of conditions considered by the plant safety analysis
(1-4) and provides the fuel cooling necessary to avoid fuel damage (1-2). Observing the limit on water temperature avoids excessive fuel pool stress (1-3).

15A.6.2.4 Operational Safety Evaluations

State A

In State A, the reactor is in a shutdown condition, the vessel head is off and the vessel is at atmospheric pressure. The applicable events for planned operations are refueling outage, achieving criticality, and cooldown (Events 1, 2, and 6, respectively).

Figure 15A-8 shows the necessary safety actions for planned operations, the corresponding plant systems and the event for which these actions are necessary. As indicated in the diagram, the required safety actions are as follows:

- Safety Action
  - Radioactive material release control
  - Reactor vessel water level control
  - Nuclear system temperature control

- Nuclear system water quality control
- Core reactivity control
- Refueling restrictions
- Stored fuel shielding, cooling and reactivity control

State B

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

Figure 15A-9 presents the necessary safety actions for planned operations, the plant systems and the event for which the safety actions are necessary. The required safety actions for planned operations in State B are as follows:

- Safety Actions
  - Radioactive material release control
  - Core power level control
  - Reactor vessel water level control
  - Nuclear system temperature control
  - Nuclear system water quality control
  - Core reactivity control
  - Rod worth control
  - Stored fuel shielding, cooling and reactivity control

State C

In State C, the reactor vessel head is on and the reactor is shutdown. Applicable planned operations are achieving criticality and cooldown (Events 2 and 6, respectively).

Sequence diagrams relating safety actions for planned operations, plant systems and applicable events are shown in Figure 15A-10. The required safety actions for planned operation in State C are as follows:

- Safety Actions
  - Radioactive material release control

- Reactor vessel pressure control
- Reactor vessel water level control
- Nuclear system temperature control
- Nuclear system water quality control
- Nuclear system leakage control
- Core reactivity control
- Containment building pressure and temperature control
- Spent fuel shielding, cooling and reactivity control

State D

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

Figure 15A-11 presents the necessary safety actions for planned operations, corresponding plant systems and events for which the safety actions are necessary. The required safety actions for planned operations in State D are as follows:

- Safety Actions
  - Radioactive material release control
  - Core cooling flow rate control
  - Core power level control
  - Core neutron flux distribution control
  - Reactor vessel water level control
  - Reactor vessel pressure control
  - Nuclear system temperature control
  - Nuclear system water quality control
  - Nuclear system leakage control
  - Core reactivity control

– Rod worth control

– Containment and reactor building pressure and temperature control

– Stored fuel shielding, cooling and reactivity control

15A.6.3 Moderate Frequency Incidents (Anticipated Operational Transients)

15A.6.3.1 General

The safety requirements and protection sequences for moderate frequency incidents (anticipated operational transients) are described in the following subsections for Events 7 through 24, 26, 27, 38-40, 43-45, 48, and 49. The protection sequence block diagrams show the sequence of frontline safety systems (Figures 15A-12 through 15A-29, 15A-31, 15A-32, 15A-45 through 15A-47, 15A-50, 15A-51, 15A-52, 15A-55, 15A-56). The auxiliaries for the frontline safety systems are presented in the auxiliary diagrams (Figures 15A-6 and 15A-7) and the commonality of auxiliary diagrams (Figures 15A-65 through 15A-70).

15A.6.3.2 Required Safety Actions/Related Unacceptable Consequences

The following list presents the safety actions for anticipated operational transients to mitigate or prevent the unacceptable safety consequences. Refer to Table 15A-2 for the unacceptable consequences criteria.

Safety Action	Related Unacceptable Consequences Criteria	Reason Action Required
Scram and/or trip of 4 RIPs	2-2, 2-3	To prevent fuel damage and to limit RPV system pressure rise.
Pressure relief	2-3	To prevent excessive RPV pressure rise.
Core and containment cooling	2-1, 2-2, 2-4	To prevent fuel and containment damage in the event that normal cooling is interrupted.
Reactor vessel isolation	2-2	To prevent fuel damage by reducing the outflow of steam and water from the reactor vessel, thereby limiting the decrease in reactor vessel water level.
Restore AC power	2-2	To prevent fuel damage by restoring AC power to systems essential to other safety actions.

Safety Action	Related Unacceptable Consequences Criteria	Reason Action Required
Prohibit rod motion	2-2	To prevent exceeding fuel limits during transients.
Containment Isolation	2-1, 2-4	To minimize radiological effects.

15A.6.3.3 Event Definitions and Operational Safety Evaluations

Event 7—Manual and Inadvertent SCRAM

The deliberate manual or inadvertent automatic SCRAM due to single operator error is an event which can occur under any operating conditions. Although assumed to occur here for examination purposes, multi-operator error or action is necessary to initiate such an event.

While all the safety criteria apply, no unique safety actions are required to control the planned-operation-like event after effects of the subject initiation actions. In all operating states, the safety criteria are therefore met through the basic design of the plant systems. Figure 15A-12 presents the protection sequences for this event.

Event 8—Loss-of-Plant Instrument or Service System Air

Loss of all plant instrument or service air system causes reactor shutdown and the closure of air-operated isolation valves. Although these actions occur, they are not a requirement to prevent unacceptable consequence in themselves. Multi-equipment failures would be necessary to cause the deterioration of the subject system to the point that the components supplied with instrument or service air cease to operate “normally” and/or “fail-safe.”

Figure 15A-13 shows how scram is accomplished by loss of air to scram solenoid valves of the Reactor Protection System and the CRD System. The nuclear system pressure relief system provides pressure relief. Pressure relief, combined with loss of feedwater flow, causes reactor vessel water level to fall. Either high-pressure core cooling system supplies water to maintain water level and to protect the core until normal steam flow (or other planned operation) is established.

Adequate reserve service air supplies are maintained exclusively for the continual operation of the Automatic Depressurization Subsystem (ADS) safety/relief valves until reactor shutdown is accomplished.

Event 9—Recirculation Flow Control Failure (Increasing Flow)—One RIP Runout

A recirculation flow control failure causing one RIP to runout is applicable in States C and D. The resulting increase in core flow is detected by the RFCS, which reduces the flow through the remaining RIPs, as shown in Figure 15A-14.

Event 10—Recirculation Flow Control Failure (Decreasing Flow)—One RIP Runback

This flow control malfunction causes a decrease in core coolant flow. This event is not applicable to States A and B because the reactor vessel head is off and the reactor internal pumps normally would not be in use. Figure 15A-15 shows that no protection sequence is needed for this event.

Event 11—Trip of Three Reactor Internal Pumps (RIPs)

The trip of three reactor internal pump produces a mild transient of flow and power reduction followed by a select control rod run-in action by the RFCS on detection of this trip. This event is not applicable in States A and B because the reactor vessel head is off and the recirculation pumps normally would not be in use. The trip could occur in States C and D. Figure 15A-16 presents the protection sequence for this event.

Event 12,13—Isolation of One or All Main Steamlines

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

Isolation of all main steamlines is most severe and rapid in operating State D during power operation.

Figure 15A-17 shows how scram is accomplished by main steamline isolation through the actions of the Reactor Protection and CRD Systems. The nuclear system pressure relief system provides pressure relief. Pressure relief, combined with loss of feedwater flow, causes reactor vessel water level to fall and the RCIC System supplies water to maintain water level and to protect the core until normal steam flow (or other planned operation) is established.

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

As shown in Figure 15A-18, the scram safety action is accomplished through the combined actions of the Neutron Monitoring, Reactor Protection and CRD Systems.

Event 14—Loss of All Feedwater Flow

A loss of feedwater flow results in a net decrease in the coolant inventory available for core cooling. A loss of feedwater flow can occur in States C and D. Appropriate responses to this transient include a reactor scram on low water level and restoration of reactor water level by the RCIC System.

As shown in Figure 15A-19, the Reactor Protection and CRD Systems effect a scram on low water level. The RCIC System maintains adequate water level for initial core cooling and to

restore and maintain water level. For long-term shutdown and extended core coolings, containment/suppression pool cooling systems are manually or automatically initiated.

Event 15—Loss of a Feedwater Heater

Loss of a feedwater heater must be considered with regard to the nuclear safety operational criteria only in operating State D because significant feedwater heating does not occur in any other operating stage.

A loss of more the 16.7°C of feedwater heating causes an alarm to be initiated by the Feedwater Control System (FWCS). Therefore, the most severe case is a loss of 16.7°C of feedwater heating, just below alarm initiation. This 16.7°C loss in feedwater heating results in a minimal 4% power increase and no scram is expected. The operator can control this minimal increase in power. The protection sequence for this event is shown on Figure 15A-20.

Event 16—Feedwater Controller Failure—Runout of One Feedwater Pump

A feedwater controller failure, causing runout of one feedpump, is possible in all operating states. In operating States A and B, no safety actions are required, because the vessel head is removed and the moderator temperature is low. In operating State D, the FWCS reduces flow from the other feedpump to maintain constant feed flow. Steady-state operation may continue, as no scram or turbine trip is expected as shown on Figure 15A-21.

Event 17—Pressure Regulator Failure—One Bypass Valve Failed Open

A pressure regulator failure in the open direction, causing the opening of one turbine control or bypass valve, applies only in operating States C and D, since in other states the pressure regulator is not in operation. An opening of a bypass valve is more severe than opening of a control valve. In either case, the pressure regulator slightly closes the remaining control valves to maintain set pressure. Steady-state operation may continue as shown in Figure 15A-22.

Event 18—Pressure Regulator Failure—One Control Valve Failed

A pressure regulator failure in the closed direction (or downscale), causing the closing of a turbine control valve, applies only in operating States C and D because in other states the pressure regulator is not in operation.

The pressure regulator slightly opens the remaining control valves or bypass valves to maintain set pressure. This action may not be fast enough to mitigate the event. A high neutron flux scram due to the increasing pressure is expected for initial rated power operation. The protection sequence is shown in Figure 15A-23.

Event 19—Main Turbine Trips (With Bypass System Operation)

A main turbine trip can occur only in operating State D (during heatup or power operation). A turbine trip during heatup is not as severe as a trip at full power because the initial power level is less than 40%, thus minimizing the effects of the transient and enabling return to planned operations via the bypass system operation. For a turbine trip above 40% power, a scram occurs via turbine stop valve closure, as will a trip of four RIPs. Subsequent relief valve actuation

occurs. Figure 15A-24 presents the protection sequences required for main turbine trips. Main turbine trip and load rejection events are similar anticipated operational transients having the same required safety actions.

Event 20—Loss of Main Condenser Vacuum

A loss of vacuum in the main turbine condenser can occur any time steam pressure is available and the condenser is in use; it is applicable to operating States C and D. However, scram protection in State C is not needed, because the reactor is not coupled to the turbine system.

For State D above 40% power, loss of condenser vacuum initiates a turbine trip with its attendant stop valve closures (which leads to SCRAM) and a trip of four RIPs and also initiates isolation, pressure relief valve and RCIC actuation. Below 40% power (State D) scram is initiated by a high neutron flux or high vessel pressure signal. Figure 15A-25 shows the protection sequences. Decay heat necessitates extended core and suppression pool cooling. When the RPV depressurizes sufficiently, the operation of RHR System shutdown cooling is achieved.

Event 21—Generator Load Rejection, Bypass On

A main generator load rejection with bypass system operation can occur only in operating State D (during heatup or power operation). Fast closure of the main turbine control valves is initiated whenever an electrical grid disturbance occurs, which results in significant loss of electrical load on the generator. The turbine control valves are required to close as rapidly as possible to prevent excessive overspeed of the main turbine-generator rotor. Closure of the turbine control valves causes a sudden reduction in steam flow, which results in an increase in system pressure. Above 40% power, scram occurs as a result of fast control valve closure, as will a trip of four RIPs. A generator load rejection during heatup (<40%) is not severe because the turbine bypass system can accommodate the decoupling of the reactor and the turbine-generator unit, thus minimizing the effects of the transient and enabling return to planned operations.
Figure 15A-26 presents the protection sequences required for a generator load rejection. Main generator load rejection event and main turbine trip are similar events having the same required safety actions.

Event 22—Loss of AC Power (Unit Auxiliary Transformer)

The loss of the unit auxiliary transformer causes a generator trip, a scram, a trip of four RIPs, a loss of feedwater flow and a loss of condenser vacuum.

Figure 15A-27 shows the protection sequence for this event, including a scram, a trip of four RIPs, a vessel isolation, pressure relief, and core and containment cooling. This event is applicable only in States C and D, because normal AC power in States A and B is supplied from the grid.

Event 23—Inadvertent HPCF Pump Start (Coolant/Moderator Temperature Decrease)

An inadvertent pump start (temperature decrease) is defined as an unintentional start of any nuclear system pump that adds sufficient cold water to the reactor coolant inventory to cause a measurable decrease in moderator temperature. This event is considered in all operating states because it can potentially occur under any operating condition. Since the HPCF pump operates over nearly the entire range of the operating states and delivers the greatest amount of cold water to the vessel, the following analysis will describe its inadvertent operation rather than other NSSS pumps (e.g., RCIC, RHR).

While all the safety criteria apply, no unique safety actions are required to control the effects of such a pump start. In operating States A and C, the safety criteria are met through the basic design of the plant systems, and no safety action is specified. In States B and D, where the reactor is not shutdown, the pressure and temperature will decrease. The operator or the plant normal control system can control any power changes in the normal manner of power control.

Figure 15A-28 illustrates the protection sequence for the subject event.

15A.6.3.4 Other Event Definitions and Operational Safety Evaluations

The following events should be classified as either infrequent incidents or limiting faults. However, criteria for moderate frequency incidents are conservatively applied.

Event 24—Inadvertent Opening of a Safety/Relief Valve

The inadvertent opening of a safety/relief valve is possible in any operating state. The protection sequences are shown in Figure 15A-29. In States A and B, the water level cannot be lowered far enough to threaten fuel damage; hence, no safety actions are required.

In States C and D, there is a slight decrease in reactor pressure following the event. The pressure regulator closes the main turbine control valves enough to stabilize pressure at a level slightly below the initial value. There are no unique safety system requirements for this event.

If the event occurs when the Feedwater System is not active, a scram is initiated by a low water level signal and core cooling is accomplished by the RCIC System, which are automatically initiated by the Nuclear Boiler Instrumentation System (NBIS). The Automatic Depressurization System (ADS) or the Manual Relief Valve System remain as the backup depressurization system, if needed. After the vessel has depressurized, long-term core cooling is accomplished by the RHR System.

Containment and suppression pool cooling are automatically or manually initiated.

Event 26—Main Turbine Trips with Failure of One Bypass Valve

A main turbine trip can occur only in operating State D (during heatup or power operation). A turbine trip during heatup is not as severe as a trip at full power because the initial power level is less than 40%, thus minimizing the effects of the transient and enabling return to planned

operations via the bypass system operation. For a turbine trip above 40% power, a scram occurs via turbine stop valve closure, as will a trip of four RIPs. Subsequent relief valve actuation occurs. Figure15A-31 presents the protection sequences required for main turbine trip with a failure of one bypass valve. The response of the plant to a turbine trip or a generator load rejection with a failure of one bypass valve is similar to that with a full bypass operation; protection sequences for these cases are the same.

Event 27—Generator Load Rejection with Failure of One Bypass Valve

A main generator load rejection with failure of one bypass valve can occur only in operating State D (during heatup or power operation). Fast closure of the main turbine control valves is initiated whenever an electrical grid disturbance occurs, which results in significant loss of electrical load on the generator. The turbine control valves are required to close as rapidly as possible to prevent excessive overspeed of the main turbine-generator rotor. Closure of the turbine control valves causes a sudden reduction in steam flow, which results in an increase in system pressure. Above 40% power, scram occurs as a result of fast control valve closure, as will a trip of four RIPs.

Prolonged shutdown of the turbine-generator unit necessitates extended core and containment cooling. Figure 15A-32 presents the protection sequences required for a main generator load rejection. Main generator load rejection with a failure of one bypass valve is similar to a load rejection with a full bypass operation. Therefore, the required safety actions for both are the same sequence.

Event 38—Abnormal Startup of Idle Reactor Internal Pump (RIP)

The abnormal startup of a reactor internal pump (RIP) can occur in any state and is most severe and rapid for those operating states in which the reactor may be critical (States B and D).

Occurrence of this event is prevented by a Recirculation Flow Control System (RFCS) interlock that prevents a pump start unless all remaining pumps are at their minimum speeds. For this case of multiple failures and operator errors, the large flow reversal and associated starting pump inverter overcurrent activates a protective logic that trips the two or three RIPs on the bus. In that case, the event is covered by Event 11. Figure 15A-45 shows the protective sequence for this event.

Event 39—Recirculation Flow Control Failure (Increasing Flow)—Runout of All RIPs

A recirculation flow control failure, causing runout of all RIPs, is applicable in States C and D. In State D, the resulting increase in power level is limited by a reactor scram. As shown in Figure 15A-46, the scram safety action is accomplished through the combined actions of the Neutron Monitoring, Reactor Protection and FMCRD Systems.

Event 40—Recirculation Flow Control Failure (Decreasing Flow)—Runback of All RIPs

This recirculation flow control malfunction causes a decrease in core coolant flow. This event is not applicable to States A and B because the reactor vessel head is off and the reactor internal pumps normally would not be in use. Figure 15A-47 shows that no protection sequences are required for this event.

Event 43—RHR Shutdown Cooling—Increased Cooling

An RHR shutdown cooling malfunction causing a moderator temperature decrease must be considered in all operating states. However, this event is not considered in States C and D if RPV system pressure is too high to permit operation of the shutdown cooling (RHRS) (Figure 15A-50). No unique safety actions are required to avoid the unacceptable safety consequences 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 at or near critical, the slow power increase resulting from the cooler moderator temperature would be controlled by the operator in the same manner normally used to control power in the source or intermediate power ranges.

Event 44—Feedwater Controller Failure—Runout of All Feedwater Pumps

A feedwater controller failure, causing an excess of coolant inventory in the reactor vessel, is possible in all operating states. Feedwater controller failures considered are those that would give failures of automatic flow control, manual flow control, or feedwater bypass valve control. In operating States A and B, no safety actions are required, since the vessel head is removed and the moderator temperature is low. In operating State D, any positive reactivity effects of the reactor caused by cooling of the moderator can be mitigated by a scram. As shown in Figure 15A-51, the accomplishment of the scram safety action is satisfied through the combined actions of the Neutron Monitoring, Reactor Protection and FMCRD Systems. Due to the increasing water level and the resulting L-8 turbine trip, pressure relief is required in States C and D and is achieved through the operation of the RPV pressure relief system. Initial restoration of the core water level is by the RCIC or HPCF Systems.

Event 45—Pressure Regulator Failure—Opening of All Turbine Control and Bypass Valves

A pressure regulator failure in the open direction, causing the opening of all turbine control and bypass valves, applies only in operating States C and D because in other states the pressure regulator is not in operation. A pressure regulator failure is most severe and rapid in operating State D at low power.

The various protection sequences giving the safety actions are shown in Figure 15A-52. Depending on plant conditions existing prior to the event, scram is initiated either on main steamline isolation, main turbine trip or reactor vessel low water level. The sequence resulting in reactor vessel isolation also depends on initial conditions. With the mode switch in RUN, isolation is initiated when main steamline pressure decreases to 5.2 MPaG. After isolation is

completed, decay heat causes reactor vessel pressure to increase until limited by the operation of the relief valves. Core cooling following isolation is provided by the RCIC or HPCF Systems. Shortly after reactor vessel isolation, normal core cooling is re-established via the main condenser and feedwater systems or, if prolonged isolation is necessary, extended core and containment cooling will be manually actuated.

Event 48—Main Turbine Trip (Without Bypass System Operation)

A main turbine trip without bypass can occur only in operating State D (during heatup of power operation). Figure 15A-55 presents the protection sequences required for main turbine trips. Plant operation with bypass system operation above or below 40% power, due to bypass system failure, results in the same transient effects: a scram, a trip of four RIPs, and subsequent relief valve actuation. After initial shutdown, extended core and containment cooling is required as noted previously in Event 19.

Turbine trips without bypass system operation results in more severe thermohydraulic impacts on the reactor core than with bypass system operation. The allowable limit or acceptable calculational techniques for this event is less restrictive, because the event is of lower probability of occurrence than the turbine trip with a bypass operation event.

Event 49—Generator Load Rejection with Failure of All Bypass Valves

A main generator trip without bypass system operation can occur only in operating State D (during heatup or power operation). A generator trip during heatup without bypass operation results in the same situation as the power operation case. Figure 15A-56 presents the protection sequences required for a generator load rejection with failure of all bypass valves. The event is basically the same as described in Event 21 at power levels above 40%. A scram, trip of four RIPs, and relief valve operation immediately results in prolonged shutdown, which follows the same pattern as Event 21.

The thermohydraulic and thermodynamic effects on the core, of course, are more severe than with the bypass operating. Because the event is of lower probability than Event 21, the unacceptable consequences are less limiting.

15A.6.4 Infrequent Incidents (Abnormal Operational Transients)

15A.6.4.1 General

The safety requirements and protection sequences for infrequent incidents (abnormal operational transients) are described in the following paragraphs for Event 25. The protection sequence block diagrams show the sequence of frontline safety systems (Figures 15A-30). The auxiliaries for the frontline safety systems are indicated in the auxiliary diagrams (Figures 15A-6 and 15A-7) and the commonality of auxiliary diagrams (Figures 15A-65 through 15A-70).

15A.6.4.2 Required Safety Actions/Related Unacceptable Consequences

Table 15A-13 relates the safety actions for infrequent incidents to mitigate or prevent the unacceptable safety consequences cited in Table 15A-3.

15A.6.4.3 Event Definition and Operational Safety Evaluation

Event 25—Control Rod Withdrawal Error During Refueling and Startup Operations

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

- Refueling

No unique safety action is required in operating State A for the withdrawal of one control rod because the core is more than one control rod subcritical. Withdrawal of more than one control rod is precluded by the protection sequence shown in
Figure 15A-30. During core alterations, the mode switch is normally in the REFUEL position, which allows the refueling equipment to be positioned over the core and also inhibits more than one control rod withdrawal.

Moreover, mechanical design of the control rod assembly prevents physical removal of the control rod blade from the top without removing the adjacent fuel assemblies.

- Startup

During startup, while pulling control rods in States C, the reactor is subcritical by more than one rod. Therefore, no protection sequence is needed for this condition.

During low power operation (States B and D), the RPS initiates SCRAM on short period or high neutron flux in addition to a short period rod block as shown on
Figure 15A-30.

Event 50—Misplaced/Misoriented Fuel Bundle Accident

Operation with a fuel assembly in the improper position or orientation is shown in Figure 15A-57 and can occur in all operating states. No protection sequences are necessary relative to this event. It requires three independent equipment/operator errors to allow this situation to develop.

15A.6.5 Limiting Faults (Design Basis Accidents)

15A.6.5.1 General

The safety requirements and protection sequences for limiting faults (accidents) are described in the following paragraphs for Events 28 through 37, 41, 42, 46, 50-52. The protection sequence block diagrams show the safety actions and the sequence of frontline safety systems used for the accidents (Figures 15A-33 through15A-44, 48, 49, 53, 57, 58, 59). The auxiliaries

for the frontline safety systems are presented in the auxiliary diagrams (Figures 15A-6 and 15A-7) and the commonality of auxiliary diagrams (Figures 15A-45 through 15A-70).

15A.6.5.2 Required Safety Actions/Unacceptable Consequences

Table 15A-14 presents the safety actions for design basis accident to mitigate or prevent the unacceptable consequences cited in Table 15A-4.

15A.6.5.3 Event Definition and Operational Safety Evaluations

Event 28—Control Rod Ejection Accident

A control rod ejection accident for the fine motion control rod drive design is not a credible event. Therefore, no protection sequence is required.

Event 29—Control Rod Drop Accident (CRDA)

A control rod drop accident for the fine motion control rod drive design is not a credible event. Therefore, no protection sequence is required.

Event 30—Control Rod Withdrawal Error (During Power Operation)

During power operation in State D, the Automated Rod Block Monitoring System (ARBM) of the Rod Control and Information System prevents control rod withdrawals that would result in thermal limit violations. Therefore, this event is not a credible event and no protection sequence is required as shown in Figure 15A-35.

Event 31—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 a spent fuel pool, this accident is considered in all operating states. Considerations include mechanical fuel damage caused by drop impact and a subsequent release of fission products. The protection sequences pertinent to this accident are shown in Figure 15A-36. Containment and/or Reactor Building isolation and standby gas treatment operation are automatically initiated by the respective building, pool and/or ventilation radiation monitoring systems.

Event 32—Loss-of-Coolant Accidents (LOCA) Resulting from Postulated Piping Breaks Within RPCB Inside Primary Containment

Pipe breaks inside the primary containment are considered only when the nuclear system is significantly pressurized (States C and D). The result is a release of steam and water into the containment. Consistent with NSOA criteria, the protection requirements consider all size line breaks, including liquid pipe breaks down to small steam instrument line breaks. The most severe cases are the circumferential break of the high pressure core flooder (liquid) system injection line and the circumferential break of the largest (steam) main steamline.

As shown in Figures 15A-37 and 15A-38, in operating State C (reactor shut down, but pressurized), a pipe break accident up to the largest pipe break can be accommodated within the nuclear safety operational criteria through the various operations of the MSIVs, Emergency

Core Cooling Systems (HPCF, ADS, RHR-LPFL, RCIC), Leak Detection and Isolation System, Standby Gas Treatment System, main control room heating, cooling and ventilation system, plant protection system (RHR heat exchangers) and the Nuclear Boiler Instrumentation System. For small pipe breaks inside the containment, pressure relief is effected by the nuclear system pressure relief system, which transfers decay heat to the suppression pool. For large breaks, depressurization takes place through the break itself. In State D (reactor not shut down, but pressurized), the same equipment is required as in State C but, in addition, the Reactor Protection System and the FMCRD System must operate to scram the reactor. The limiting items, on which the operation of the above equipment is based, are the allowable fuel cladding temperature and the containment pressure capability. The FMCRD housing supports are considered necessary whenever the system is pressurized to prevent excessive control rod movement through the bottom of the reactor pressure vessel following the postulated rupture of one FMCRD housing (a lesser case of the design basis LOCA and a related preventive of a postulated rod ejection accident).

After completion of the automatic action of the above equipment, manual operation of the RHR (suppression pool, drywell and wetwell cooling modes) and ADS or relief valves operation (controlled depressurization) may be required to maintain containment pressure and fuel cladding temperature within limits during extended core cooling.

Event 33—Loss-of-Coolant Accidents (LOCA) Resulting from Postulated Pipe Breaks—Outside Primary Containment

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

The protection sequences for the various possible pipe breaks outside the containment are shown in Figures 15A-39 and 15A-40. The sequences also show that for small breaks (breaks not requiring immediate action), the reactor operator can use a large number of process indications to identify the break and isolate it.

In Operating State D (reactor not shut down, but pressurized), scram is accomplished through operation of the Reactor Protection System and the FMCRD System. Reactor vessel isolation is accomplished through operation of the main steamline isolation valves and the Leak Detection and Isolation System.

For a main steamline break, initial core cooling is accomplished by either the HPCF or RCIC, or the Automatic Depressurization System (ADS) or manual relief valve operation in conjunction with RHR-LPFL. These systems provide parallel paths to effect initial core cooling, thereby satisfying the single-failure criterion. Extended core cooling is accomplished by the single-failure proof, parallel combination of HPCF and RHR LPFL Systems. The ADS or relief valve system operation and the RHR suppression pool cooling, wetwell and drywell spray modes are required to maintain containment temperature, pressure, and fuel cladding

temperature within limits during extended core cooling. Subsequent to isolation of the break and depressurization of the vessel, RHR shutdown cooling mode may be operated for long term decay heat removal from the core.

Event 34—Gaseous Radwaste System Leak or Failure

It is assumed that the line leading to the steam jet air ejector fails near the main condenser. This results in activity normally processed by the Offgas Treatment System being discharged directly to the Turbine Building and subsequently through the ventilation system to the environment. This failure results in a loss-of-flow signal to the Offgas System. This event is applicable only in States A, B, C and D, and is shown in Figure 15A-41.

The reactor operator initiates a normal shutdown of the reactor to reduce the gaseous activity being discharged. A loss of main condenser vacuum will result (timing dependent on leak rate) in a main turbine trip, a vessel isolation that terminates the steam and activity outflow from the reactor, and ultimately a reactor shutdown. Refer to Event 20 for reactor protection sequence (Figure 15A-25).

Event 35—Augmented Offgas Treatment System Failure

An evaluation of those events which could cause a gross failure in the Offgas System has resulted in the identification of a postulated seismic event, more severe than the one for which the system is designed, as the only conceivable event which could cause significant damage.

The detected gross failure of this system will result in manual isolation of this system from the main condenser. The isolation results in high main condenser pressure and ultimately a main turbine trip and associated reactor scram and vessel isolation (that terminates the steam and activity discharge from the vessel). Protective sequences for the event are shown in Figure 15A-42. The loss of vacuum in the main condenser transient has been analyzed in Event 20 (Figure 15A-25).

Event 36—Liquid Radwaste Leak or Failure

Releases which could occur inside and outside of the containment, not covered by Events 28, 29, 30, 33, 35 and 36, include small spills and equipment leaks of radioactive materials inside structures housing the subject process equipment. Conservative values for leakage have been assumed and evaluated in the plant under routine releases. The offsite dose that results from any small spill which could occur outside containment is negligible in comparison to the dose resulting from the accountable (expected) plant leakages. The protective sequences for this event are presented in Figure 15A-43.

Event 37—Liquid Radwaste System—Storage Tank Failure

An unspecified event causes the complete release of the average radioactivity inventory in the storage tank containing the largest quantities of significant radionuclides from the Liquid Radwaste System. This is assumed to be one of the concentrator waste tanks in the Radwaste Building. The airborne radioactivity released during the accident passes directly to the environment via the Radwaste Building vent.

The postulated events that could cause release of the radioactive inventory of the concentrator waste tank include cracks in the vessels and operator error. The possibility of small cracks and consequent low-level release rates receives primary consideration in system and component design. The concentrator waste tank is designed to operate at atmospheric pressure and 93.3^{o}C maximum temperature so the possibility of failure is considered small. A liquid radwaste release caused by operator error is also considered a remote possibility. Operating techniques and administrative procedures emphasize detailed system and equipment operating instruction. A positive action interlock system is provided to prevent inadvertent opening of a drain valve. Should a release of liquid radioactive wastes occur, floor drain sump pumps in the floor of the Radwaste Building will receive a high water level alarm, activate automatically and remove the spilled liquid to a contained storage tank. The protective sequences for this event are presented in Figure 15A-44.

Event 41—Trip of All Reactor Internal Pumps (RIPs)

This event is not applicable in States A and B because the reactor vessel head is off and the RIPs normally would not be in use. The trip could occur in States C and D. A trip of all RIPs results in a scram and may cause a high water level trip of the main turbine and the feedpump turbines. Figure 15A-48 provides the protection sequence for this event. A simultaneous trip of all RIPs may cause some fuel cladding heatup due to momentary transition boiling. The cladding heatup is insignificant, its temperature is below 1204°C, the fuel enthalpy is lower than 1.17 kJ/g and event consequences are acceptable.

Event 42—Loss of Shutdown Cooling

Loss of shutdown cooling is applicable in States A, B, C and D, during normal shutdown and cooldown. Because each of the three RHR loops may be lined up independently in the shutdown cooling mode, a simultaneous loss of all three loops is not a credible event and therefore no protection sequence is required as shown in Figure 15A-49.

Event 46—Pressure Regulator Failure—Closure of All Turbine Control and Bypass Valves

A pressure regulator failure in the close direction (or downscale), causing the closing of all turbine control and bypass valves, applies only in operating States C and D because in other states the pressure regulator is not in operation. The protection sequence shown on Figure 15A-53 includes a high neutron flux scram by the Neutron Monitoring, Reactor Protection and FMCRD Systems, a high pressure trip of four RIPs, pressure relief and core and containment cooling.

Event 51—Reactor Internal Pump (RIP) Seizure

An RIP seizure event considers the instantaneous stoppage of the pump motor shaft of one RIP. The case involves operation at design power in State D. Because a seizure of one out of ten RIPs produces a flow disturbance of less than 10%, consequences of a RIP seizure are mild and no scram occurs. Therefore, normal operation may continue and no protection sequence is required as shown in Figure 15A-58.

Event 52—Reactor Internal Pump (RIP) Shaft Break

An RIP shaft break event considers the degraded, delayed stoppage of the pump motor shaft of one RIP. The case involves operation at design power in State D. The consequences of this event are bounded by Event 51—RIP Seizure. Normal operation may continue and no protection sequence is required as shown in Figure 15A-59.

15A.6.6 Special Events

15A.6.6.1 General

Additional special events are postulated to demonstrate that the plant is capable of accommodating off-design occurrences (Events 53 through 56). As such, these events are beyond the safety requirements of the other event categories. The safety actions shown on the sequence diagrams (Figures 15A-60 through 15A-63) for the additional special events follow directly from the requirements cited in the demonstration of the plant capability.

Auxiliary system support analyses are shown in Figures 15A-6 and 15A-7, and 15A-65 through 15A-70.

15A.6.6.2 Required Safety Action/Unacceptable Consequences

Table 15A-15 relates the safety actions for special events to demonstrate the capabilities cited in Table 15A-5.

15A.6.6.3 Event Definitions and Operational Safety Evaluation

Event 53—Shipping Cask Drop and Spent Fuel Cask Drop Accident

Due to the redundant nature of the crane, the cask drop accident is not a credible accident. However, the accident is assumed to occur as a consequence of an unspecified failure of the cask lifting mechanism, thereby allowing the cask to fall from the level of the refueling floor to ground level through the refueling floor maintenance hatch.

The largest size of BWR fuel cask is conservatively assumed to be dropped approximately 29 m from the refueling floor level to ground level on transport from the decontamination pit out of the Reactor Building. Some of the coolant in the outer cask structure may leak from the cask.

The reactor operator ascertains the degree of cask damage and, if possible, makes the necessary repairs and refill the cask coolant to its normal level if coolant has been lost.

It is assumed that if the coolant is lost from the external cask shield, the operator establishes forced cooling of the cask by introducing water into the outer structure annulus or by spraying water on the cask exterior surface. Maintaining the cask in a cool condition therefore ensures no fuel damage as a result of a temperature increase due to decay heat.

Because the cask is still within the Reactor Building volume, any activity postulated to be released can be accommodated by the secondary containment and Standby Gas Treatment

System. The protective sequences for this event are provided in Figure 15A-60.

Event 54—Reactor Shutdown—ATWS

This event is applicable in States B, C and D. Figure 15A-61 shows the protection sequence for this extremely improbable and demanding event in each operating state.

State D is the most limiting case. Upon initiation of the plant transient situation (MSIV closure), a scram is initiated. The scram using hydraulic force is assumed to fail. However, the control rods can still be moved by the electric motors. This FMCRD insertion is sufficient to shut down a reactor. The reactor internal pumps are tripped; a trip of 4 RIPs on high pressure or turbine trip signals (or at Level 3) and a trip of 6 RIPs at Level 2. These trips cause a power decrease if the vessel becomes isolated from the main condenser, reactor power can be transferred from the reactor to the suppression pool via the relief valves. The Nuclear Boiler Instrumentation System initiates operation of the RCIC and HPCF Systems on low water level, which maintains reactor vessel water level. The Standby Liquid Control System is manually initiated and the transition from low reactor power to decay heat occurs. The RHR suppression pool cooling, and drywell and wetwell spray modes are used to remove the reactor power and decay heat from the suppression pool and primary containment as required. When RPV pressure falls to 0.689 to 1.38 MPaG level, the RHR shutdown cooling mode is started and continued until reaching cold shutdown.

Event 55—Reactor Shutdown from Outside Main Control Room

Reactor shutdown from outside the main control room is an event investigated to evaluate the capability of the plant to be safely shutdown and cooled to the cold shutdown state from outside the main control room. The event is applicable in any operating States A, B, C and D.

Figure 15A-62 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. In State C, only cooldown is required, since the reactor is already shutdown.

A scram from outside the main control room can be achieved by opening the AC supply breakers for the Reactor Protection System. If the nuclear system becomes isolated from the main condenser, decay heat is transferred from the reactor to the suppression pool via the relief valves. The Nuclear Boiler Instrumentation System initiates the operation of the RCIC and HPCF Systems on low water level which maintains reactor vessel water level, and the RHR suppression pool cooling mode is used to remove the decay heat from the suppression pool if required. When reactor pressure falls below the shutdown cooling interlock pressure, the RHR shutdown cooling mode is started.

Event 56—Reactor Shutdown Without Control Rods

Reactor shutdown without control rods is an event requiring an alternate method of reactivity control—the Standby Liquid Control System (SLCS). By definition, this event can occur only

when the reactor is not already shutdown. Therefore, this event is considered only in operating States B and D.

The SLCS must operate to avoid unacceptable consequence criteria 5-3. The design bases for the SLCS result from these operating criteria when applied under the most severe conditions (State D at rated power). As indicated in Figure 15A-63, the SLCS is manually initiated and controlled in States B and D.

15A.7 Remainder of NSOA

With the information presented in the protection sequence block diagrams, the auxiliary diagrams and the commonality of auxiliary diagrams, it is possible to determine the exact functional and hardware requirements of each system. This is done by considering each event in which the system is employed and deriving a limiting set of operational requirements. This limiting set of operational requirements establishes the lowest acceptable level of performance for a system or component, or the minimum number of components or portions of a system that must be operable in order that plant operation may continue.

The operational requirements derived using this process may be complicated functions of operating states, parameter ranges, and hardware conditions. The final step is to simplify these complex requirements into technical specifications that encompass the operational requirements that can be used by plant operations and management personnel.

15A.8 Conclusions

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

Table 15A-1 Unacceptable Consequences Criteria Plant Event Category: Normal Operation

Unacceptable Consequences
1-1 Release of radioactive material to the environs that exceed the limits of either 10CFR20 or 10CFR50.
1-2 Fuel failure to such an extent that were the freed fission products released to the environs via the normal discharge paths for radioactive material, the limits of 10CFR20 would be exceeded.
1-3 Nuclear system stress in excess of that allowed for planned operation by applicable industry codes.
1-4 Existence of a plant condition not considered by plant safety analyses.

Table 15A-2 Unacceptable Consequences Criteria Plant Event Category: Moderate Frequency Incidents (Anticipated Operational Transients)

Unacceptable Consequences
2-1 Release of radioactive material to the environs that exceed the limits of 10CFR20.
2-2 Reactor operation induced fuel cladding failure.
2-3 Nuclear system stress exceeding that allowed for transients by applicable industry codes.
2-4 Containment stresses exceeding that allowed for transients by applicable industry codes.

Table 15A-3 Unacceptable Consequences Criteria Plant Event Category: Infrequent Incidents (Abnormal Operational Transients)

Unacceptable Consequences
3-1 Radioactive material release exceeding of a small fraction of 10CFR100.
3-2 Fuel damage that would preclude resumption of normal operation after a normal restart.
3-3 Generation of a condition that results in consequential loss of function of the reactor coolant system.
3-4 Generation of a condition that results in a consequential loss of function of a necessary containment barrier.

Table 15A-4 Unacceptable Consequences Criteria Plant Event Category: Limiting Faults (Design Basis Accidents)

Unacceptable Consequences
4-1 Radioactive material release exceeding the guideline values of 10CFR100.
4-2 Failure of the fuel barrier which would cause changes in core geometry such that core cooling would be inhibited.
4-3 Nuclear system stresses exceeding that allowed for transients by applicable industry codes.
4-4 Containment stresses exceeding that allowed for transients by applicable industry codes when containment is required.
4-5 Overexposure to radiation of plant main control room personnel (in excess of 0.05 Sv whole body, 0.3 Sv inhalation and 0.75 Sv skin).

Table 15A-5 Capability Consequences Plant Event Category: Special Events

Special Events Considered
A. Reactor shutdown from outside control room.
B. Reactor shutdown without control rods.
C. Reactor shutdown with anticipated transient without scram (ATWS).
D. Shipping Cask Drop.
Capability Demonstration
5-1 Ability to shut down reactor by manipulating controls and equipment outside the main control room
5-2 Ability to bring the reactor to the cold shutdown condition from outside the main control room.
5-3 Ability to shut down the reactor independent of control rods.
5-4 Ability to contain radiological contamination.
5-5 Ability to limit radiological exposure

Table 15A-6 General Nuclear[3] Safety Operational Criteria

Applicability	Nuclear Safety Operation Criteria
Planned operation moderate frequency and infrequent incidents limiting faults and additional special plant capability events.	The plant shall be operated so as to avoid unacceptable consequences.
Moderate frequency and infrequent incidents and design basis accidents.	The plant shall be designed and operated in such a manner that no single active component failure can prevent (1) safety-related core activity control, (2) safety-related core and containment heat removal, (3) reactor coolant pressure boundary integrity, (4) safety-related containment isolation and (5) safety-related containment atmosphere control and cleanup.

Table 15A-7 ABWR Operating States*

	States			
Conditions	**A**	**B**	**C**	**D**
Reactor vessel head off	X	X		
Reactor vessel head on			X	X
Shutdown	X		X	
Not Shutdown		X		X
Definition				
Shutdown: K_{eff} sufficiently less than 1.0 such that the full withdrawal of one control rod pair (with the same HCU) or one control rod of maximum worth could not produce criticality under the most restrictive conditions of temperature, pressure, core age and fission product concentrations.				

* Further discussion is provided in Subsection 15A.6.2.4.

Table 15A-8 Normal Operation

NSOA Event No.	Event Description	NSOA Event Figure No	DCD Section No.	ABWR Operating State A	B	C	D
1	Refueling	15A-8	—	X			
2	Achieving Criticality	15A-8, 15A-9 15A-10, 15A-11	—	X	X	X	X
3	Heatup	15A-11	—				X
4	Power Operation—Electric Generation - Steady State - Daily Load Reduction and Recover—Grid Frequency Control Responses—Control Rod Sequence Exchanges - Power Generation Surveillance Testing • Turbine Control Valve Surveillance Tests • Turbine Stop Valve Surveillance Tests • MSIV Surveillance Tests	15A-11	—				X
5	Achieving Shutdown	15A-9, 15A-11			X		X
6	Cooldown	15A-8 15A-10		X		X	

Table 15A-9 Moderate Frequency Incidents (Anticipated Operational Transients)

NSOA Event No.	Event Description	NSOA Event Figure No	DCD Section No.	ABWR Operating State A	B	C	D
7	Manual or Inadvertent SCRAM	15A-12	7.2	X	X	X	X
8	Loss of Plant Instrument or Service Air System	15A-13	9.3.1	X	X	X	X
9	Recirculation Flow Control Failure—One RIP Runout	15A-14	15.4.5			X	X
10	Recirculation Flow Control Failure—One RIP Runback	15A-15	15.3.2			X	X
11	Three RIPs Trip	15A-16	15.3.1			X	X
12	All MSIV Closure	15A-17	15.2.4			X	X
13	One MSIV Closure	15A-18	15.2.4			X	X
14	Loss of All Feedwater Flow	15A-19	15.2.7			X	X
15	Loss of a Feedwater Heater	15A-20	15.1.1				X
16	Feedwater Controller Failure—Runout of One Feedwater Pump	15A-21	15.1.2	X	X	X	X
17	Pressure Regulator Failure—Opening of One Bypass Valve	15A-22	15.1.3			X	X
18	Pressure Regulator Failure—Closing of One Control Valve	15A-23	15.2.1			X	X
19	Main Turbine Trip with Bypass System Operational	15A-24	15.2.3				X
20	Loss of Main Condenser Vacuum	15A-25	15.2.5			X	X
21	Generator Load Rejection with Bypass System Operational	15A-26	15.2.2				X
22	Loss of AC Power (Unit Auxiliary Transformer)	15A-27	15.2.6			X	X
23	Inadvertent Startup of HPCF Pump	15A-28	15.5.1	X	X	X	X
24	Inadvertent Opening of a Safety Relief Valve	15A-29	15.1.4			X	X
26*	Main Turbine Trip with One Bypass Valve Failure	15A-31	15.2.3				X
27*	Generator Load Rejection with One Bypass Valve Failure	15A-32	15.2.2				X

Table 15A-9 Moderate Frequency Incidents (Anticipated Operational Transients) (Continued)

NSOA Event No.	Event Description	NSOA Event Figure No	DCD Section No.	ABWR Operating State A	B	C	D
38*	Abnormal Startup of Idle System Reactor Internal Pump	15A-45	15.4.4	X	X	X	X
39*	Recirculation Flow Control Failure—All RIPs Runout	15A-46	15.4.5			X	X
40*	Recirculation Flow Control Failure—All RIPs Runback	15A-47	15.3.2			X	X
43	RHR Shutdown Cooling Increased Cooling	15A-50	15.1.6	X	X	X	X
44*	Feedwater Controller Failure Runout of Two Feedwater Pumps	15A-51	15.1.2	X	X	X	X
45*	Pressure Regulator Failure—Opening of all Bypass and Control Valves	15A-52	15.1.3			X	X
48*	Main Turbine Trip with Bypass Failure	15A-55	15.2.3				X
49*	Generator Load Rejection with Bypass Failure	15A-56	15.2.2				X

* This event should be classified as an infrequent event or a limiting fault. However, criteria for moderate frequent incidents are conservatively applied.

Table 15A-10 Infrequent Incidents (Abnormal Operational Transients)

NSOA Event No.	Event Description	NSOA Event Figure No.	DCD Section No.	ABWR Operating State A	B	C	D
24	Inadvertent Opening of a Safety/Relief Valve	15A-29	15.1.4			X	X
25	Control Rod Withdrawal Error—Startup and Refueling Operations	15A-30	15.4.1	X	X	X	X
50	Misplaced/Misoriented Fuel Bundle Accident	15A-57	15.4.7 15.4.8	X	X	X	X

Table 15A-11 Limiting Faults (Design Basis Accidents)

NSOA Event No.	Event Description	NSOA Event Figure No	DCD Section No.	ABWR Operating State A	B	C	D
28	Control Rod Ejection Accident	15A-33	15.4.9	X	X	X	X
29	Control Rod Drop Accident	15A-34	15.4.10	X	X	X	X
30	Control Rod Withdrawal Error—Power Operation	15A-35	15.4.2				X
31	Fuel-Handling Accident	15A-36	15.7.4	X	X	X	X
32	Loss-of-Coolant Accident Resulting from Spectrum of Postulated Piping Breaks Within the RCPB Inside Containment	15A-37 and 15A-38	15.6.5			X	X
33	Small, Large, Steam and Liquid Piping Breaks Outside Containment	15A-39 and 15A-40	15.6.2, 15.6.4, 15.6.6			X	X
34	Gaseous Radwaste System Leak or Failure	15A-41	15.7.1	X	X	X	X
35	Augmented Offgas Treatment System Failure	15A-42	15.7.1	X	X	X	X
36	Liquid Radwaste System Leak or Failure	15A-43	15.7.2	X	X	X	X
37	Liquid Radwaste System Storage Tank Failure	15A-44	15.7.3	X	X	X	X
41	Trip of All RIPs	15A-48	15.3.1			X	X
42	Loss of RHR Shutdown Cooling	15A-49	15.2.9	X	X	X	X
46	Pressure Regulator Failure—Closure of all Bypass and Control Valves	15A-53	15.2.1			X	X
51	Reactor Internal Pump Seizure	15A-58	15.3.3				X
52	Reactor Internal Pump Shaft Break	15A-59	15.3.4				X

Table 15A-12 Special Events

NSOA Event No.	Event Description	NSOA Event Figure No	DCD Section No.	ABWR Operating State A	B	C	D
53	Shipping Cask Drop Spent Radwaste Spent Fuel New Fuel	15A-60	15.7.5	X	X	X	X
54	Reactor Shutdown From Anticipated Transient Without SCRAM (ATWS)	15A-61	15.8	X	X	X	X
55	Reactor Shutdown From Outside Control Room	15A-62	7.5	X	X	X	X
56	Reactor Shutdown Without Control Rods	15A-63	9.3.5	X	X	X	X

Table 15A-13 Safety Actions for Infrequent Incidents

Safety Action	Related Unacceptable Consequences	Reason Action Required
Scram and/or trip of four RIPs	3-2 3-3	To limit gross core-wide fuel damage and to limit nuclear system pressure rise.
Pressure relief	3-3	To prevent excessive nuclear system pressure rise.
Core, suppression pool and containment cooling	3-2 3-4	To limit further fuel and containment damage in the event that normal cooling is interrupted.
Reactor vessel isolation	3-2	To limit further fuel damage by reducing the outflow of steam and water from the reactor vessel, thereby limiting the decrease in reactor vessel water level.
Restore AC power	3-2	To limit initial fuel damage by restoring AC power to systems essential to other safety actions.
Containment isolation	3-1	To limit radiological effects.

Table 15A-14 Safety Actions for Design Basis Accidents

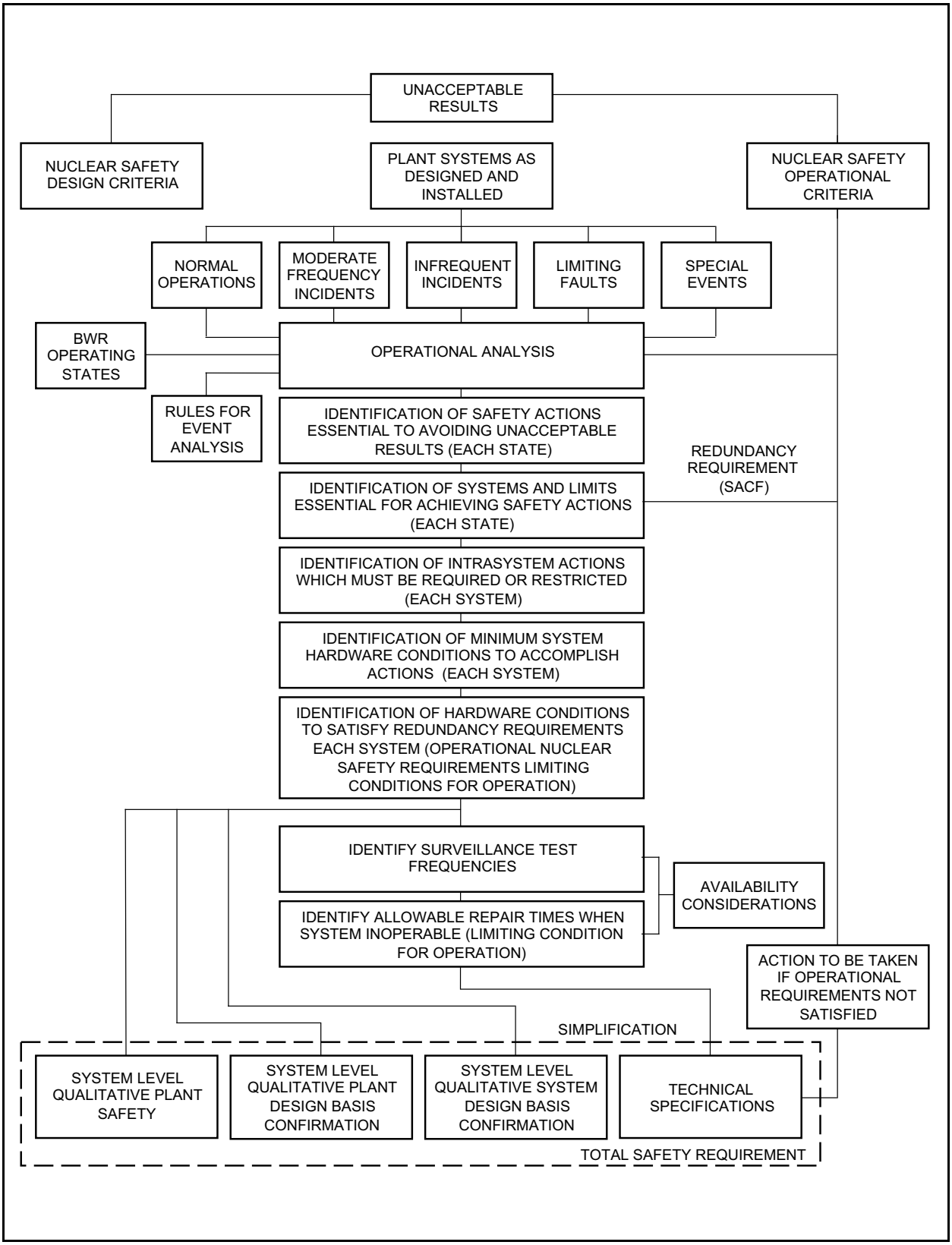
Safety Action	Related Unacceptable Consequences	Reason Action Required
Scram	4-2 4-3	To prevent fuel cladding failure* and excessive nuclear system pressures.
Pressure relief	4-3	To prevent excessive nuclear system pressure.
Core cooling	4-2	To prevent fuel cladding failure.
Reactor vessel isolation	4-1	To limit radiological effects to not exceed the guideline values of 10CFR100.
Containment isolation	4-1	To limit radiological effects to not exceed the guideline values of 10CFR100.
Containment cooling	4-4	To prevent excessive pressure in the containment when containment is required.
Stop rod ejection	4-2	To prevent fuel cladding failure.
Restrict loss of reactor coolant (passive)	4-2	To prevent fuel cladding failure.
Main Control Room environmental control	4-5	To prevent overexposure to radiation of plant personnel in the control room.
Limit reactivity insertion rate	4-2 4-3	To prevent fuel cladding failure and to prevent excessive nuclear system pressure.

* Failure of the fuel barrier includes fuel cladding fragmentation (LOCA) and excessive fuel enthalpy (CRDA).

Table 15A-15 Safety Actions for Special Events

Safety Action	Related Unacceptable Consequences	Reason Action Required
A. Main Control Room Considerations		
Manually initiate all shutdown controls from local panels	5-1 5-2	Local panel control has been provided and is available outside main control room.
Manually initiate SLCS	5-3	Standby Liquid Control System to control reactivity to assure cold shutdown is available.
B. Shipping Cask Considerations See Subsection 9.1.4		

Figure 15A-1 Block Diagram of Method Used to Derive Nuclear Safety Operational


UNACCEPTABLE RESULTS
NUCLEAR SAFETY DESIGN CRITERIA
PLANT SYSTEMS AS DESIGNED AND INSTALLED
NUCLEAR SAFETY OPERATIONAL CRITERIA
NORMAL OPERATIONS
MODERATE FREQUENCY INCIDENTS
INFREQUENT INCIDENTS
LIMITING FAULTS
SPECIAL EVENTS
BWR OPERATING STATES
OPERATIONAL ANALYSIS
RULES FOR EVENT ANALYSIS
IDENTIFICATION OF SAFETY ACTIONS ESSENTIAL TO AVOIDING UNACCEPTABLE RESULTS (EACH STATE)
REDUNDANCY REQUIREMENT (SACF)
IDENTIFICATION OF SYSTEMS AND LIMITS ESSENTIAL FOR ACHIEVING SAFETY ACTIONS (EACH STATE)
IDENTIFICATION OF INTRASYSTEM ACTIONS WHICH MUST BE REQUIRED OR RESTRICTED (EACH SYSTEM)
IDENTIFICATION OF MINIMUM SYSTEM HARDWARE CONDITIONS TO ACCOMPLISH ACTIONS (EACH SYSTEM)
IDENTIFICATION OF HARDWARE CONDITIONS TO SATISFY REDUNDANCY REQUIREMENTS EACH SYSTEM (OPERATIONAL NUCLEAR SAFETY REQUIREMENTS LIMITING CONDITIONS FOR OPERATION)
IDENTIFY SURVEILLANCE TEST FREQUENCIES
AVAILABILITY CONSIDERATIONS
IDENTIFY ALLOWABLE REPAIR TIMES WHEN SYSTEM INOPERABLE (LIMITING CONDITION FOR OPERATION)
ACTION TO BE TAKEN IF OPERATIONAL REQUIREMENTS NOT SATISFIED
SIMPLIFICATION
SYSTEM LEVEL QUALITATIVE PLANT SAFETY
SYSTEM LEVEL QUALITATIVE PLANT DESIGN BASIS CONFIRMATION
SYSTEM LEVEL QUALITATIVE SYSTEM DESIGN BASIS CONFIRMATION
TECHNICAL SPECIFICATIONS
TOTAL SAFETY REQUIREMENT

Requirements System-Level Qualitative Design Basis Confirmation Audits and Technical Specifications

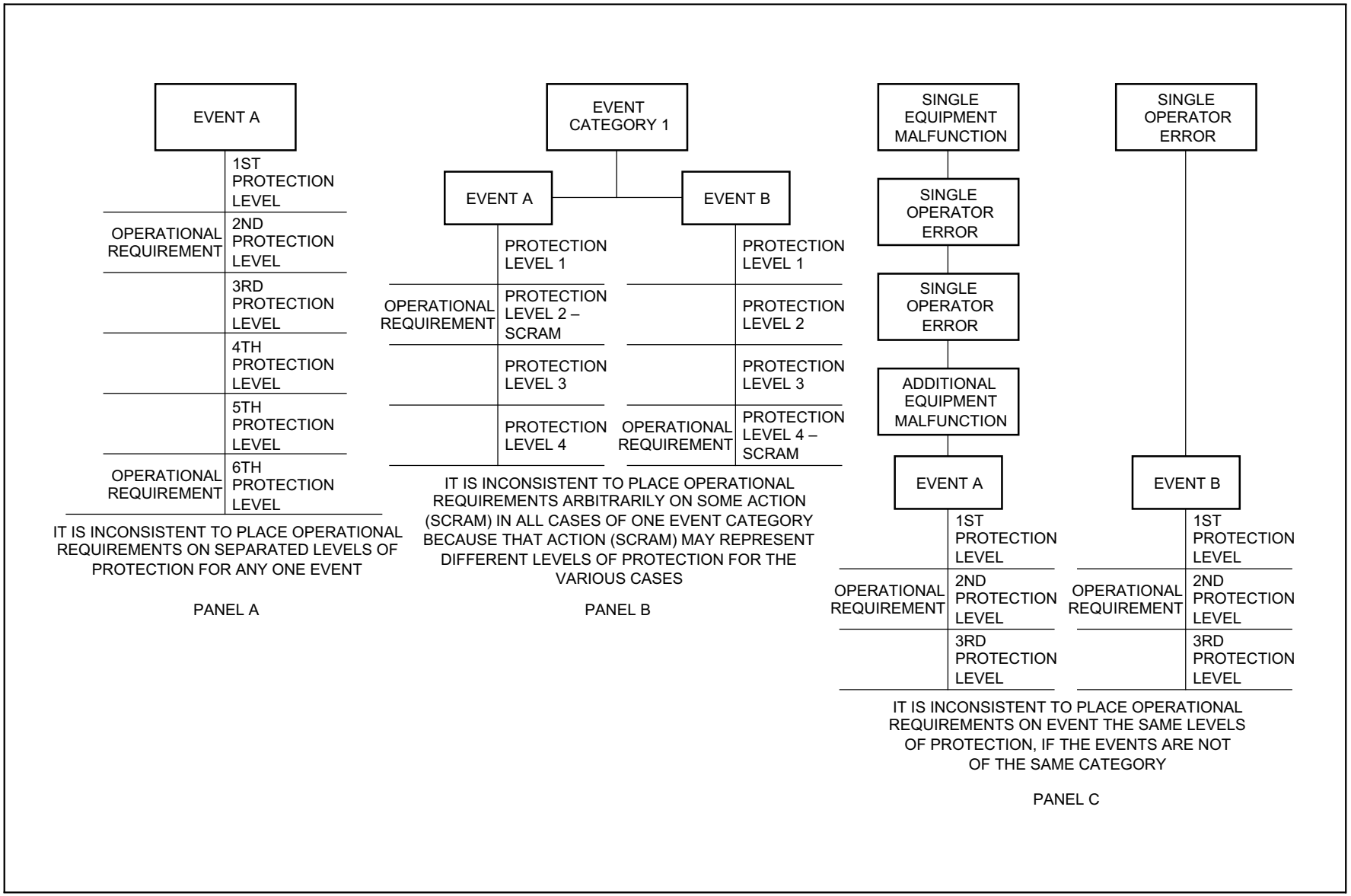


Figure 15A-2 Possible Inconsistencies in the Selection of Nuclear Safety Operational Requirements

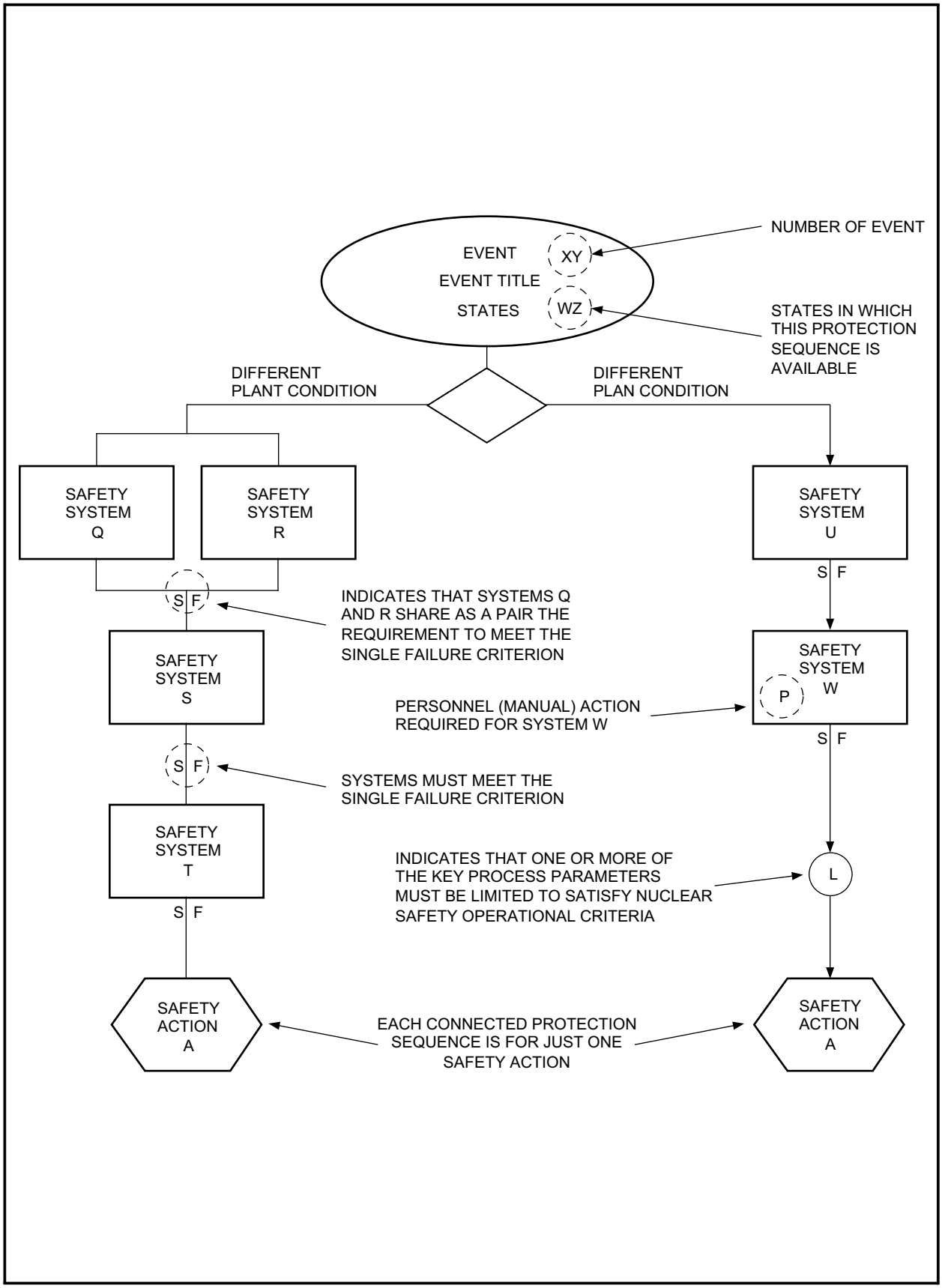


Figure 15A-3 Format for Protection Sequence Diagrams

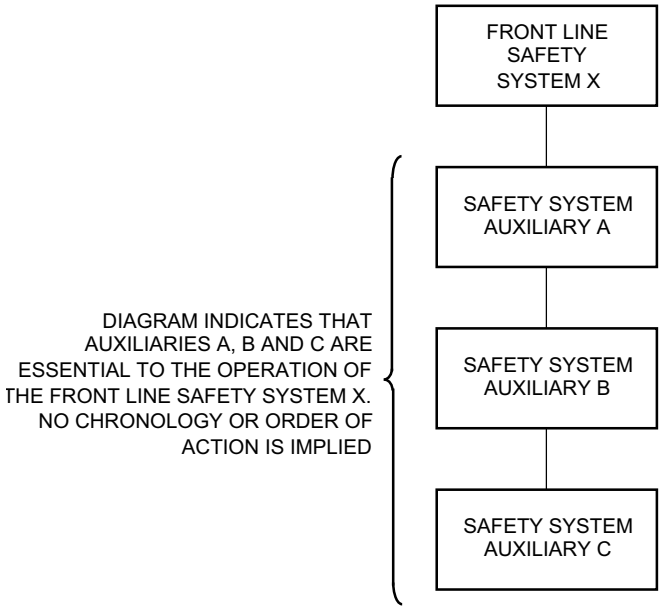


Figure 15A-4 Format for Safety System Auxiliary Diagrams

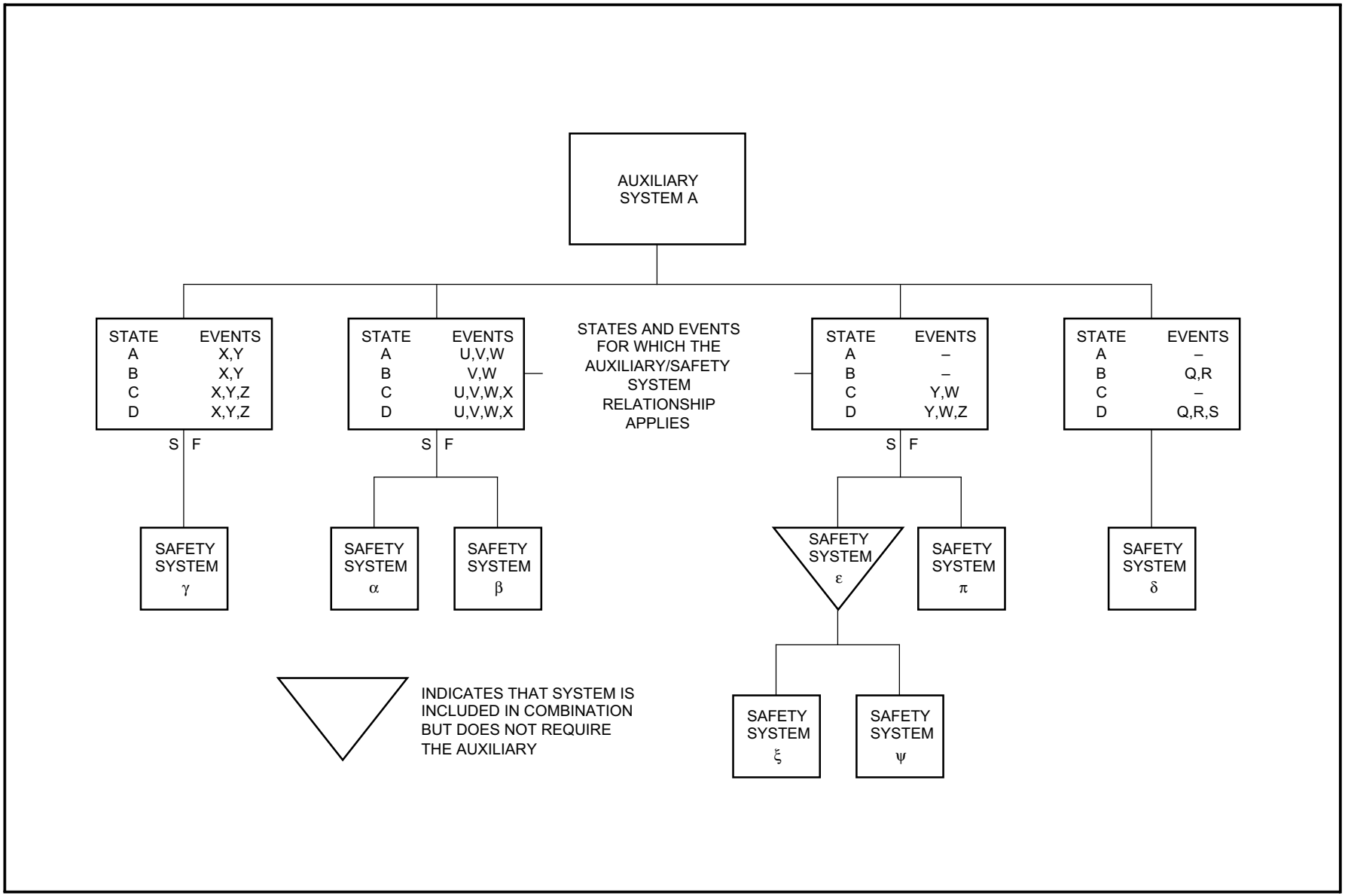


Figure 15A-5 Format for Commonality of Auxiliary Diagrams

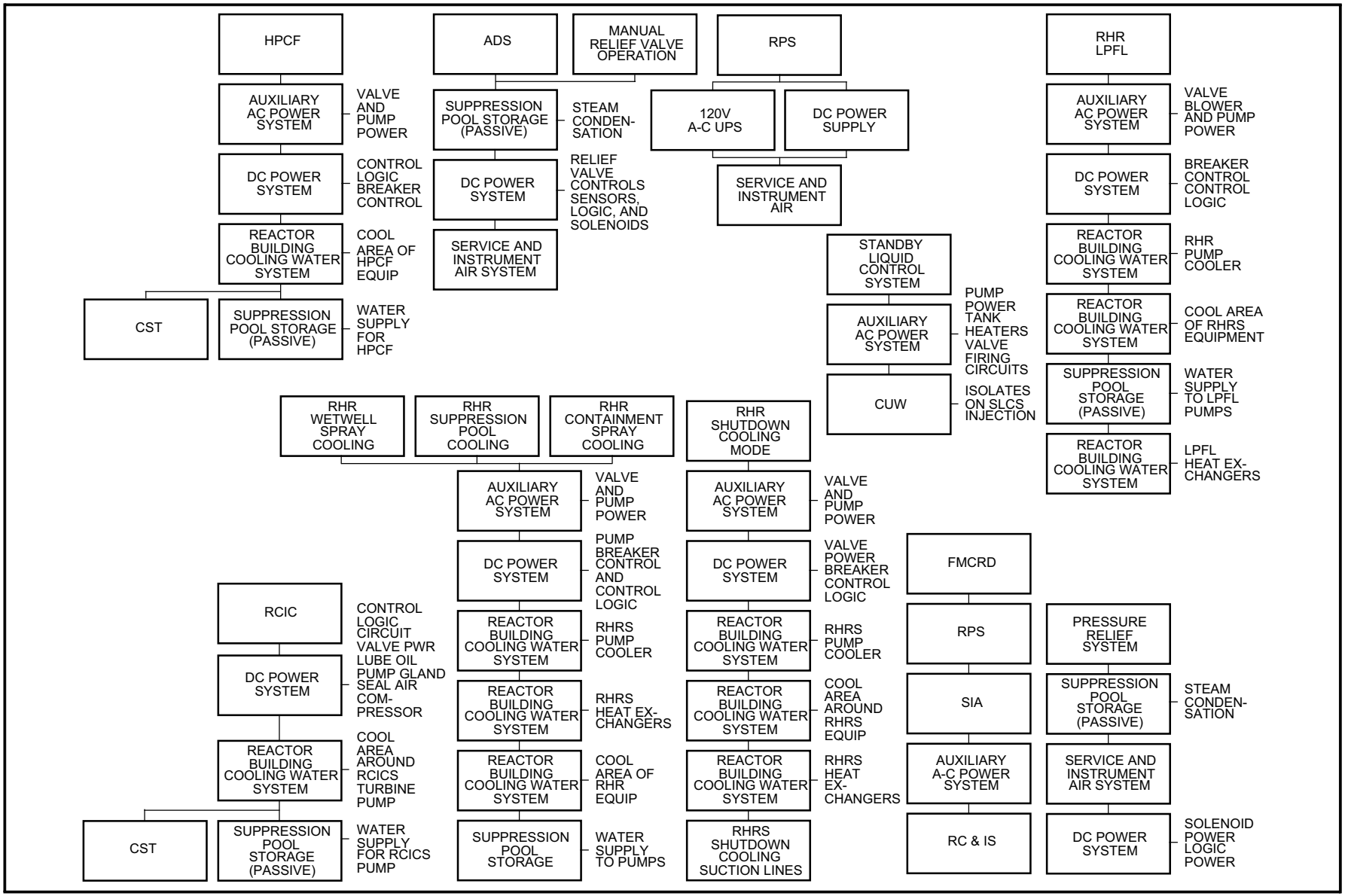


Figure 15A-6 Safety System Auxiliaries — Group 1

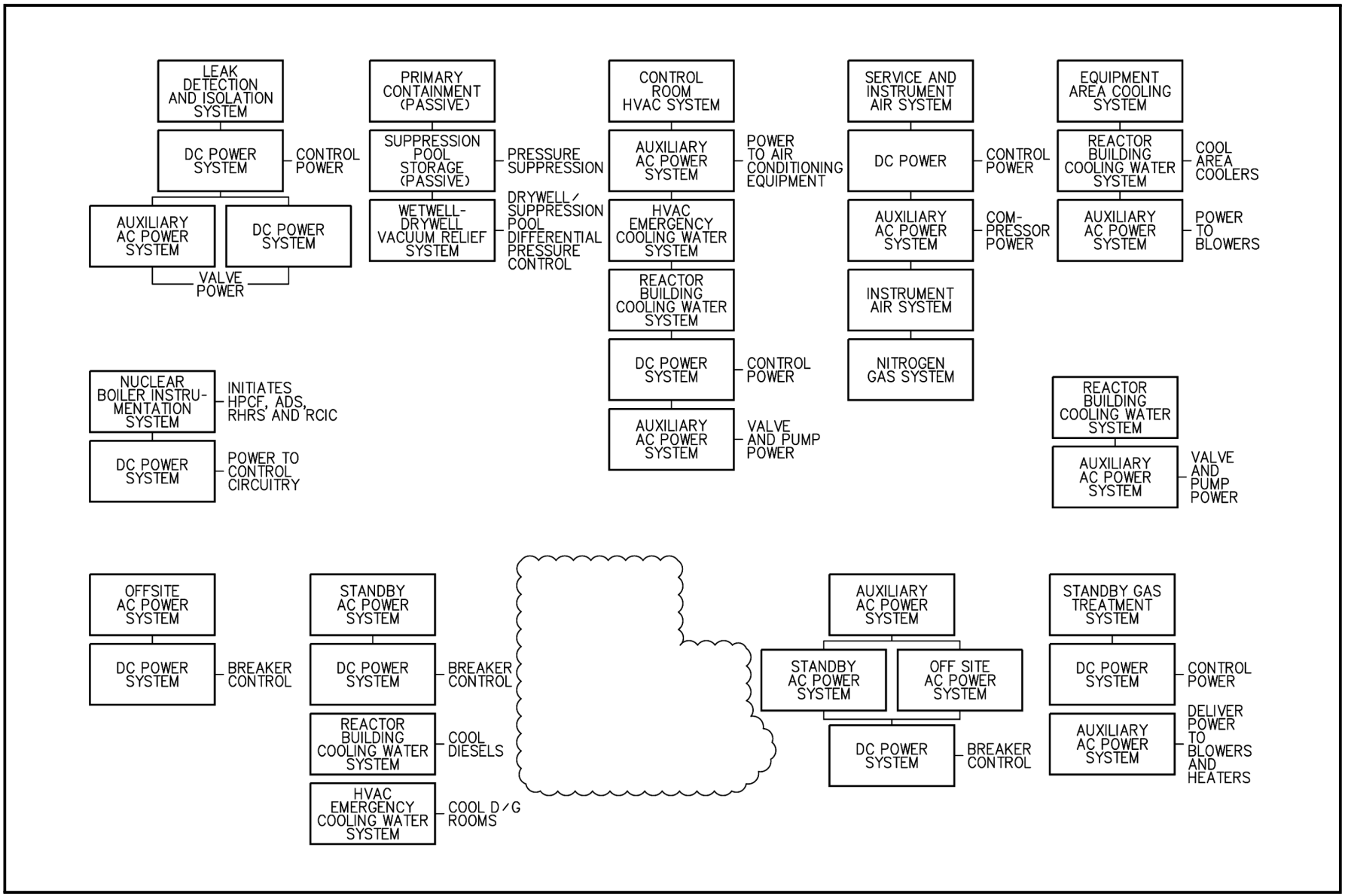


Figure 15A-7 Safety System Auxiliaries — Group 2

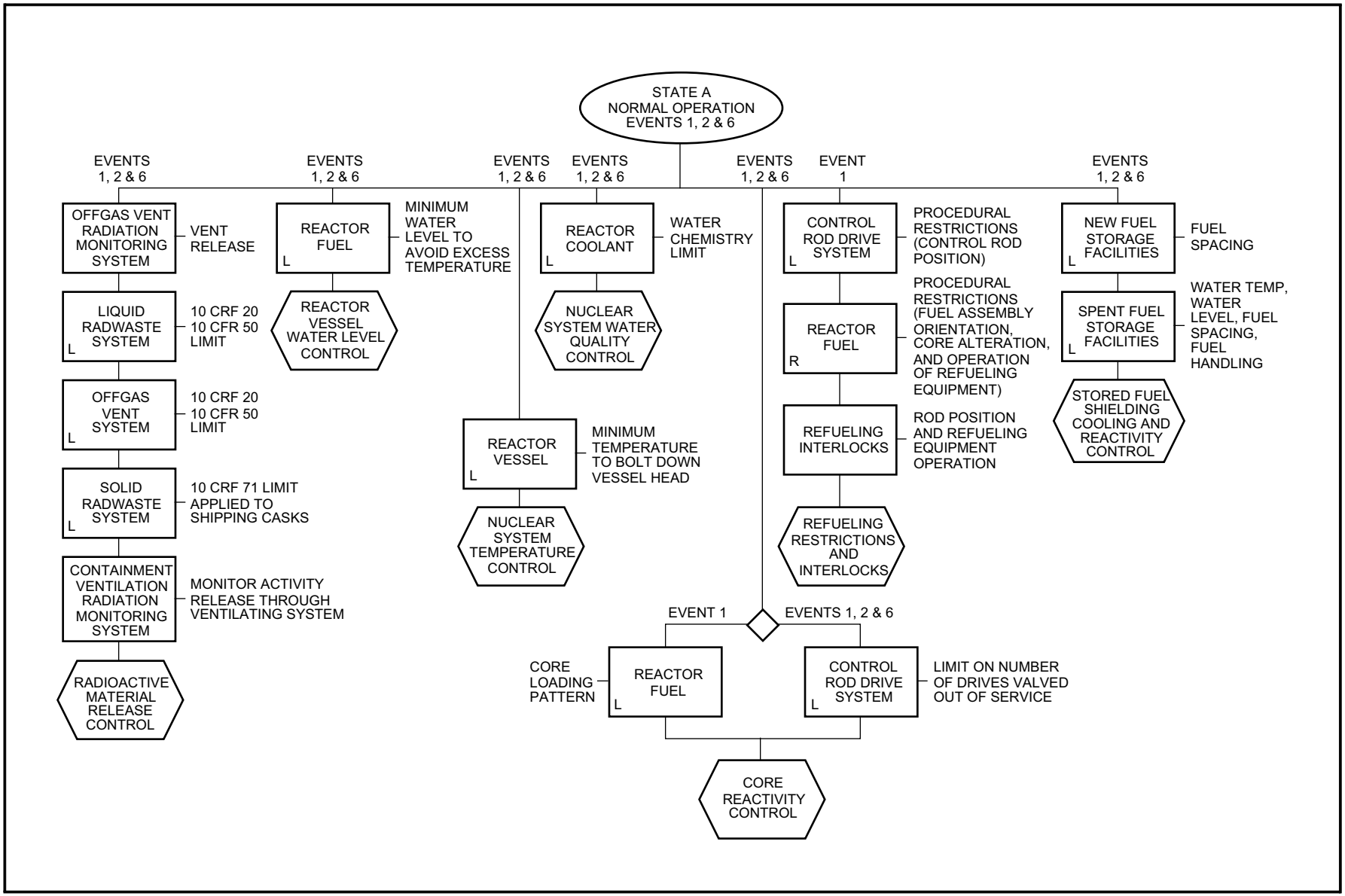


Figure 15A-8 Safety Action Sequences for Normal Operation in State A

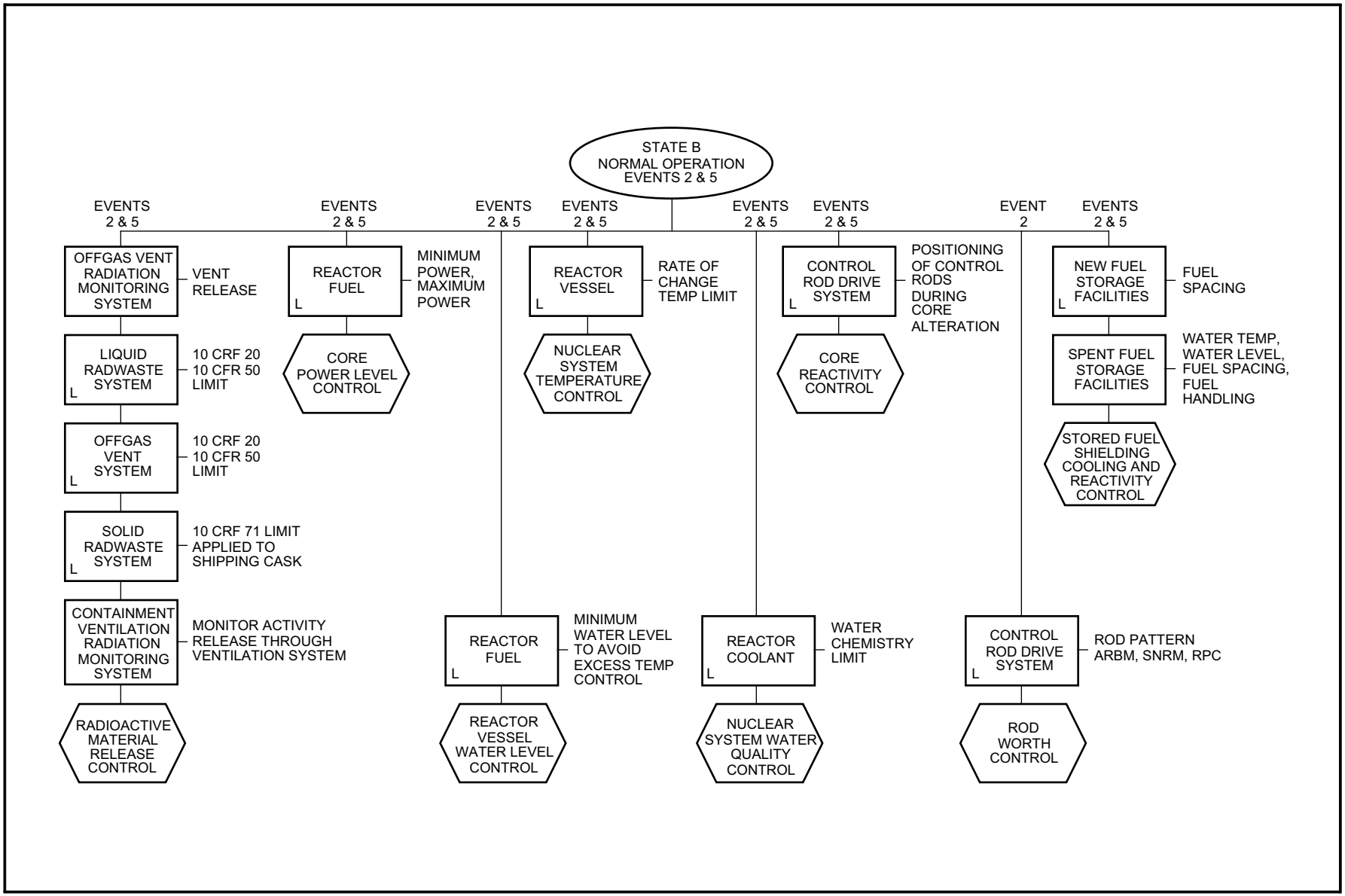


Figure 15A-9 Safety Action Sequences for Normal Operation in State B

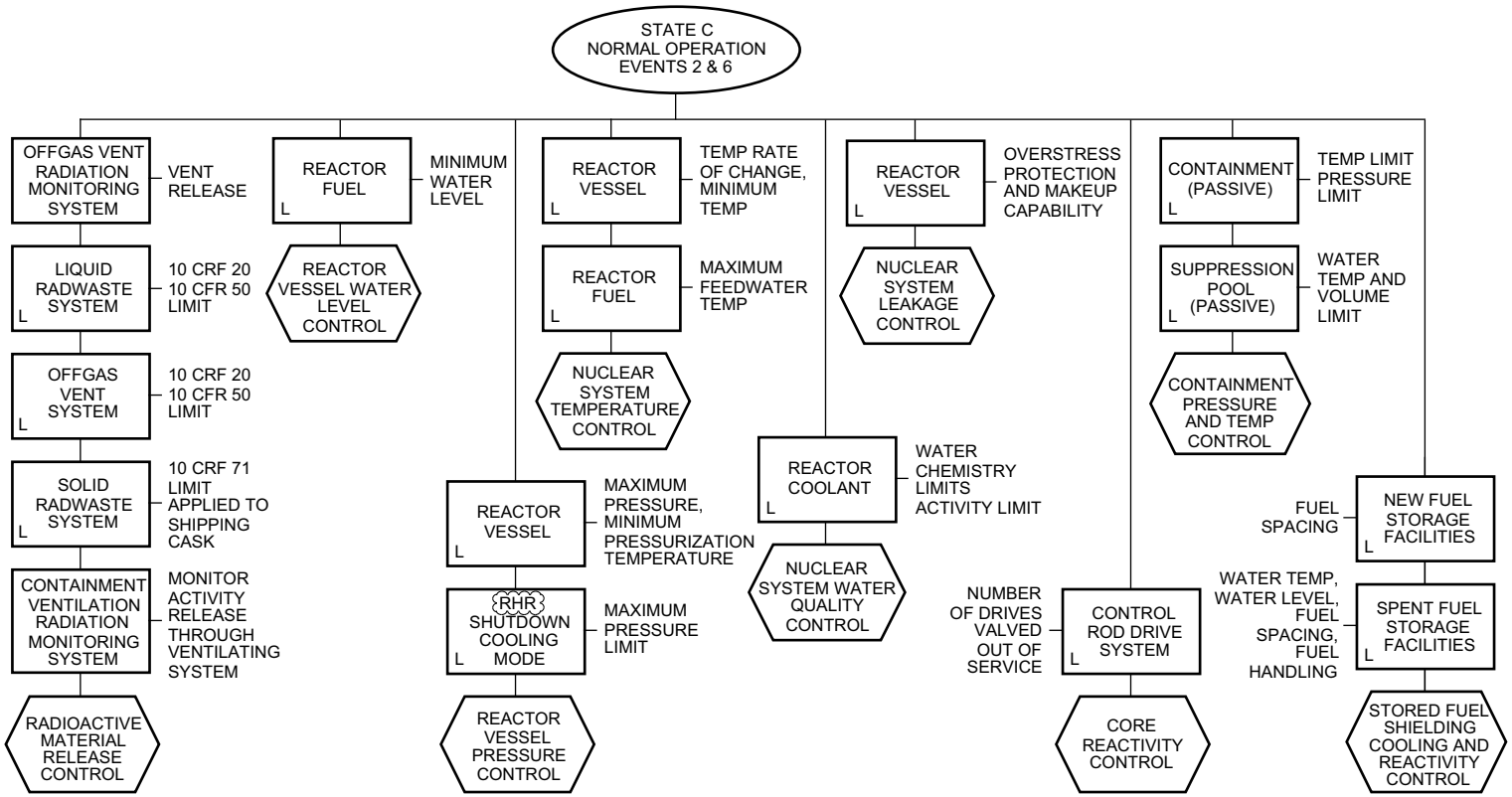


Figure 15A-10 Safety Action Sequences for Normal Operation in State C

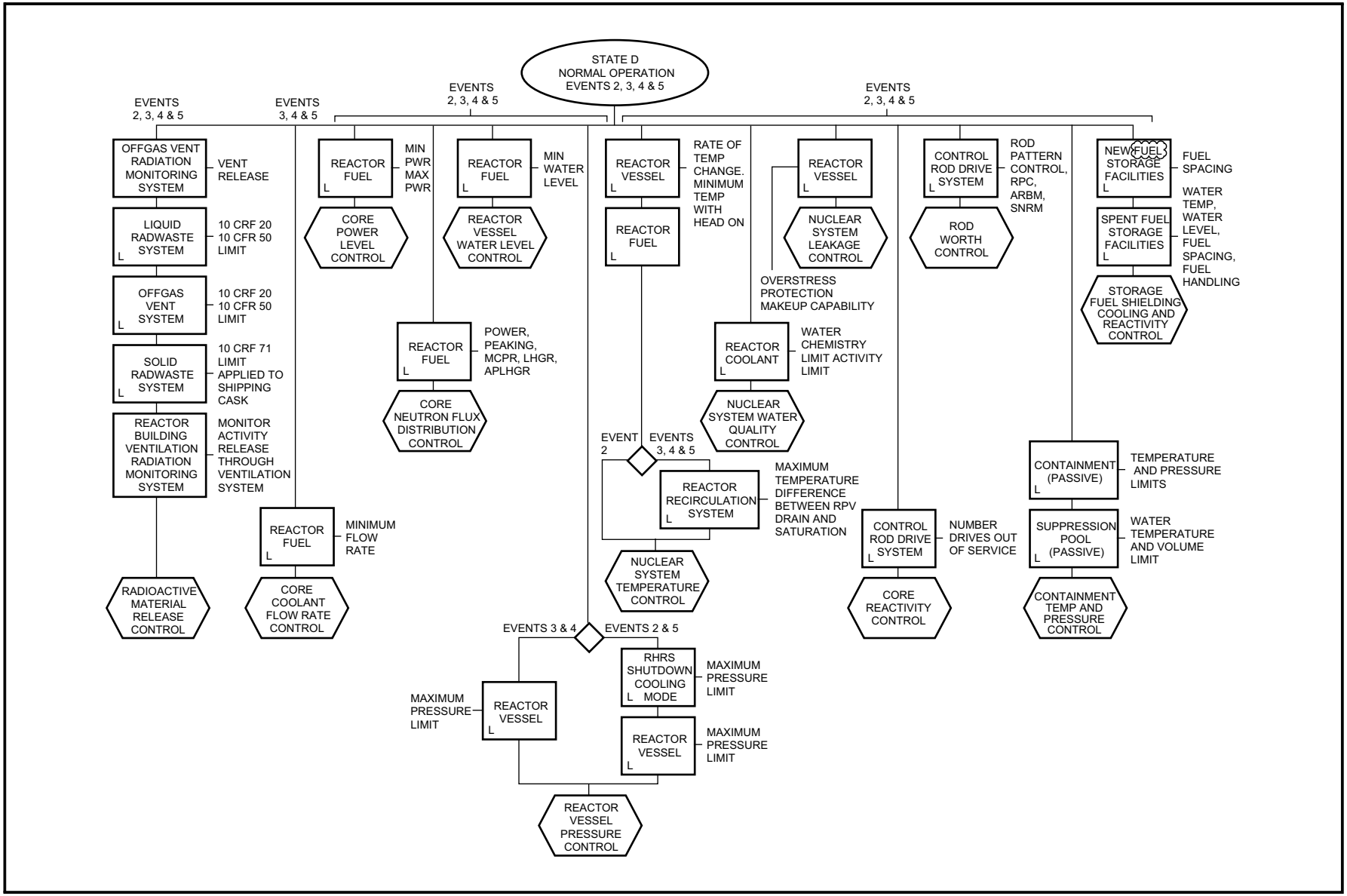


Figure 15A-11 Safety Action Sequences for Normal Operation in State D

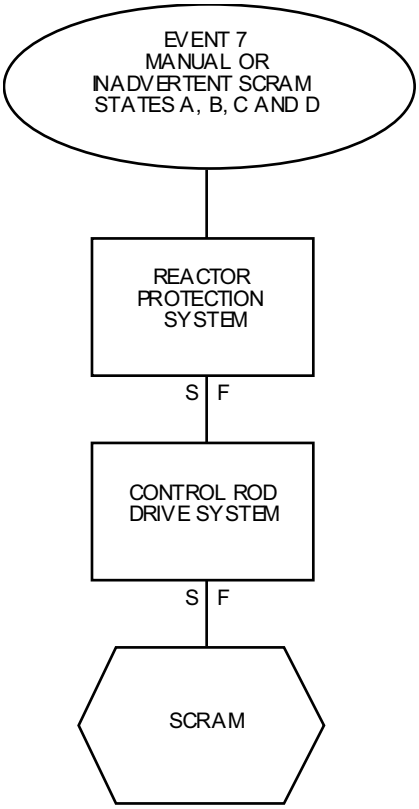


Figure 15A-12 Protection Sequence for Manual or Inadvertent Scram

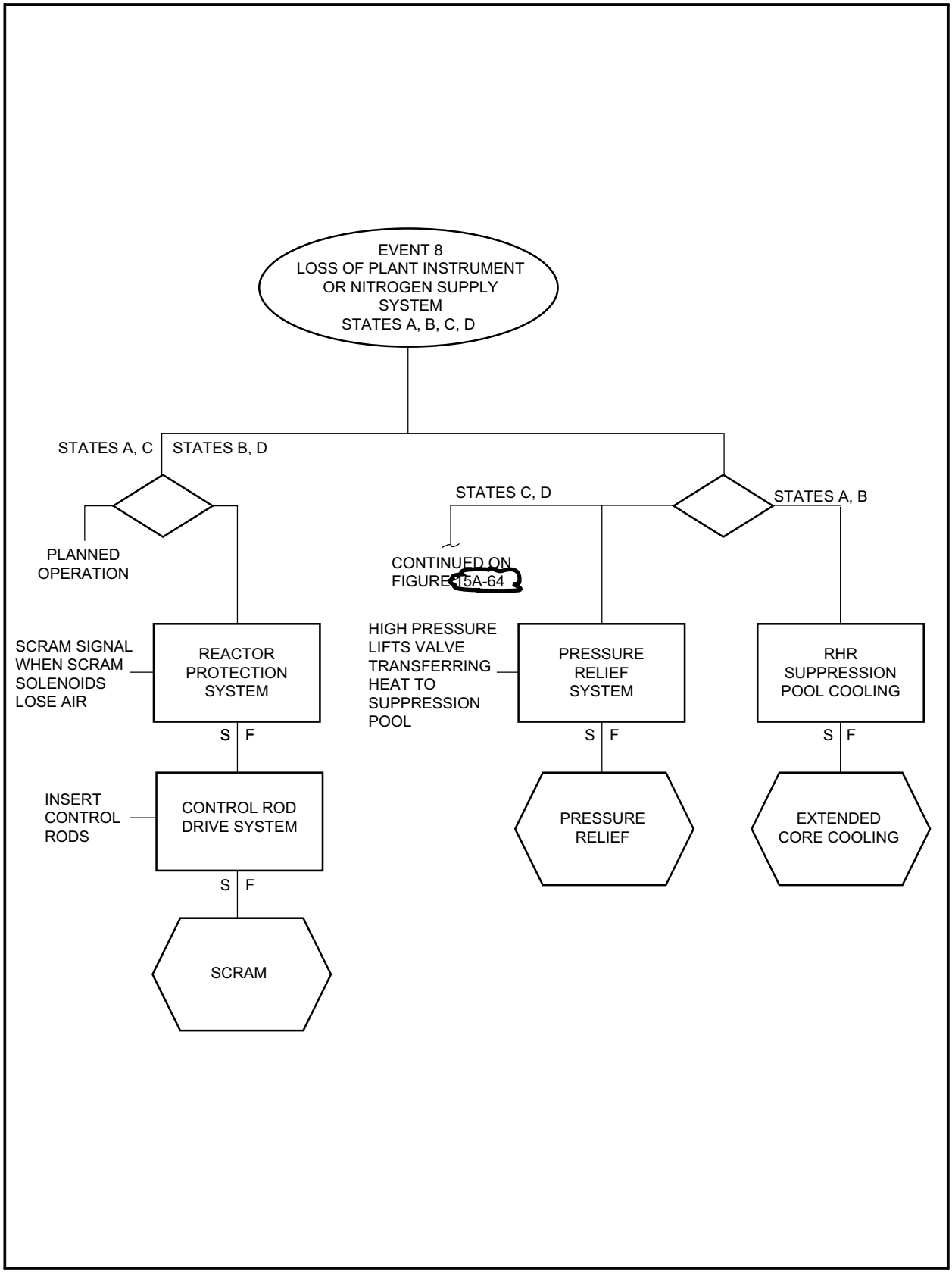


Figure 15A-13 Protection Sequence for Loss of Plant Instrument or Service Air System

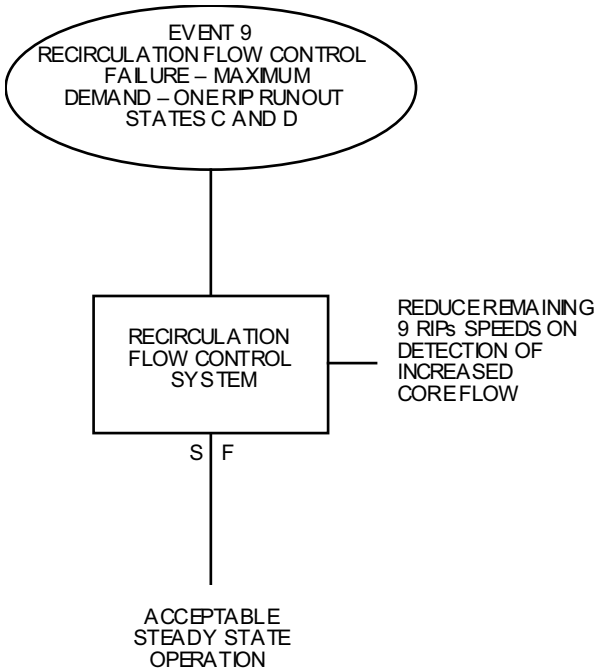


Figure 15A-14 Protection Sequence for Recirculation Flow Control Failure—Maximum Demand—One Reactor Internal Pump (RIP) Runout

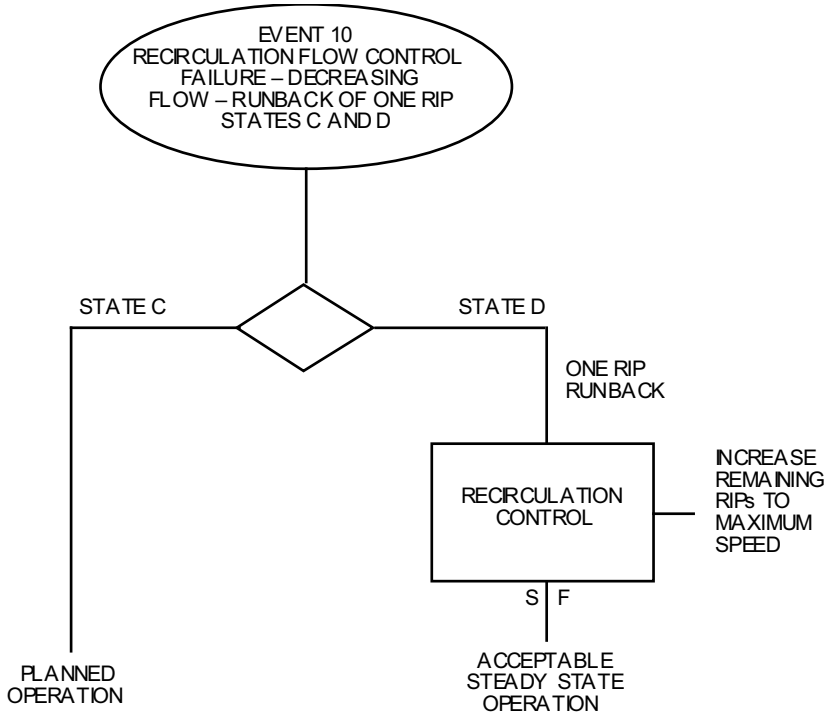


Figure 15A-15 Protection Sequence for Recirculation Flow Control Failure—Decreasing Flow Runback of One Reactor Internal Pump (RIP)

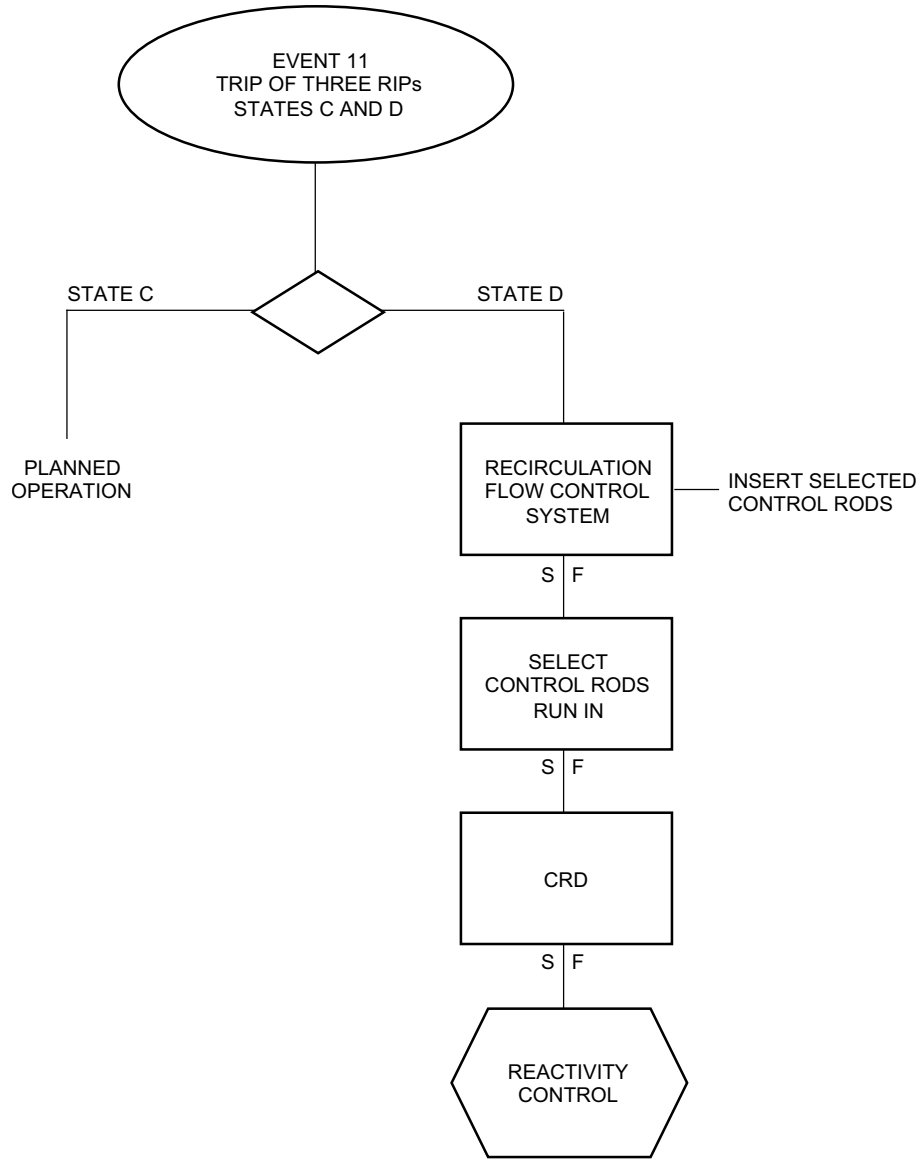


Figure 15A-16 Protection Sequence for Trip of Three Reactor Internal Pumps (RIPs)

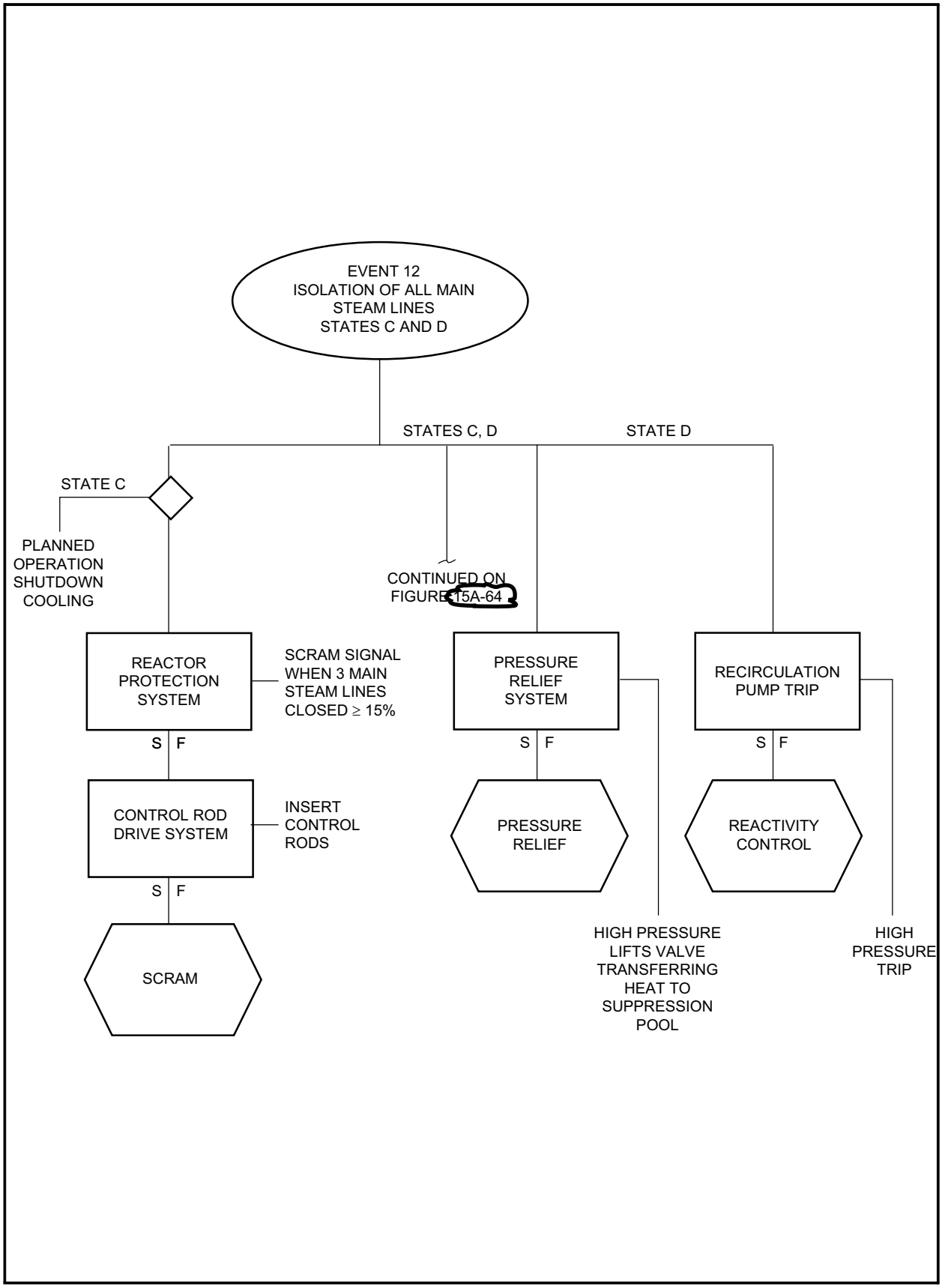


Figure 15A-17 Protection Sequences for Isolation of All Main Steamlines

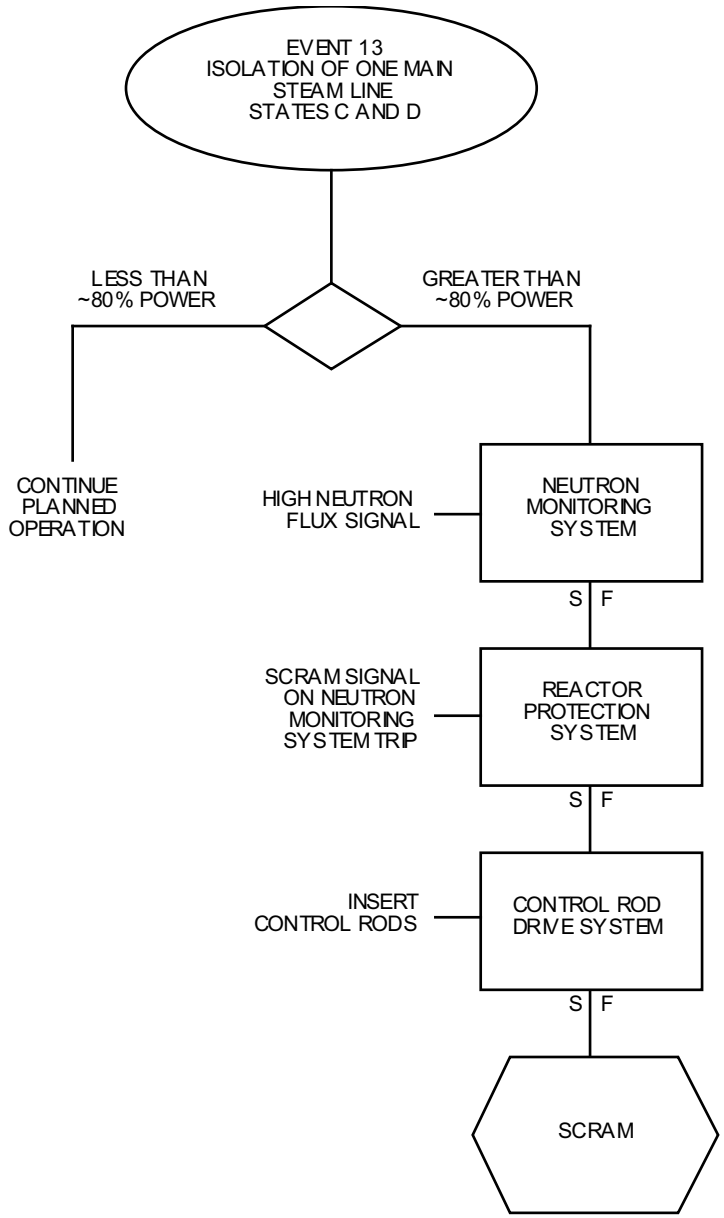


Figure 15A-18 Protection Sequences for Isolation of One Main Steamline

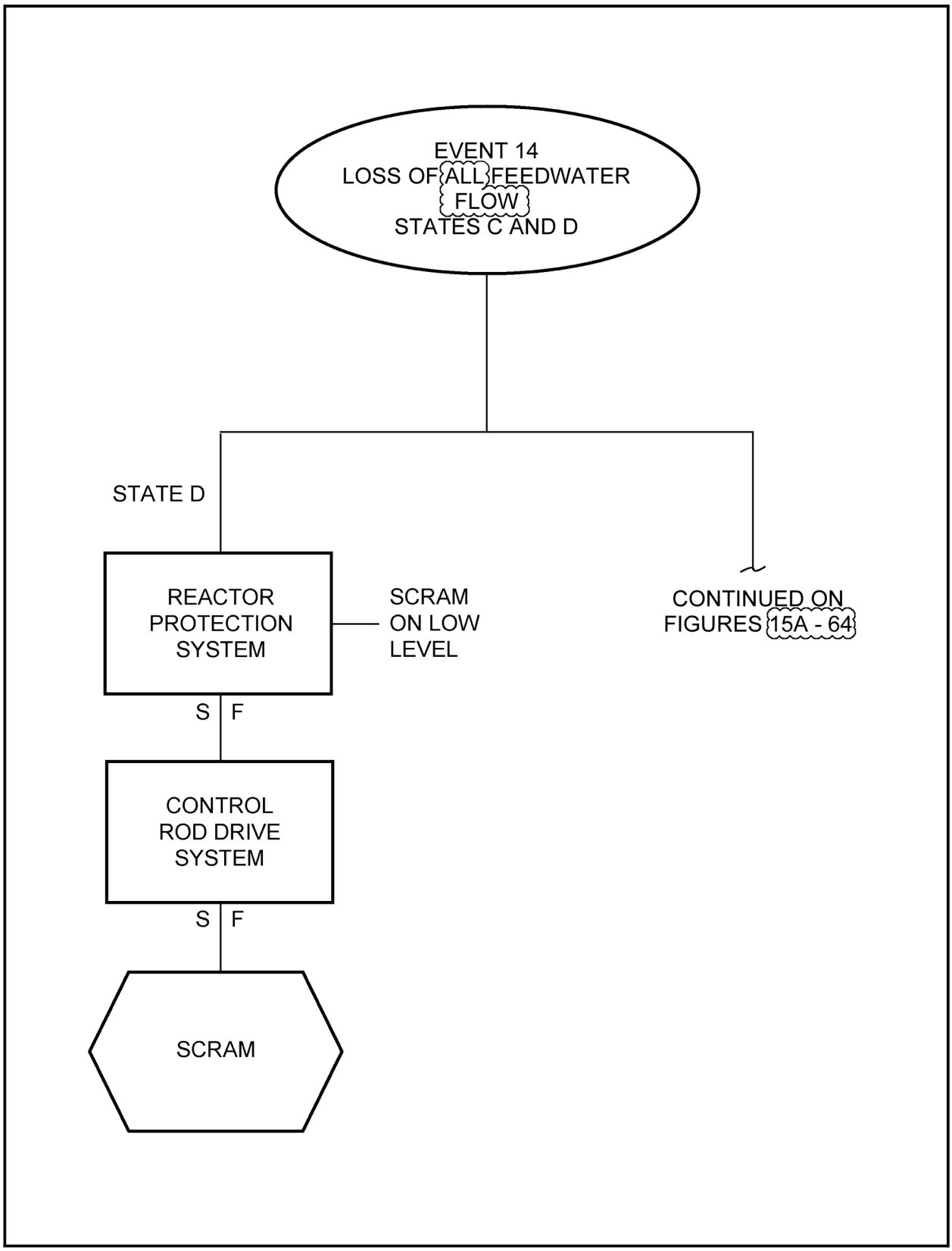


Figure 15A-19 Protection Sequence for Loss of All Feedwater Flow

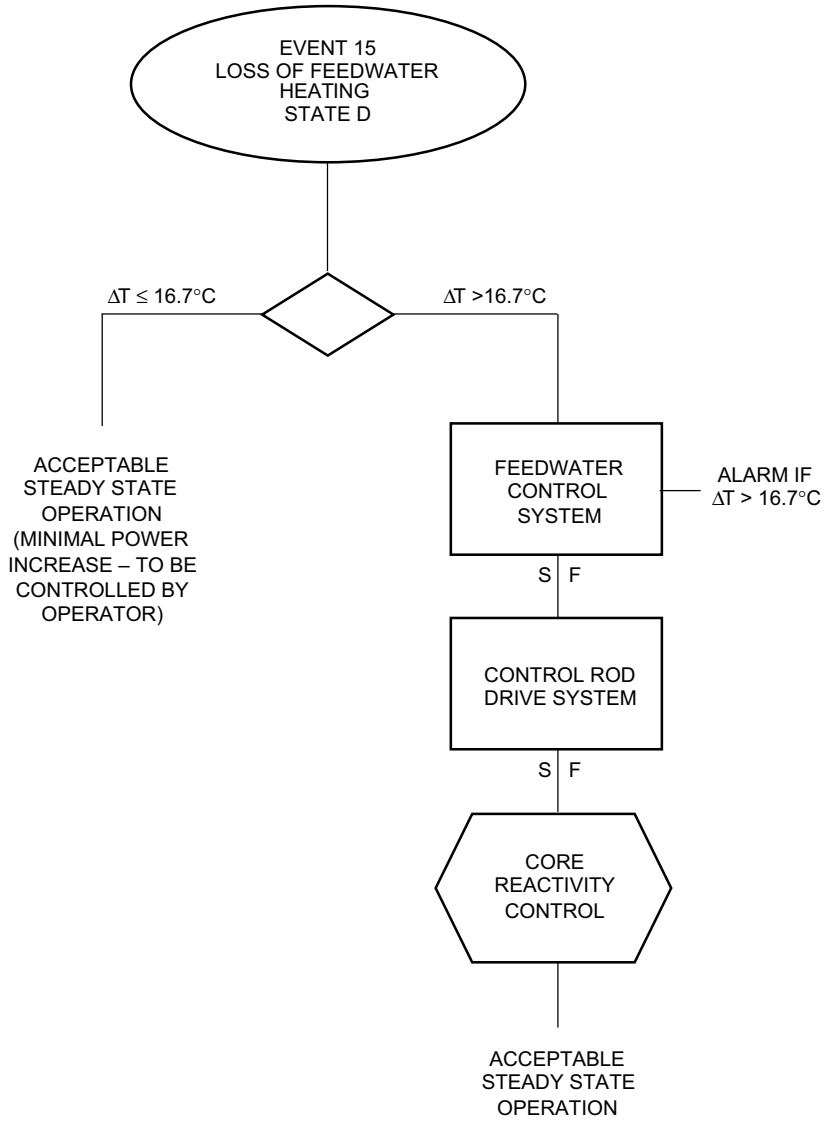


Figure 15A-20 Protection Sequence for a Loss of Feedwater Heating

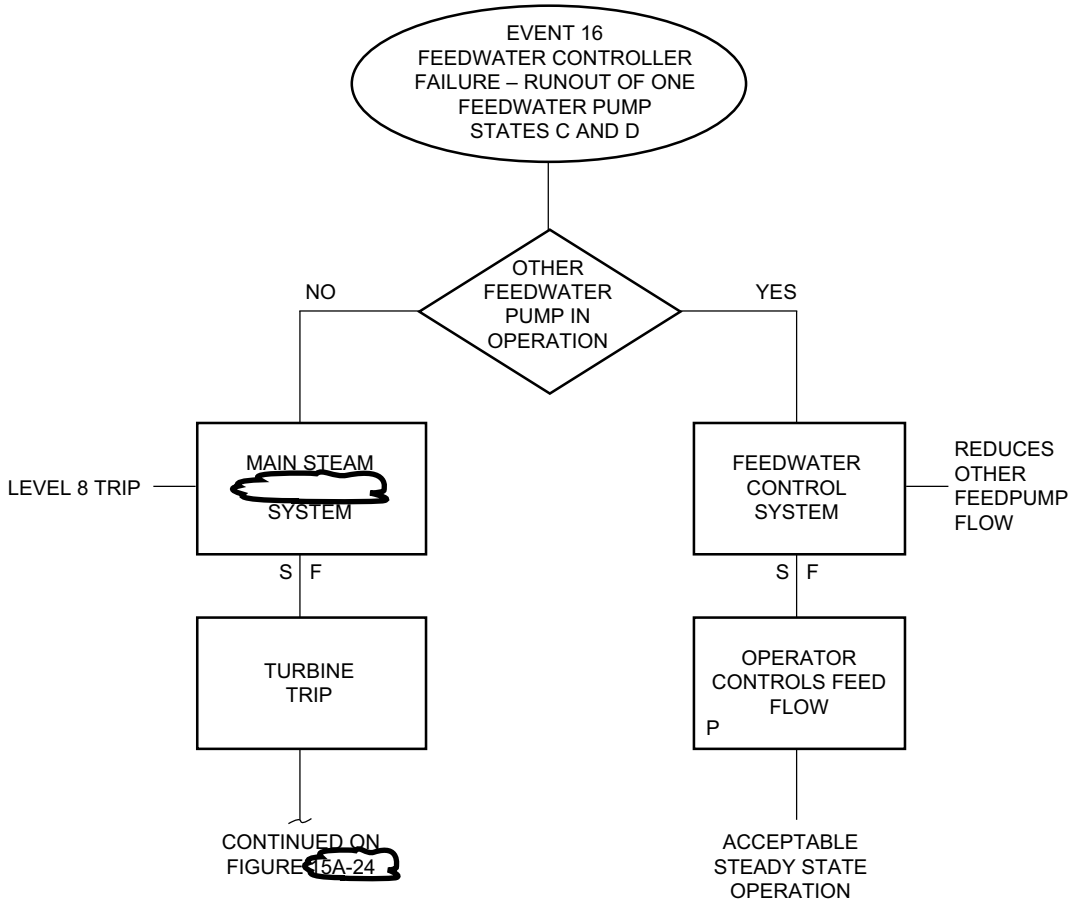


Figure 15A-21 Protection Sequence for Feedwater Controller Failure—Runout of One Feedwater Pump

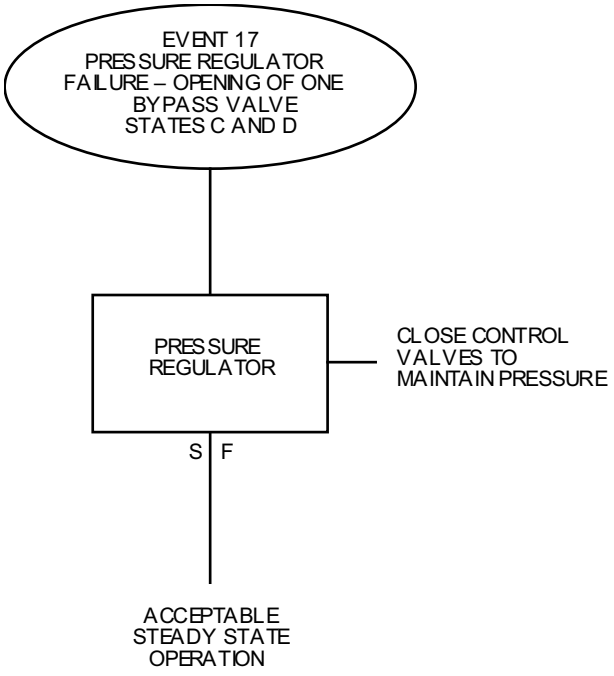


Figure 15A-22 Pressure Regulator Failure—Opening of One Bypass Valve

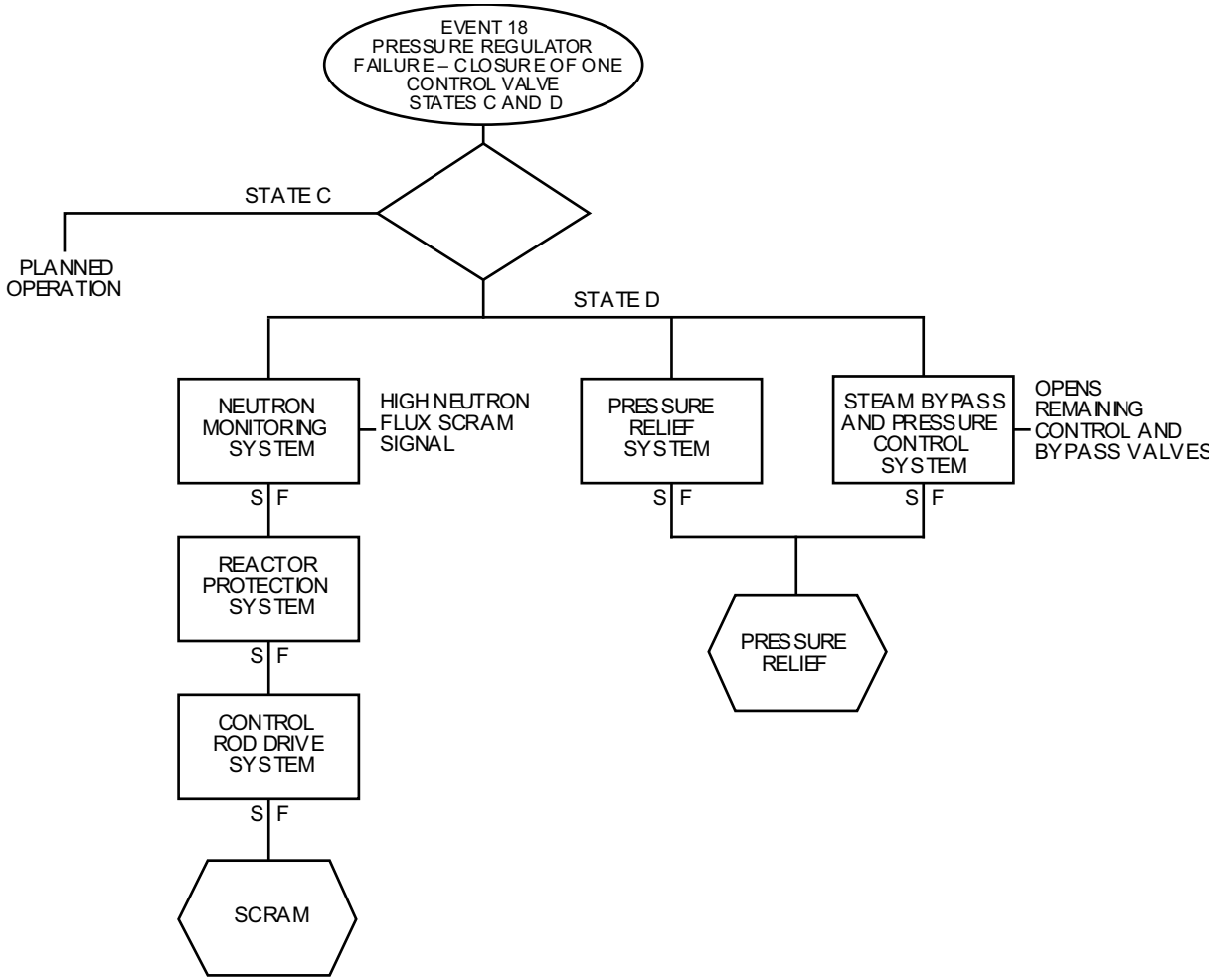


Figure 15A-23 Pressure Regulator Failure—Closure of One Control Valve

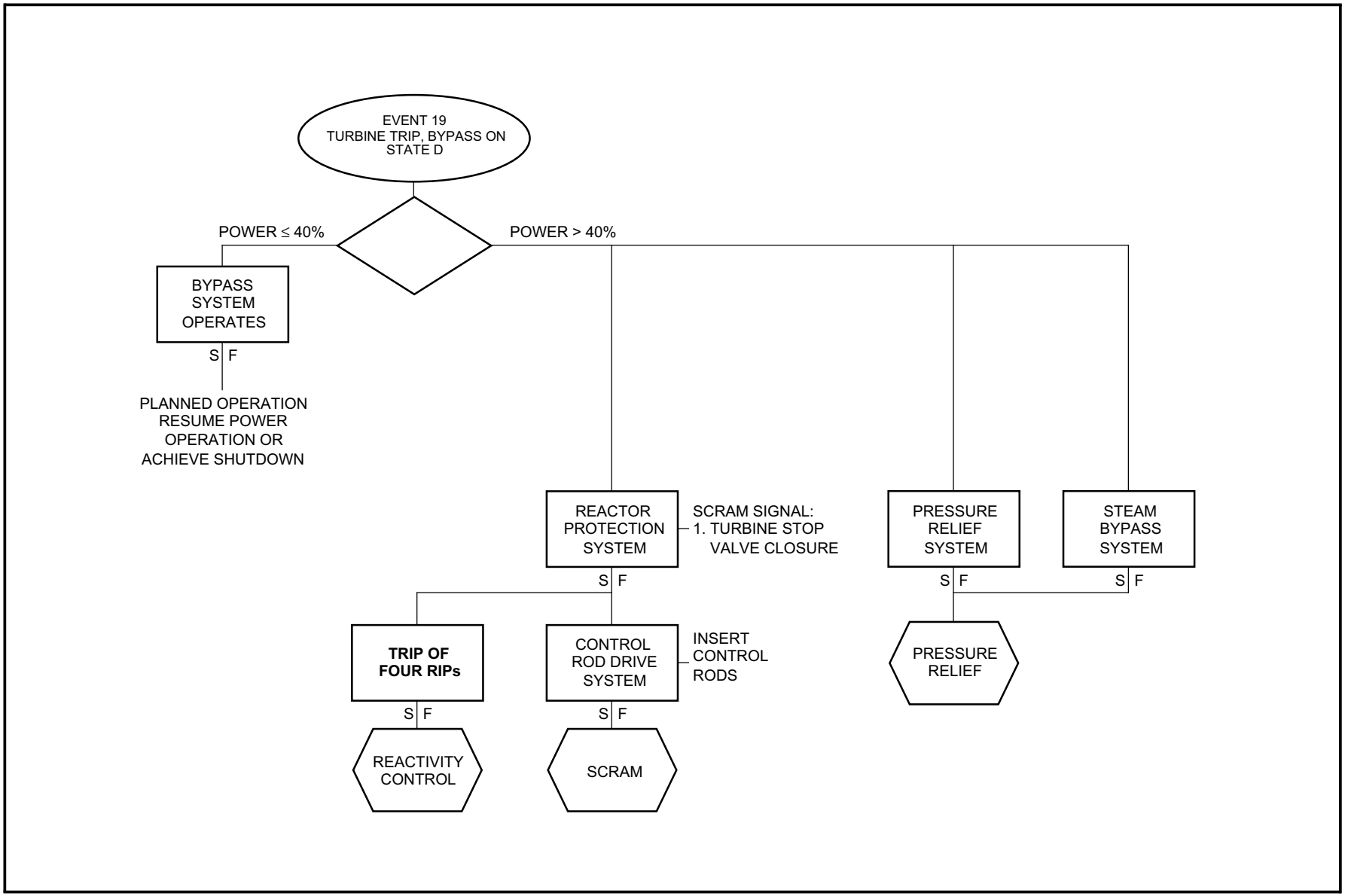


Figure 15A-24 Protection Sequences for Main Turbine Trip, Bypass On

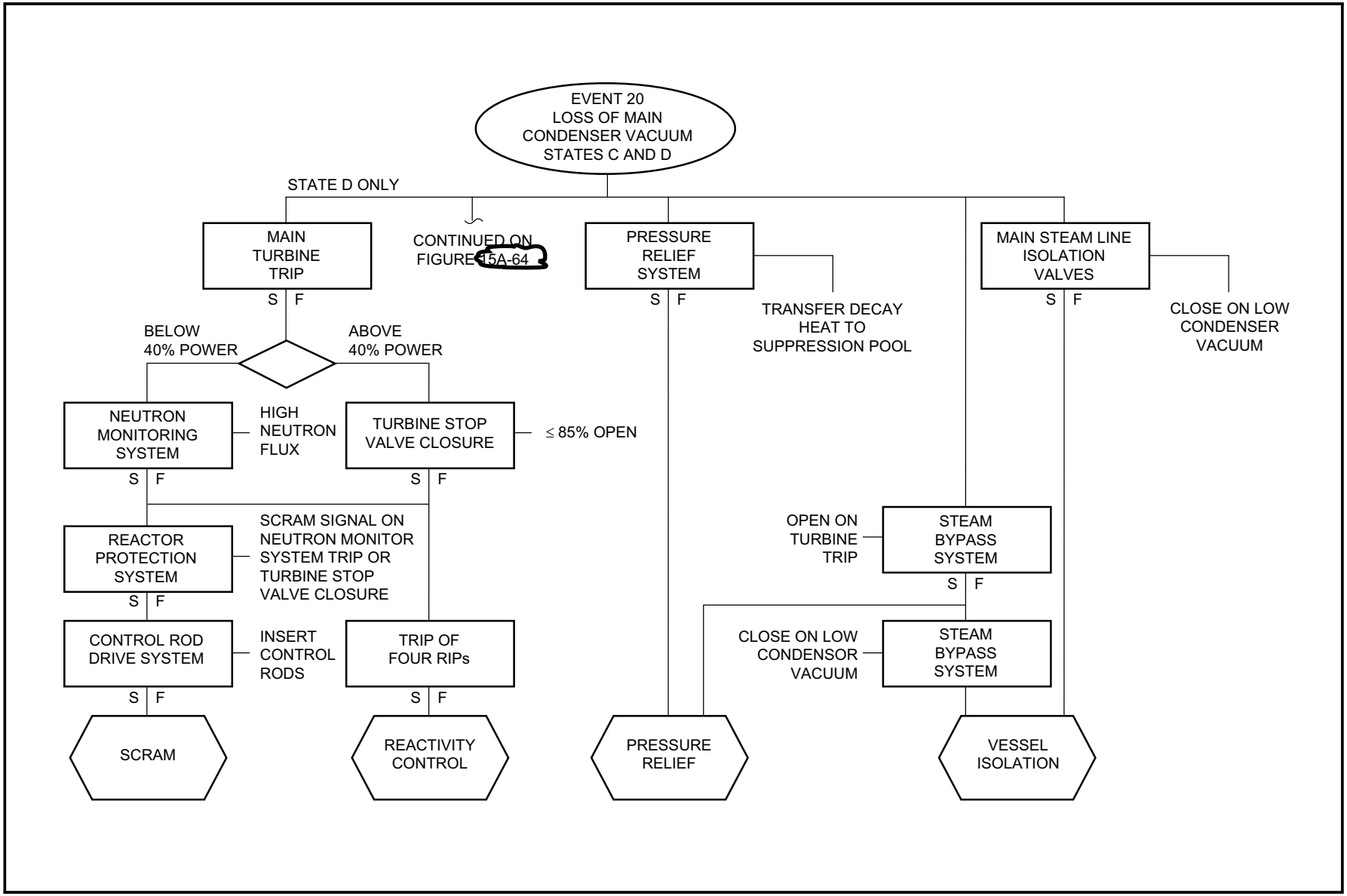


Figure 15A-25 Protection Sequences for Loss of Main Condenser Vacuum

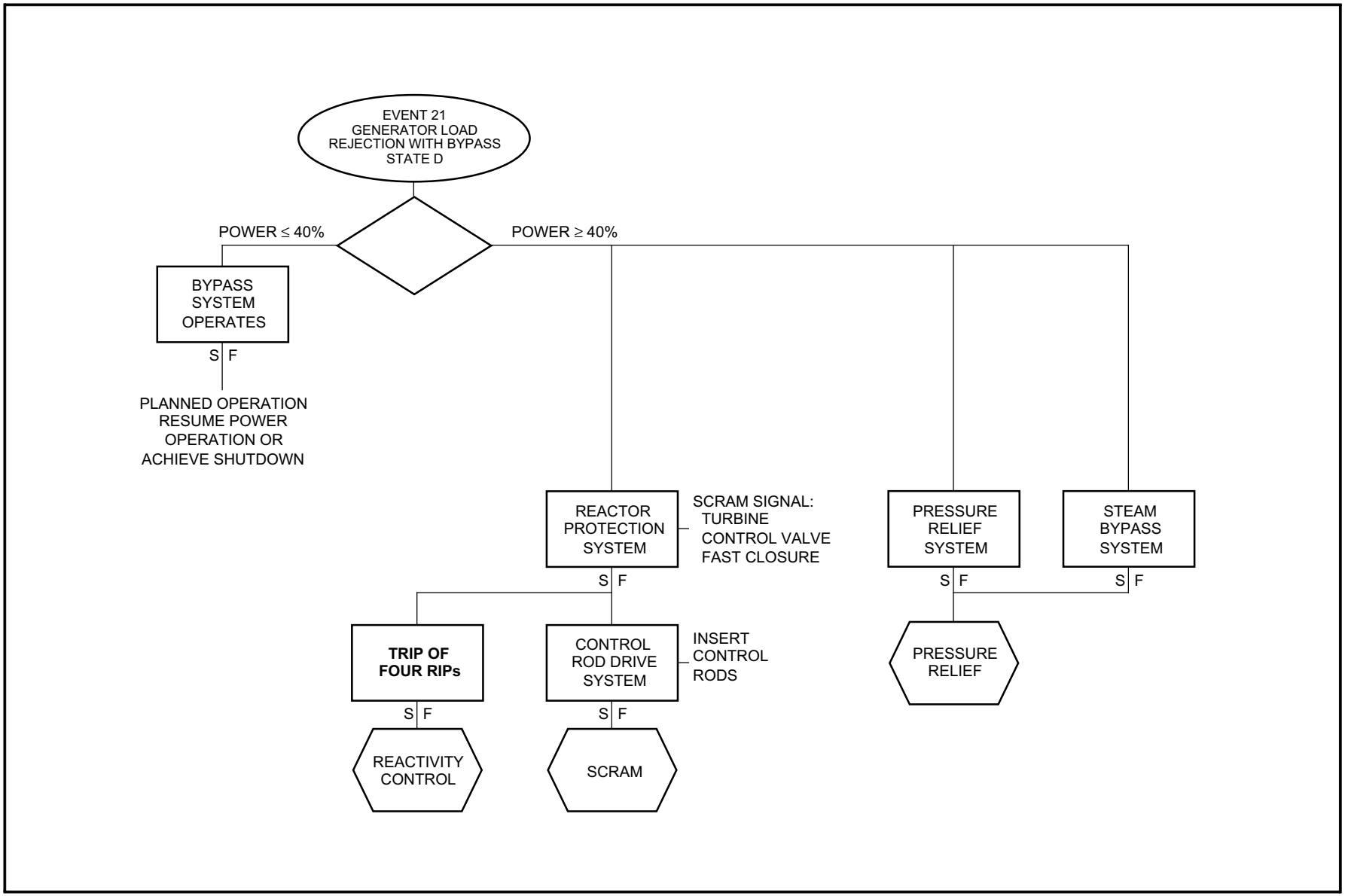


Figure 15A-26 Protection Sequences for Generator Load Rejection, Bypass On

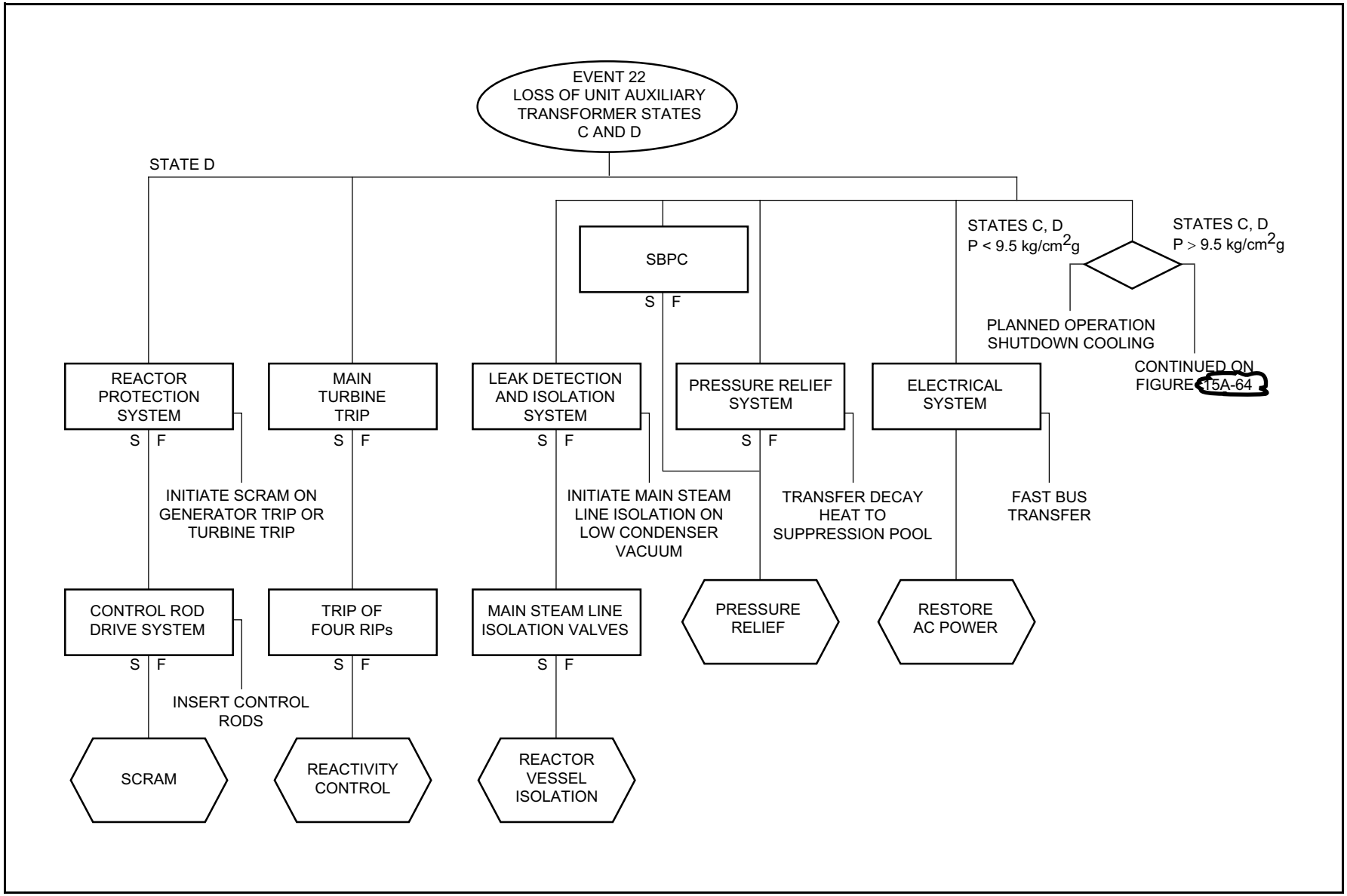


Figure 15A-27 Protection Sequence for Loss of Normal AC Power—Auxiliary Transformer Failure

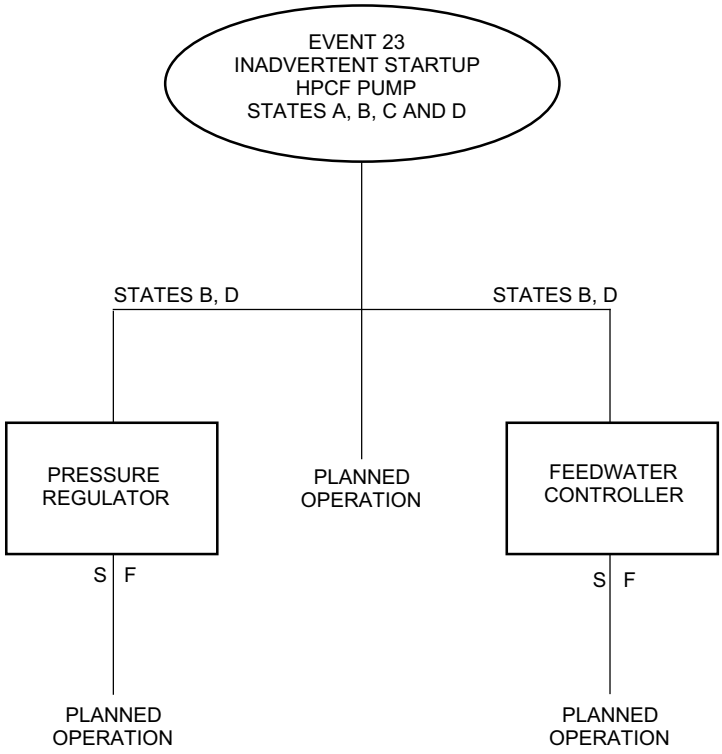


Figure 15A-28 Protection Sequence for Inadvertent Startup of HPCF Pumps

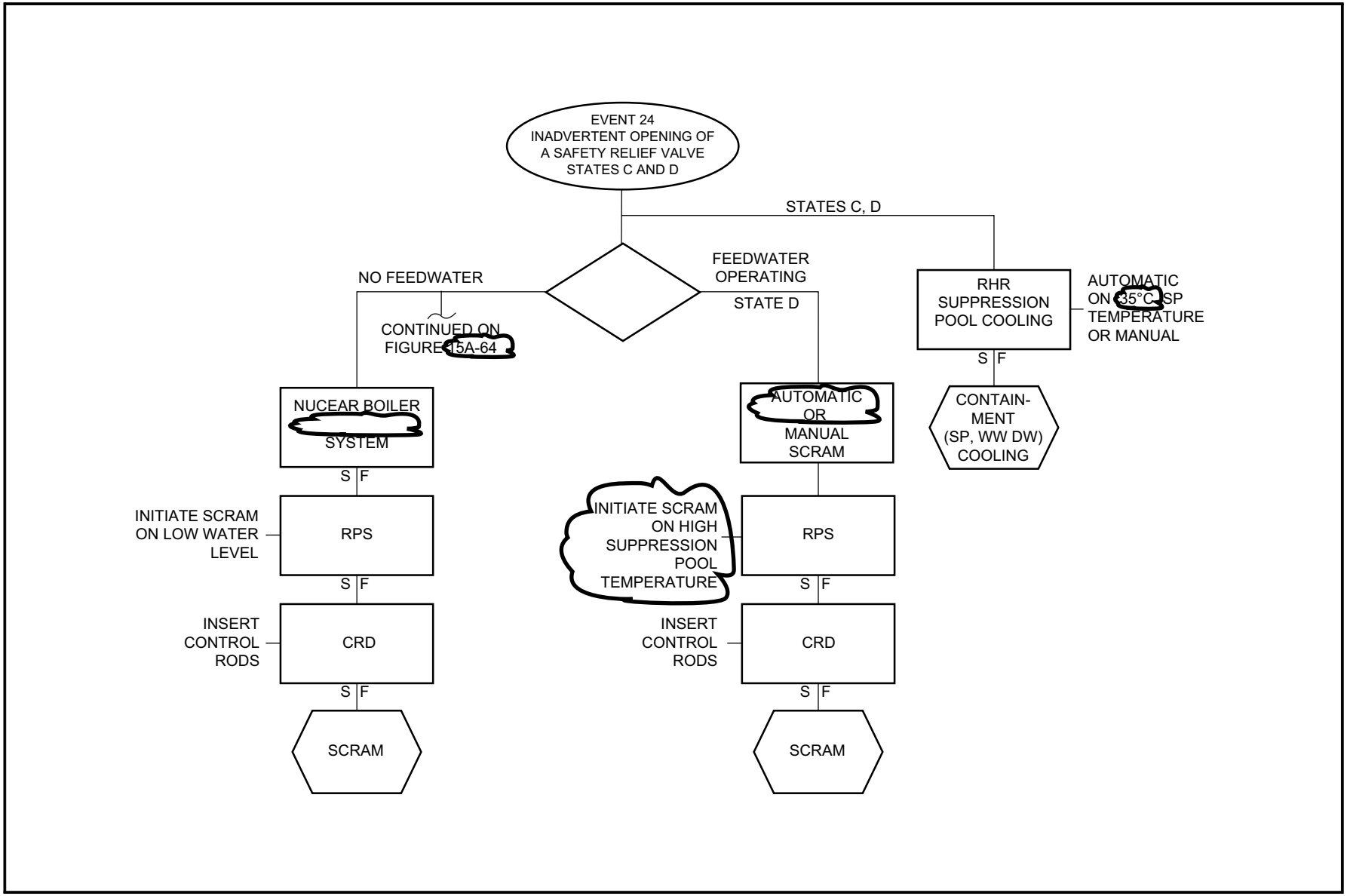


Figure 15A-29 Protection Sequences for Inadvertent Opening of a Safety Relief Valve

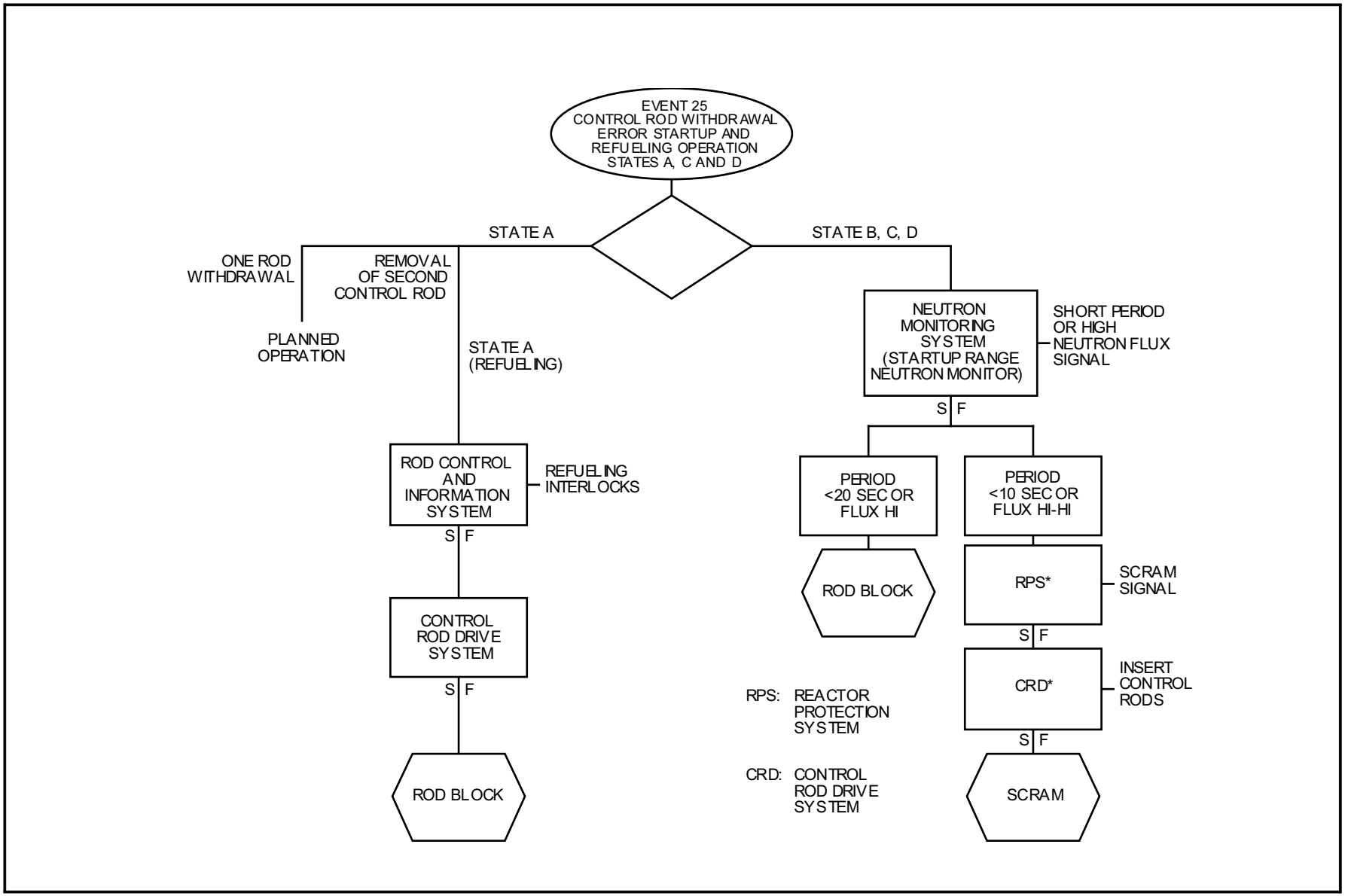


Figure 15A-30 Protection Sequence for Control Rod Withdrawal Error for Startup and Refueling Operations

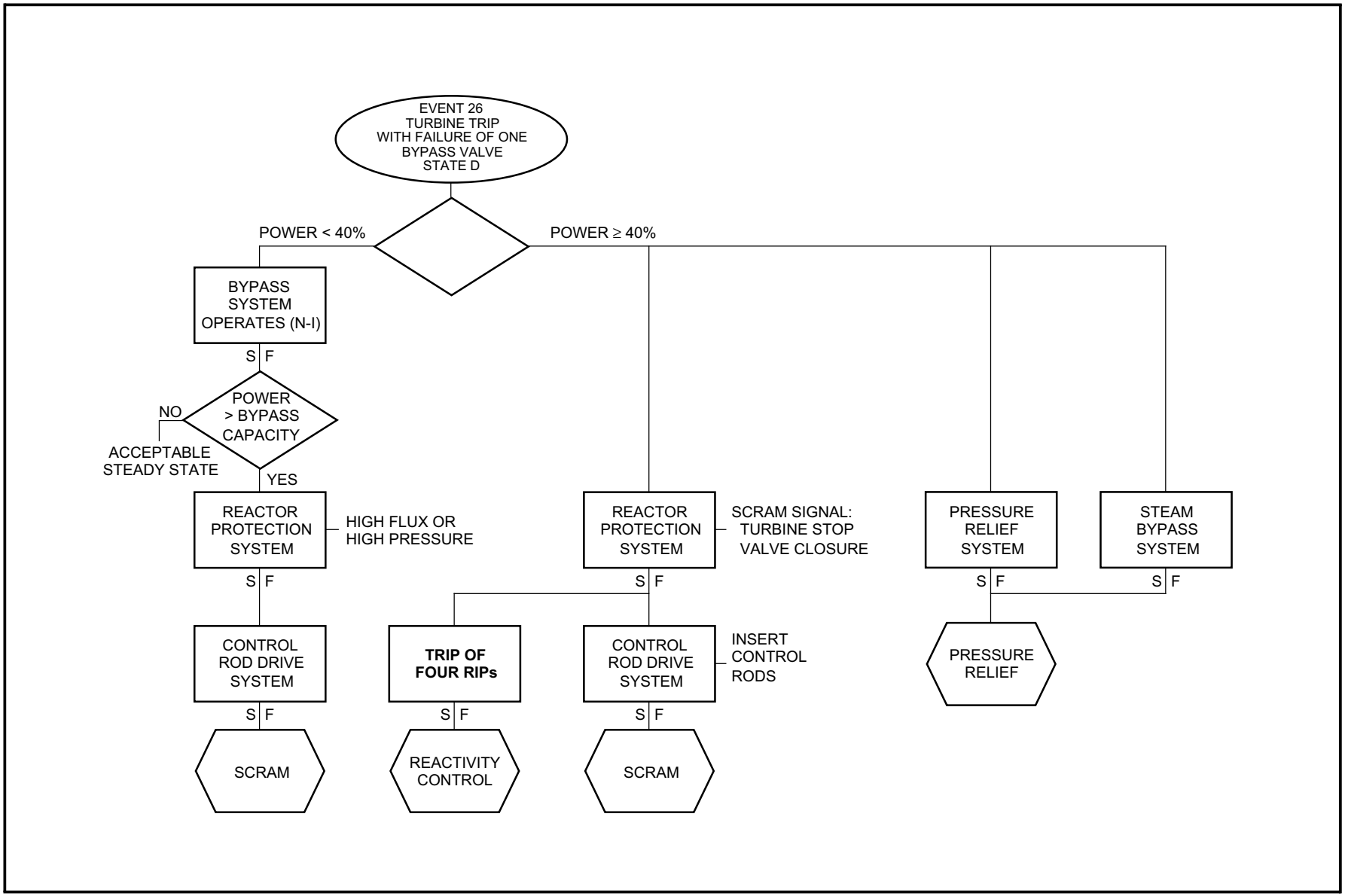


Figure 15A-31 Protection Sequences for Main Turbine Trip with Failure of One Bypass Valve

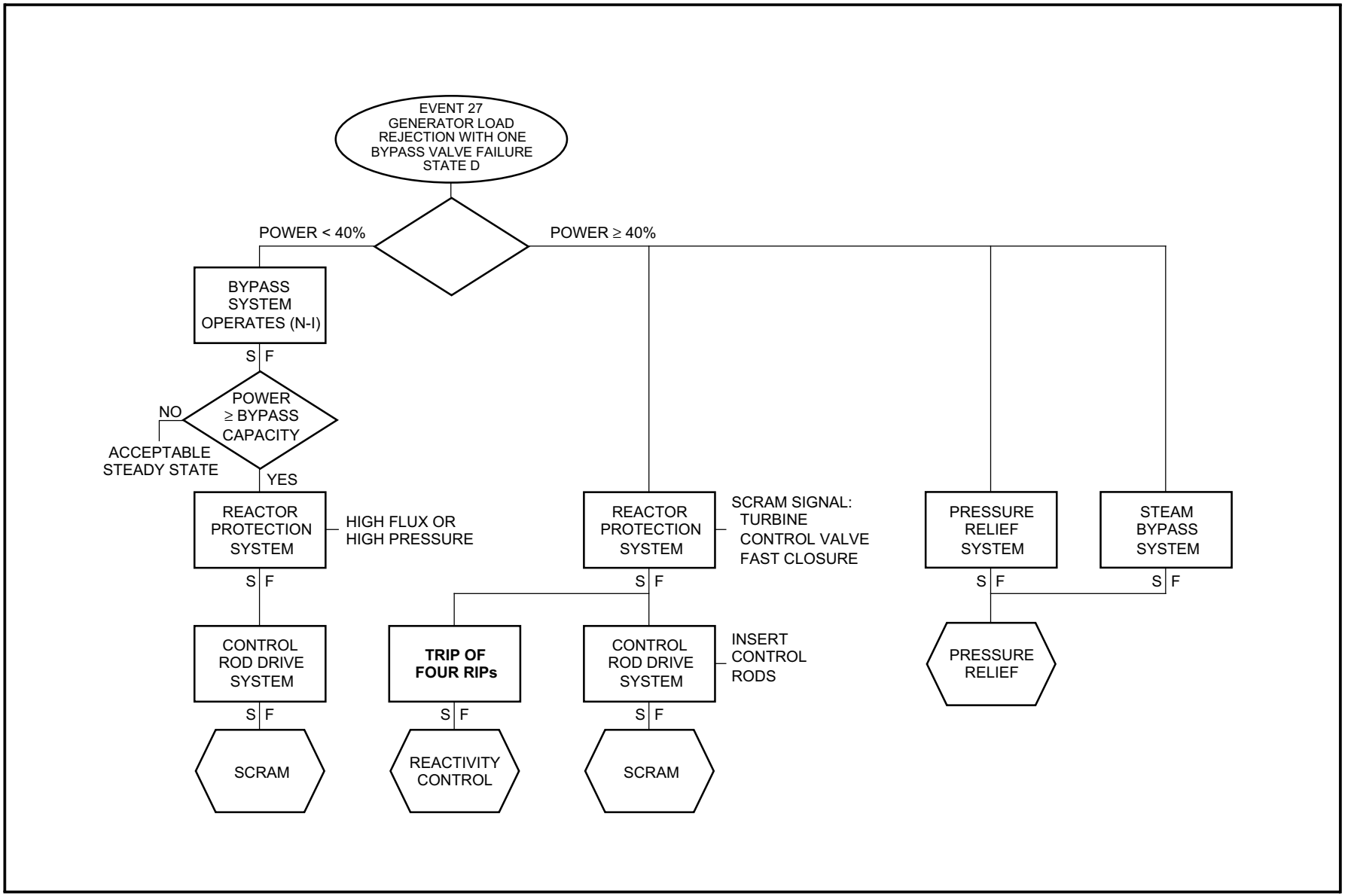


Figure 15A-32 Protection Sequences for Generator Load Rejection with One Bypass Valve Failure

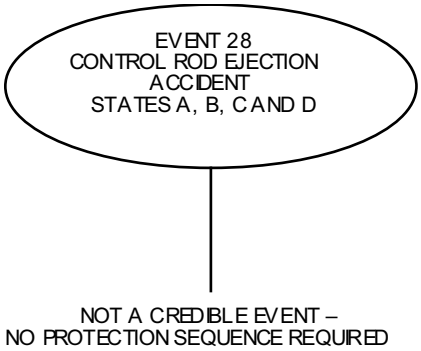


Figure 15A-33 Protection Sequence for Control Rod Ejection Accident

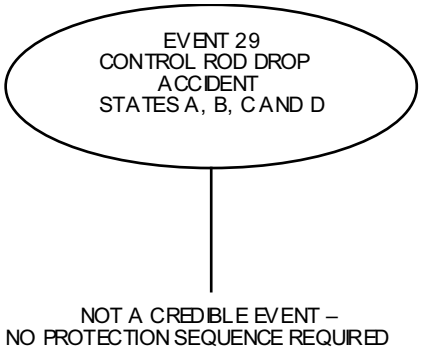


Figure 15A-34 Protection Sequence for Control Rod Drop Accident

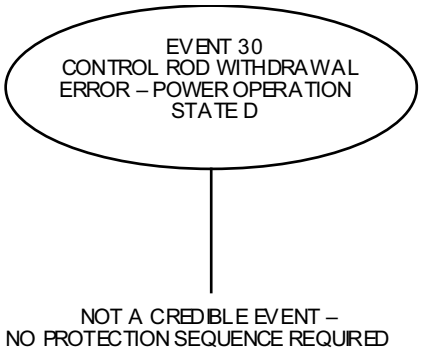


Figure 15A-35 Protection Sequence for a Control Rod Withdrawal Error During Power Operation

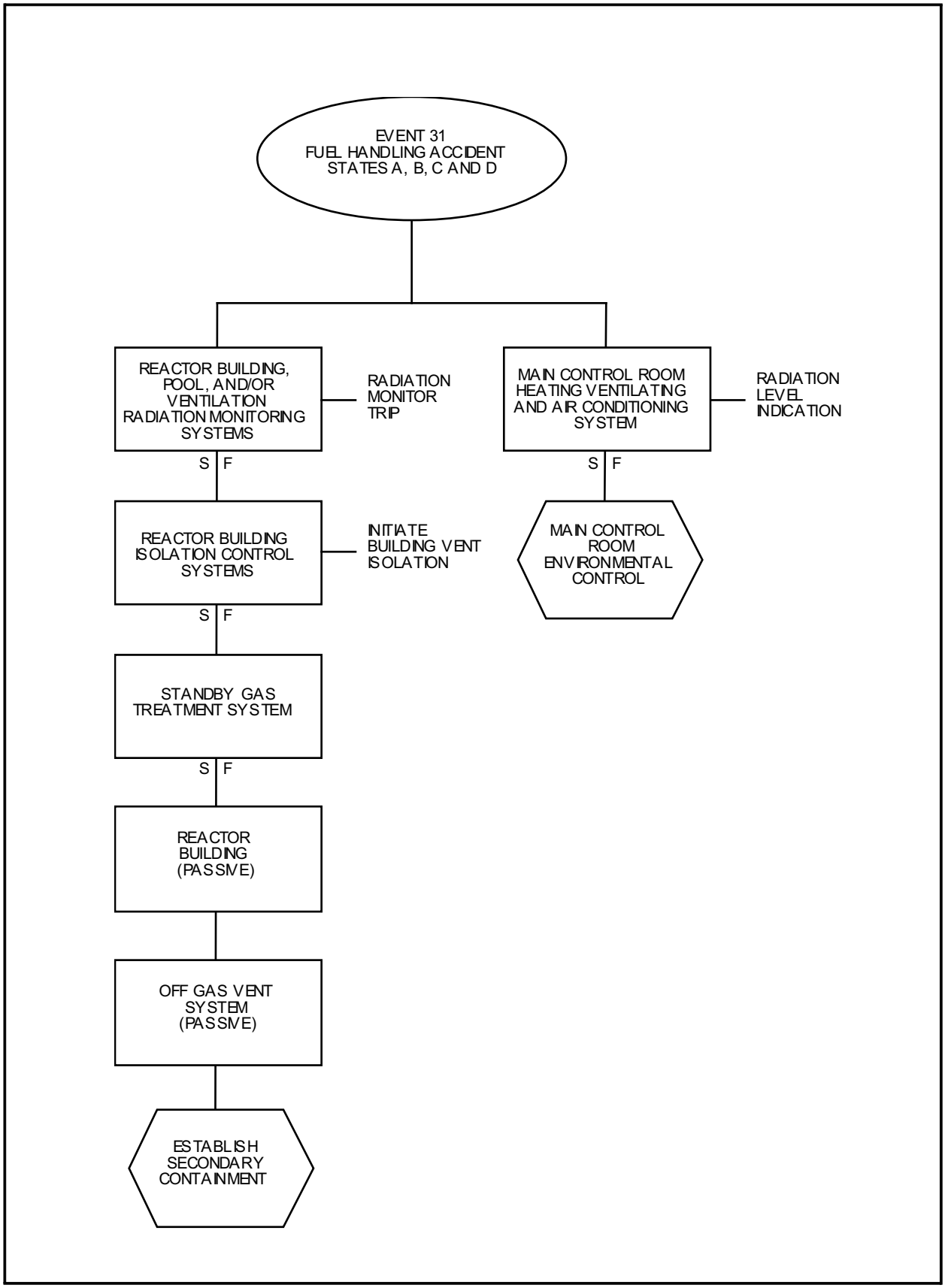


Figure 15A-36 Protection Sequences for Fuel-Handling Accident

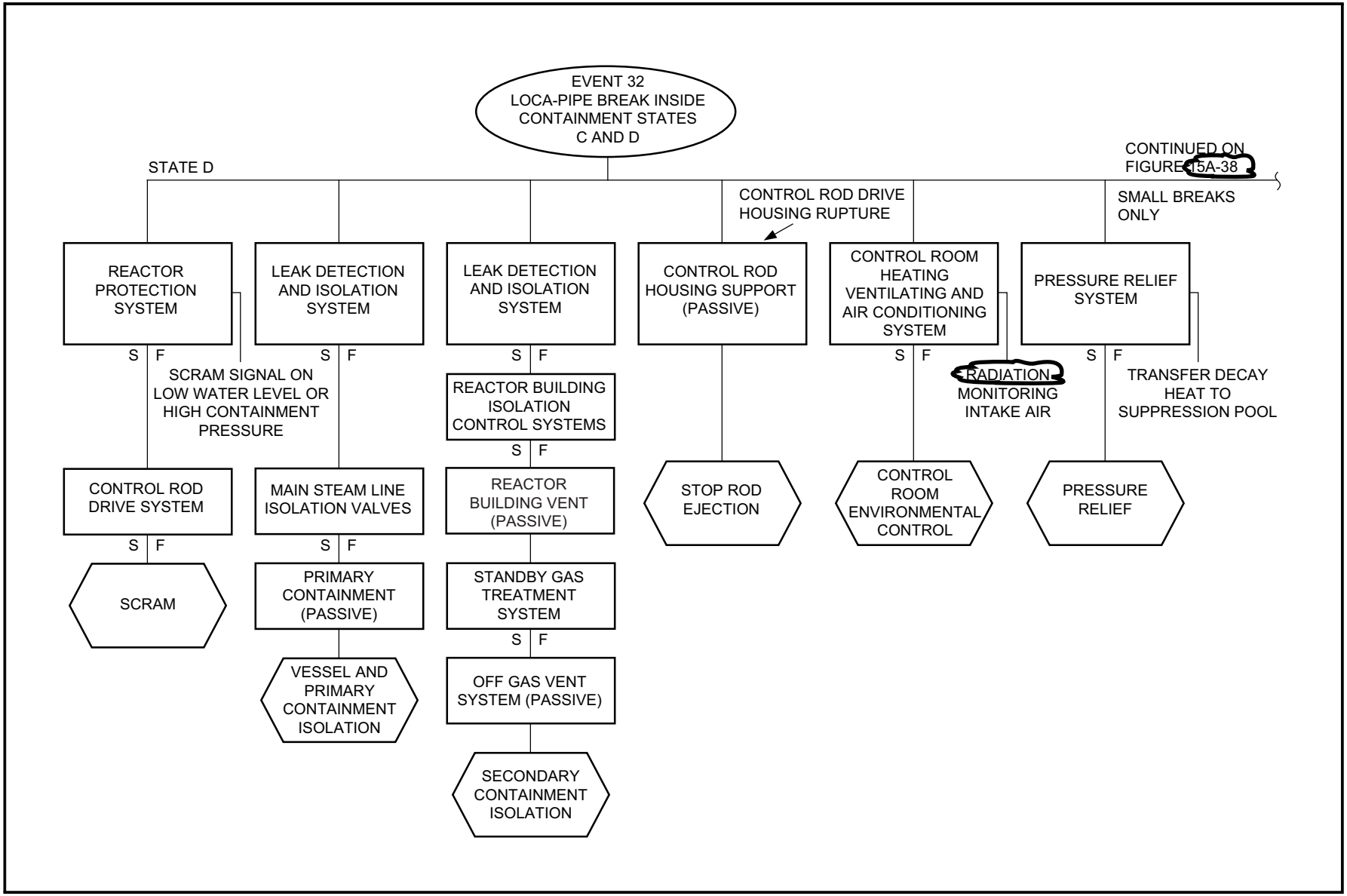


Figure 15A-37 Protection Sequences for Loss of Coolant Piping Breaks in RCPB—Inside Containment

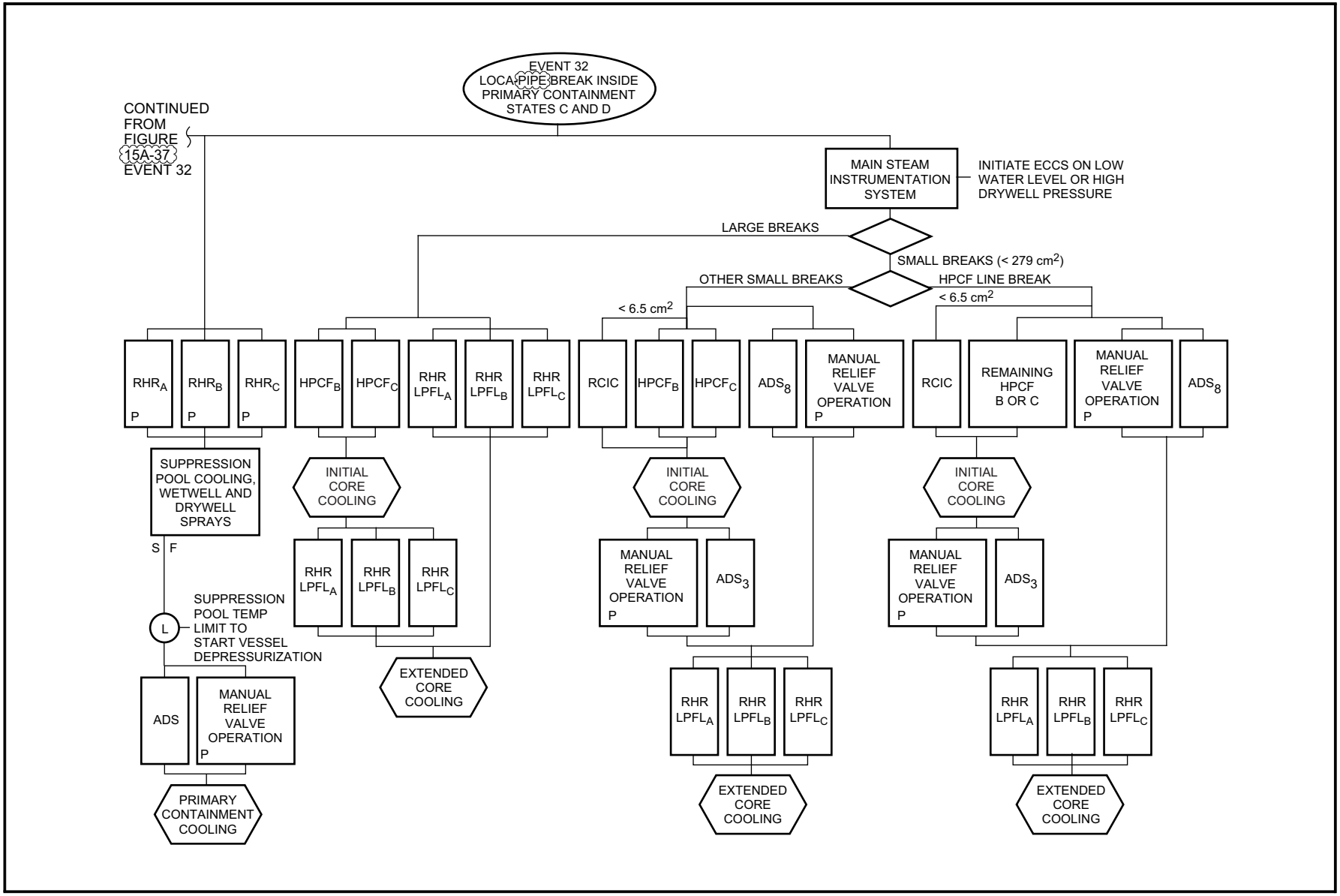
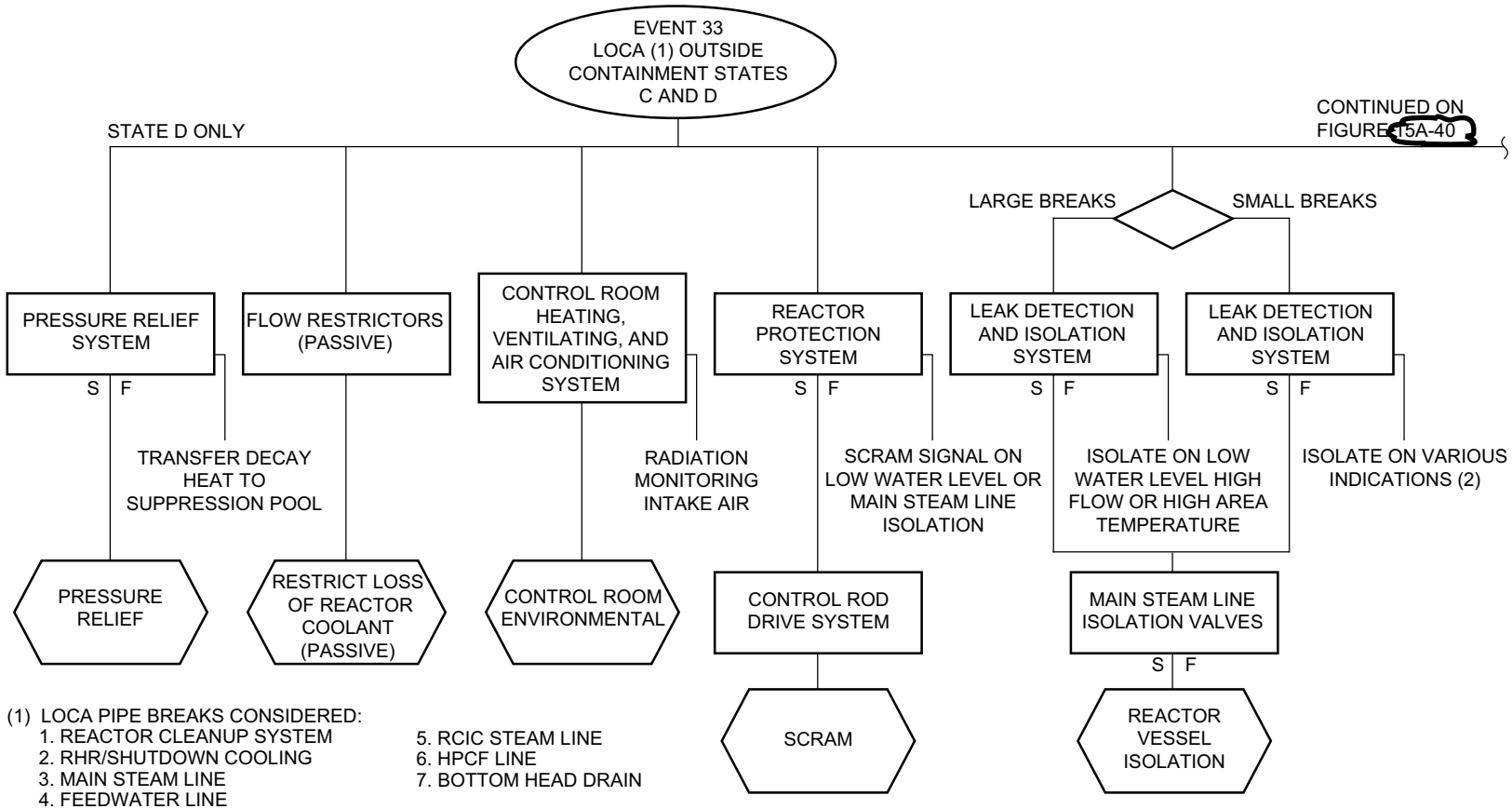


Figure 15A-38 Protection Sequence for Loss of Coolant Piping Breaks in RCPB – Inside Primary Containment



(1) LOCA PIPE BREAKS CONSIDERED:
1. REACTOR CLEANUP SYSTEM
2. RHR/SHUTDOWN COOLING
3. MAIN STEAM LINE
4. FEEDWATER LINE
5. RCIC STEAM LINE
6. HPCF LINE
7. BOTTOM HEAD DRAIN

(2) VARIOUS INDICATIONS:
1. FEED SIGNALS TO PUMPS
2. FEED TEMPERATURE
3. SPACE TEMPERATURE
4. FLOW INDICATIONS
5. REACTOR VESSEL WATER FLOW
6. FEEDWATER FLOW
7. HOT WELL LEVEL
8. VISUAL INSPECTION
9. LEAKAGE INDICATIONS

Figure 15A-39 Protection Sequences for Liquid and Steam, Large and Small Piping Breaks Outside Containment

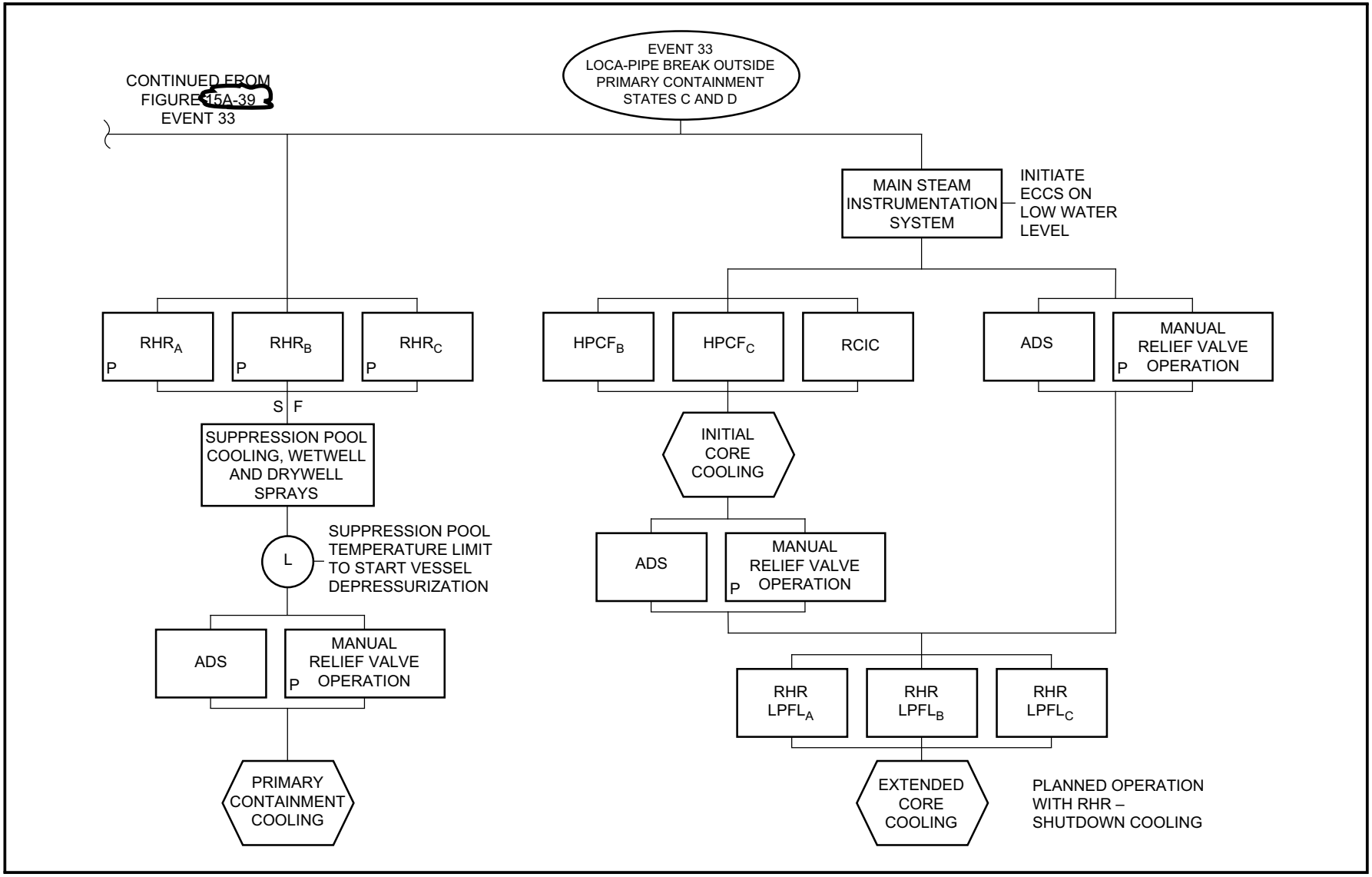


Figure 15A-40
Protection Sequence for Liquid and Steam, Large and Small Piping Breaks Outside Primary Containment

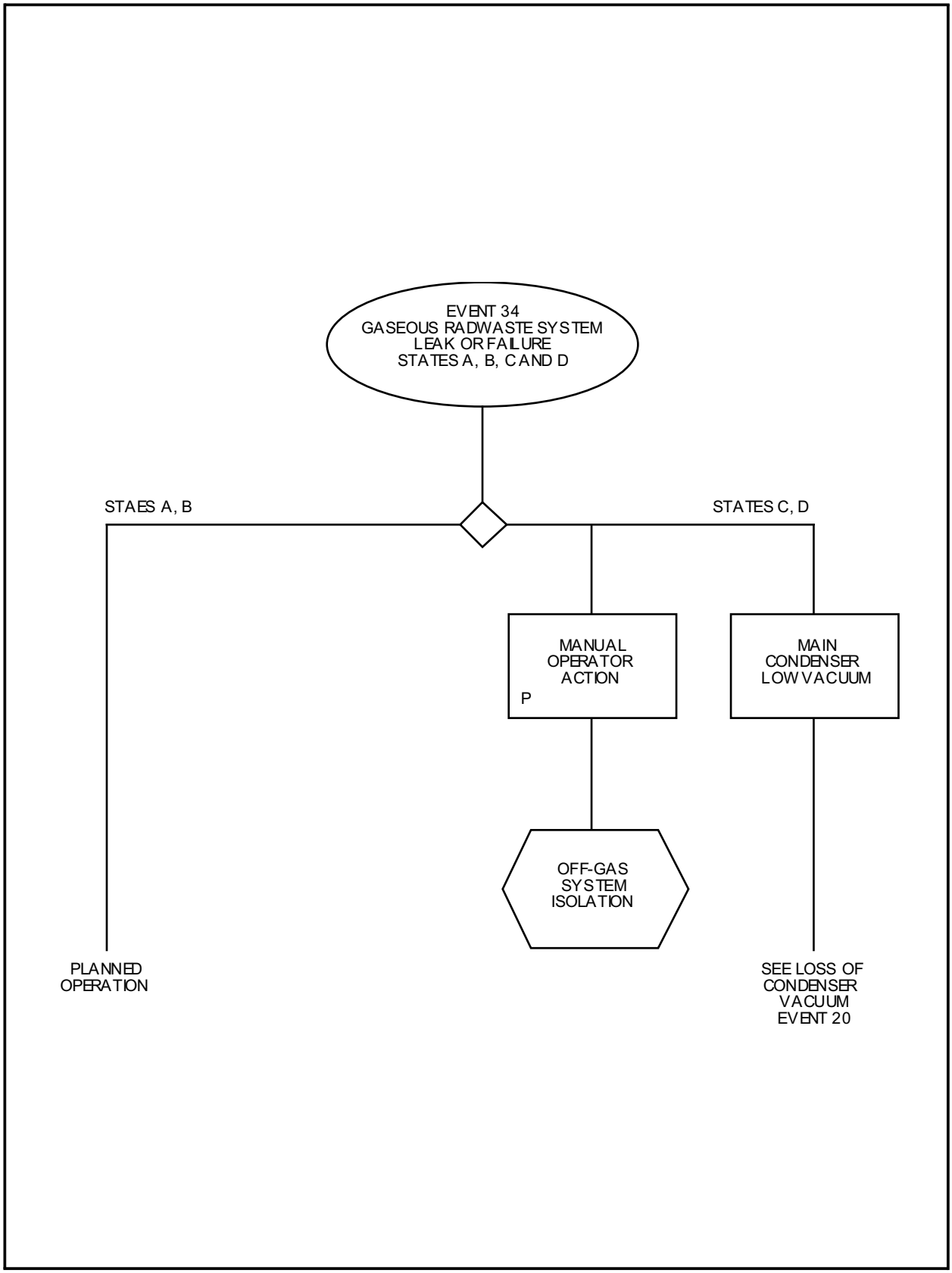


Figure 15A-41 Protection Sequence for Gaseous Radwaste System Leak or Failure

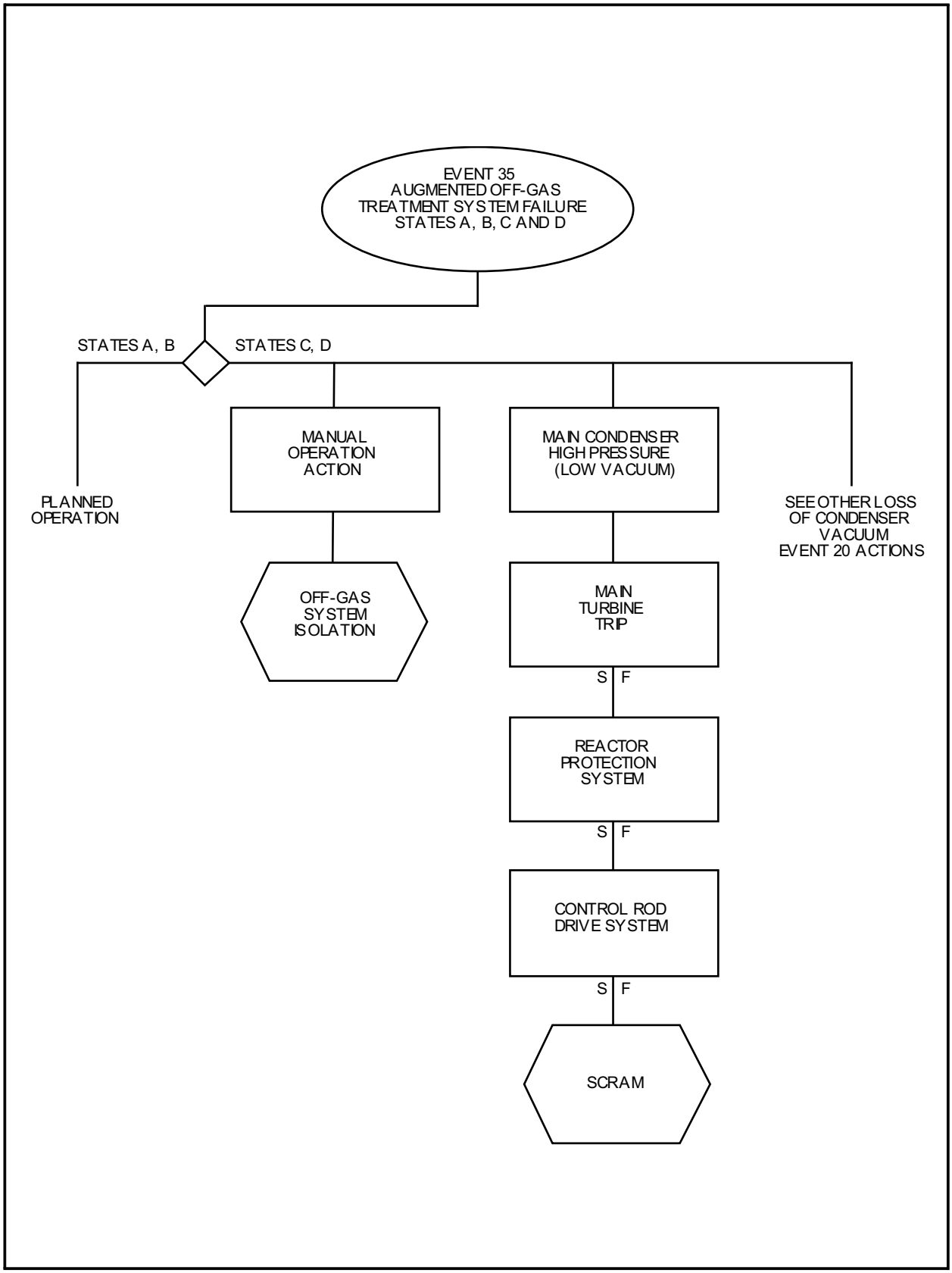


Figure 15A-42
Protection Sequence for Augmented Offgas Treatment System Failure

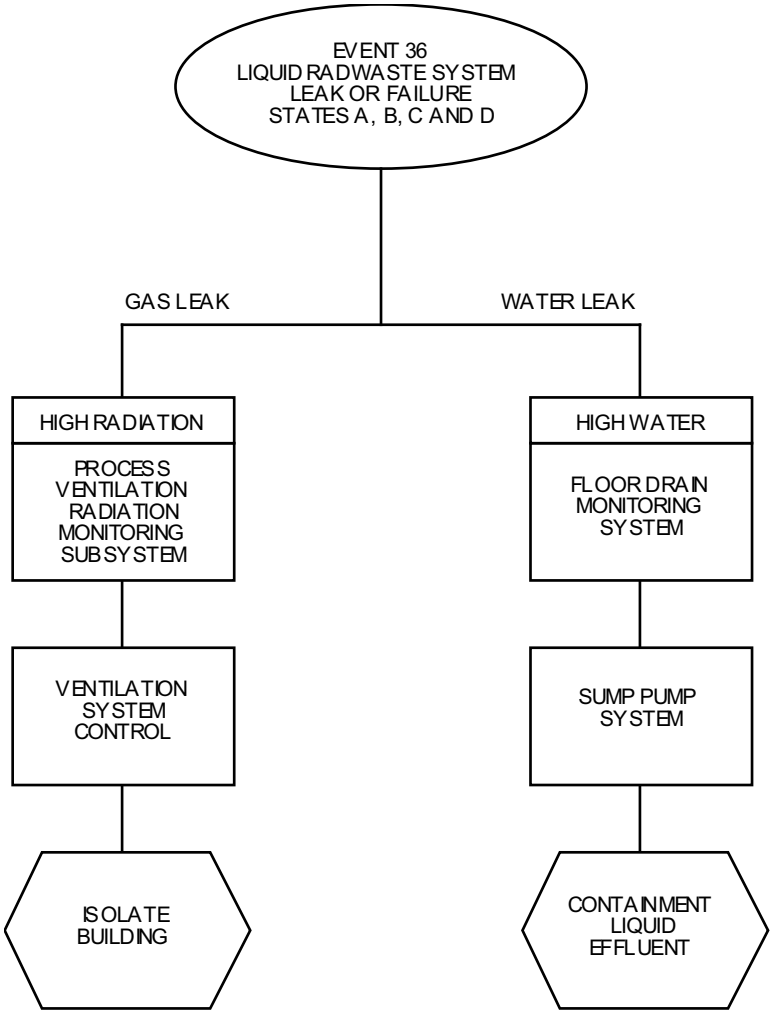


Figure 15A-43 Protection Sequence for Liquid Radwaste System Leak or Failure

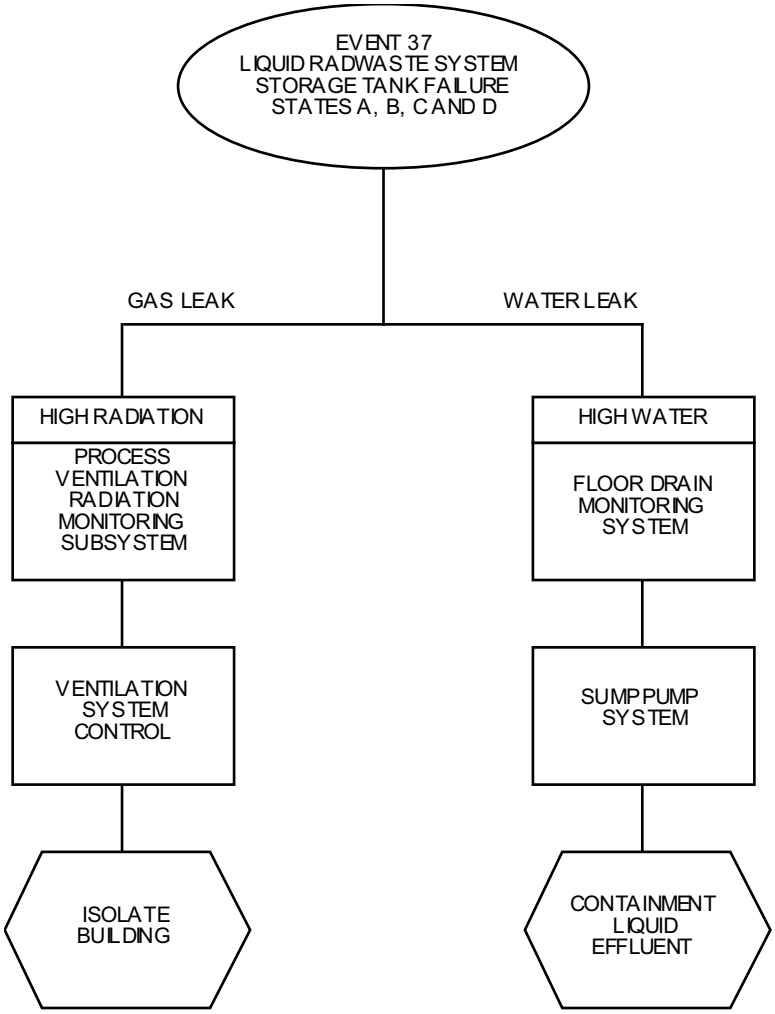


Figure 15A-44
Protection Sequence for Liquid Radwaste System Storage Tank Failure

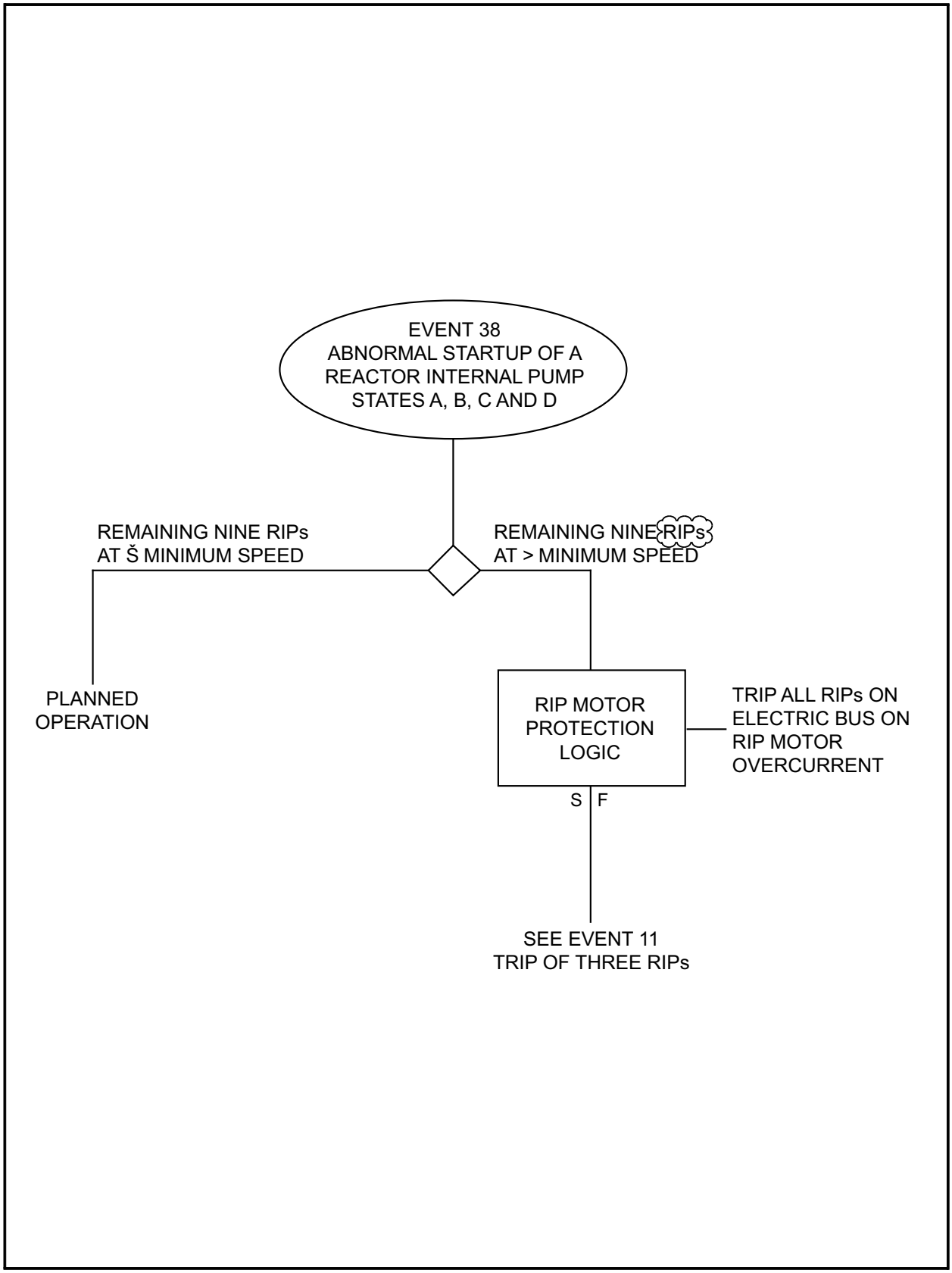


Figure 15A-45
Protection Sequence for Abnormal Startup of a Reactor Internal Pump

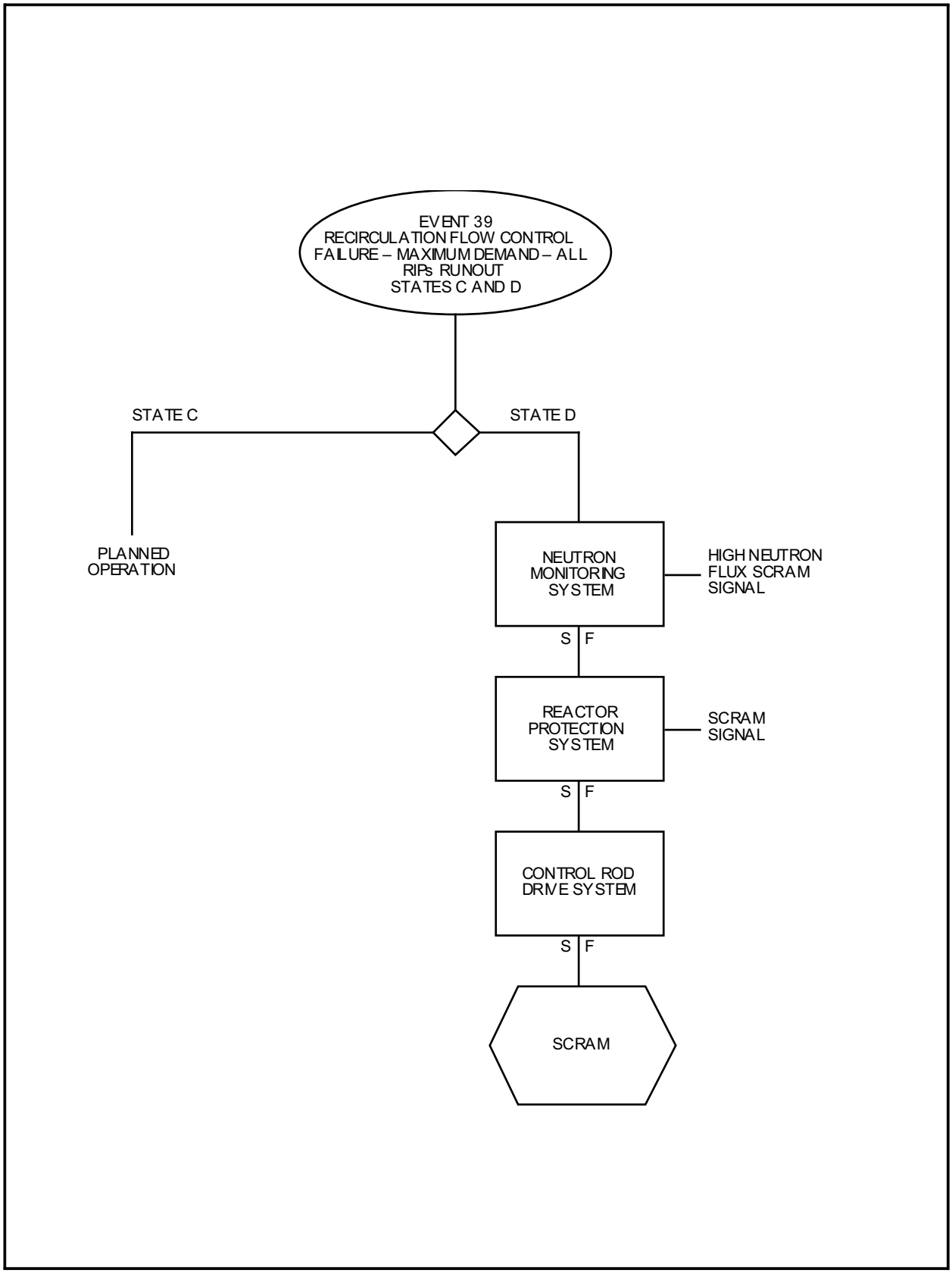


Figure 15A-46 Protection Sequence for Recirculation Flow Control Failure—Maximum Demand—All Reactor Internal Pumps (RIPs) Runout

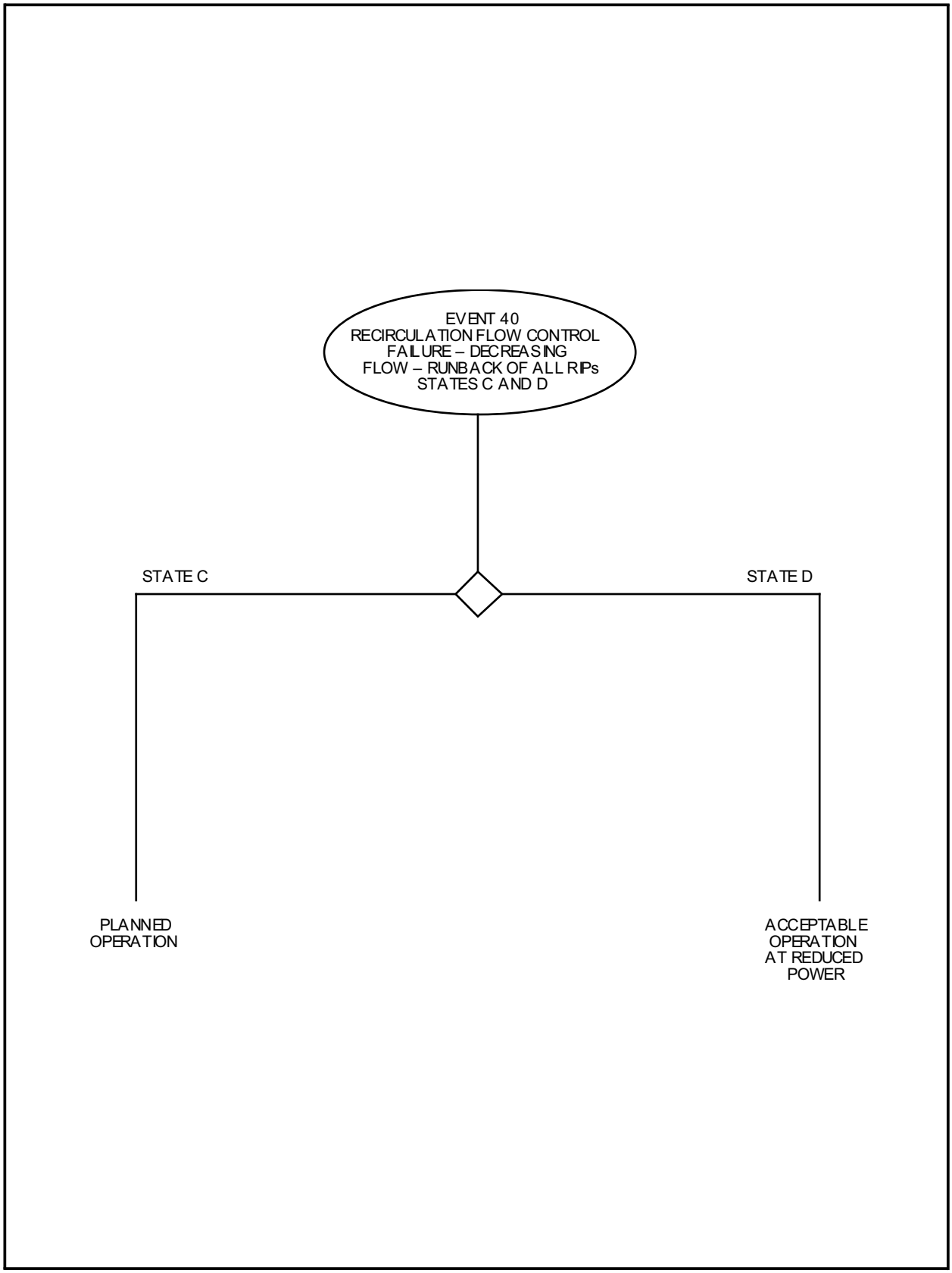


Figure 15A-47 Protection Sequence for Recirculation Flow Control Failure—Decreasing Flow—Runback of All Reactor Internal Pumps (RIPs)

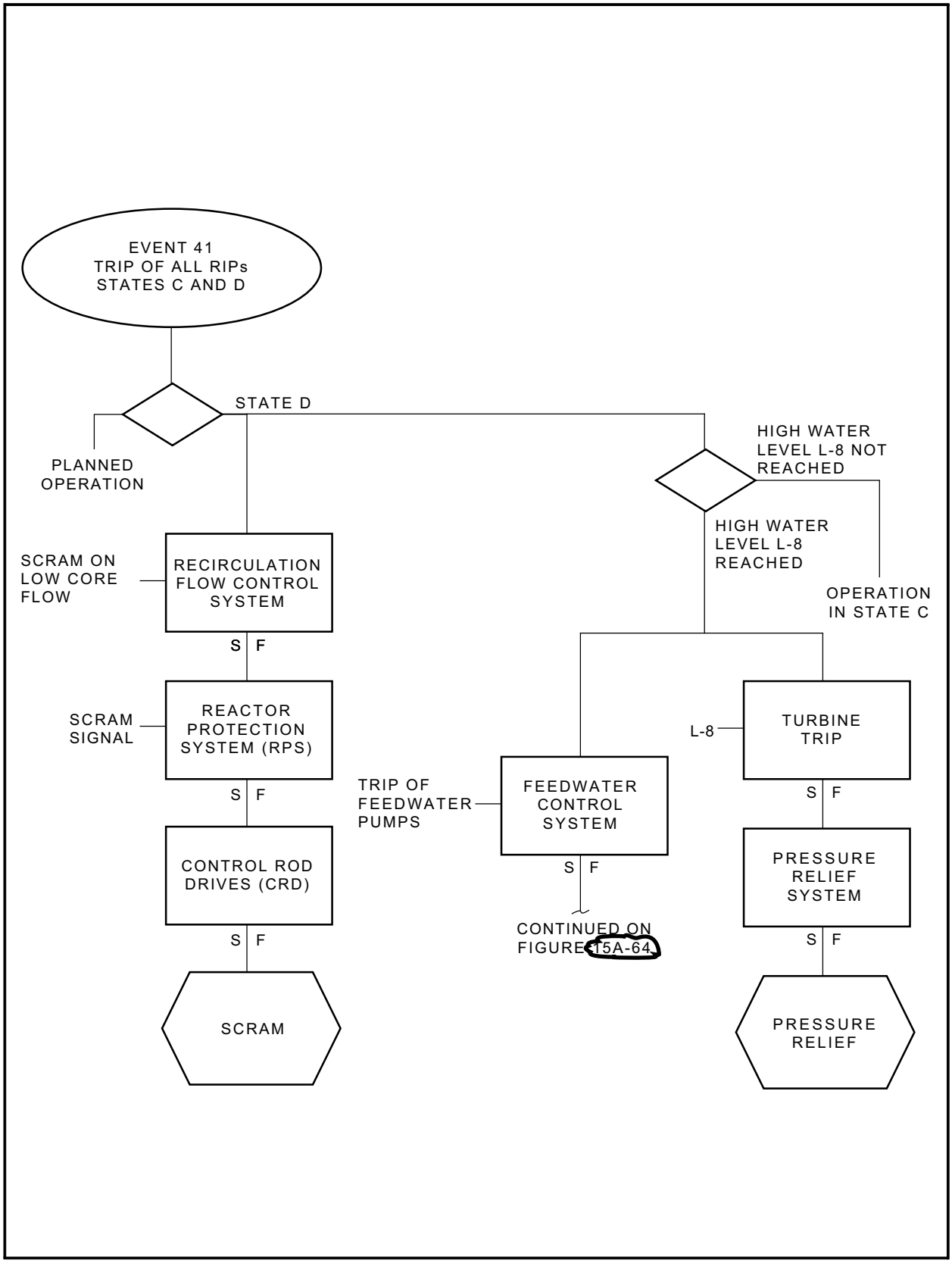


Figure 15A-48 Protection Sequence for Trip of All Reactor Internal Pumps (RIPs)

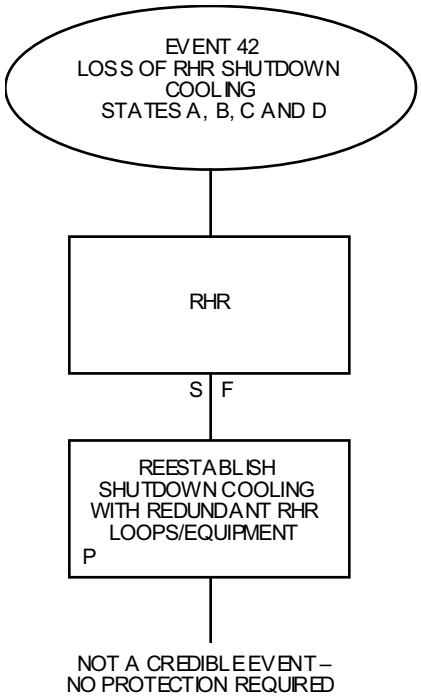


Figure 15A-49 Protection Sequence for RHR—Loss of Shutdown Cooling

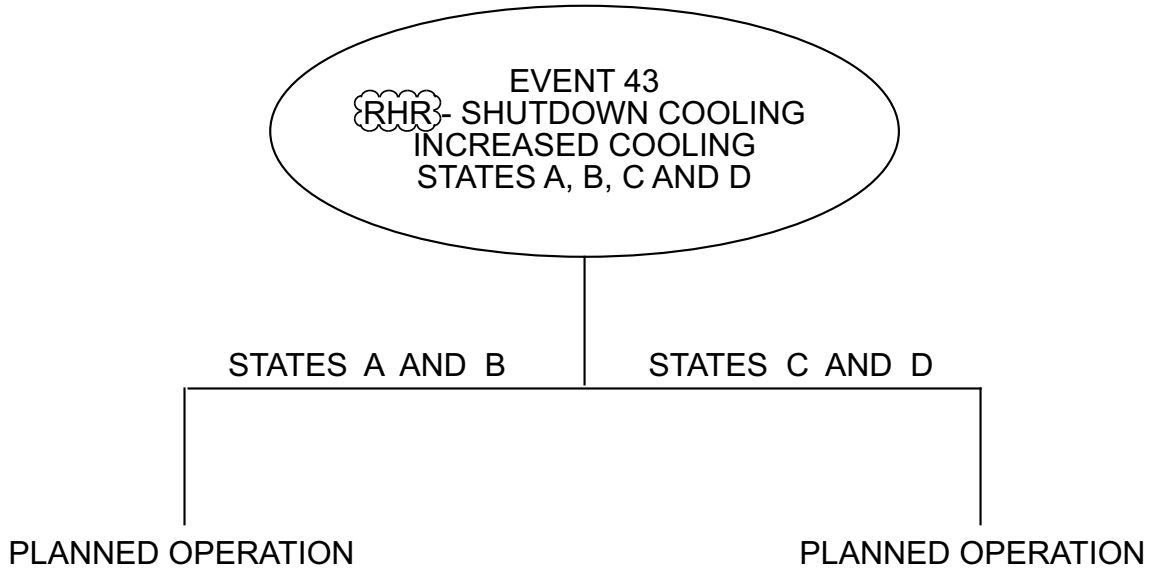


Figure 15A-50 RHR—Shutdown Cooling Failure—Increased Cooling

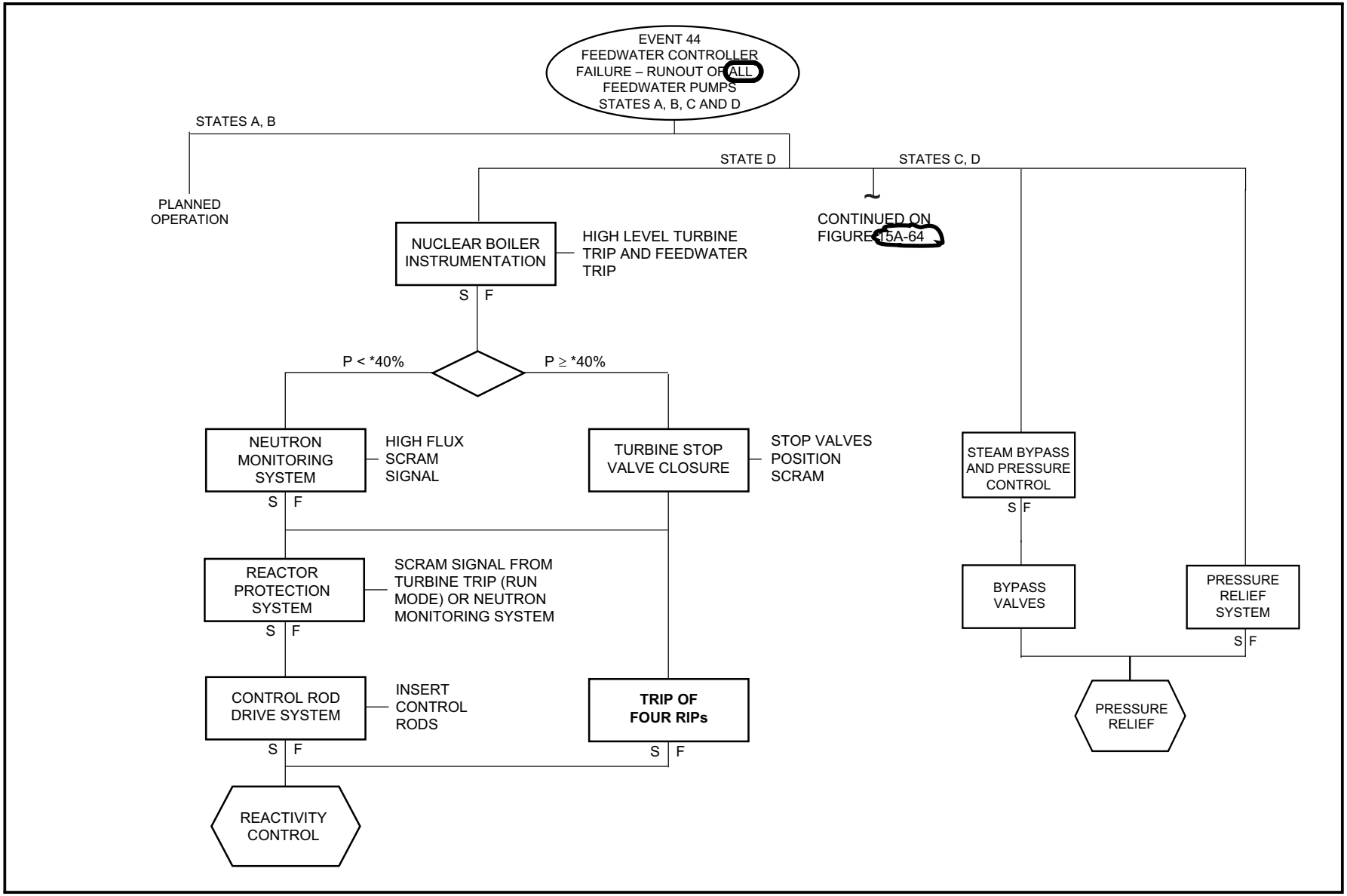


Figure 15A-51 Protection Sequences for Feedwater Controller Failure—Runout All Pumps

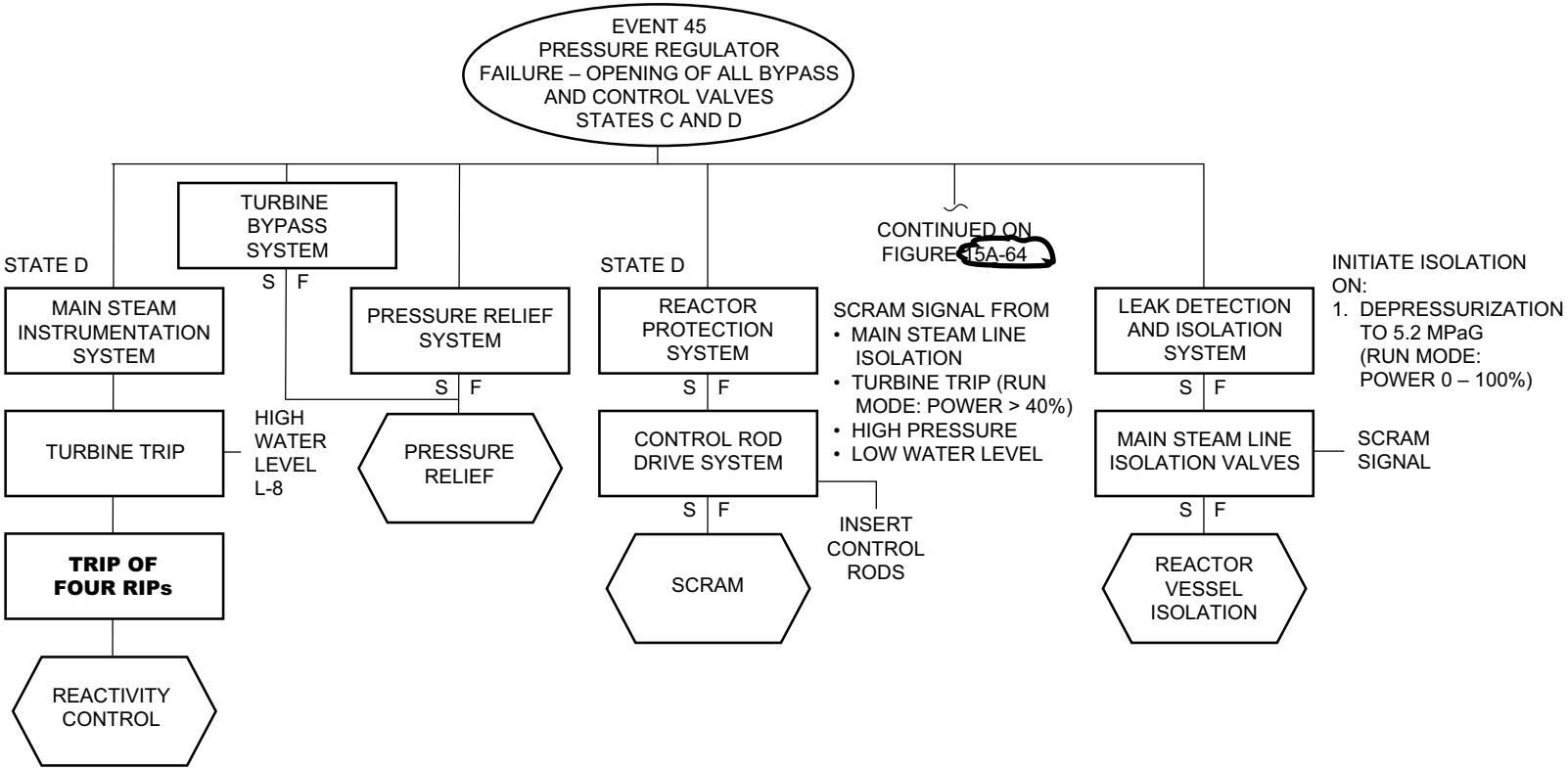


Figure 15A-52 Protection Sequences for Pressure Regulator Failure—Opening of All Bypass and Control Valves

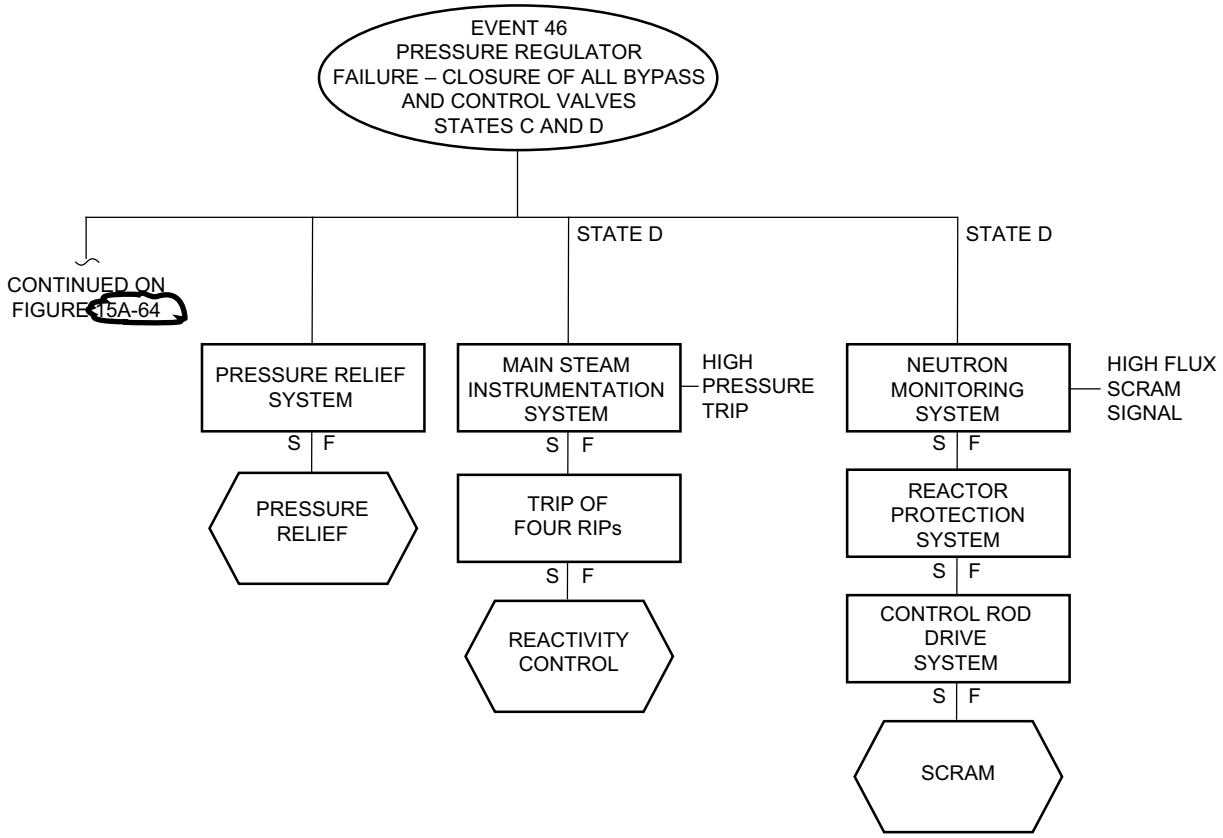


Figure 15A-53 Pressure Regulator Failure—Closure of All Bypass Valves and Control Valves

Figure 15A-54 Not Used

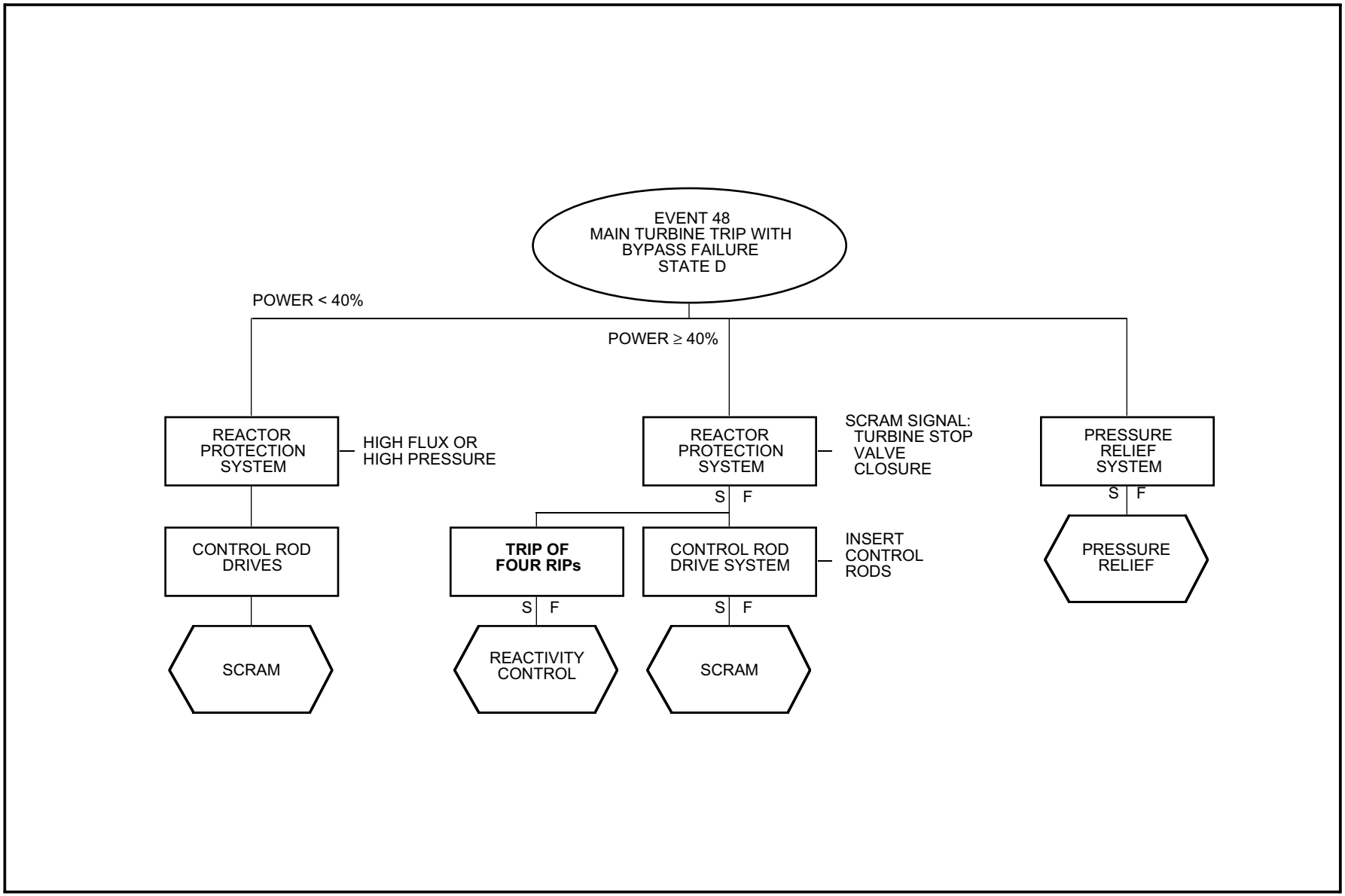


Figure 15A-55 Protection Sequences Main Turbine Trip—with Bypass Failure

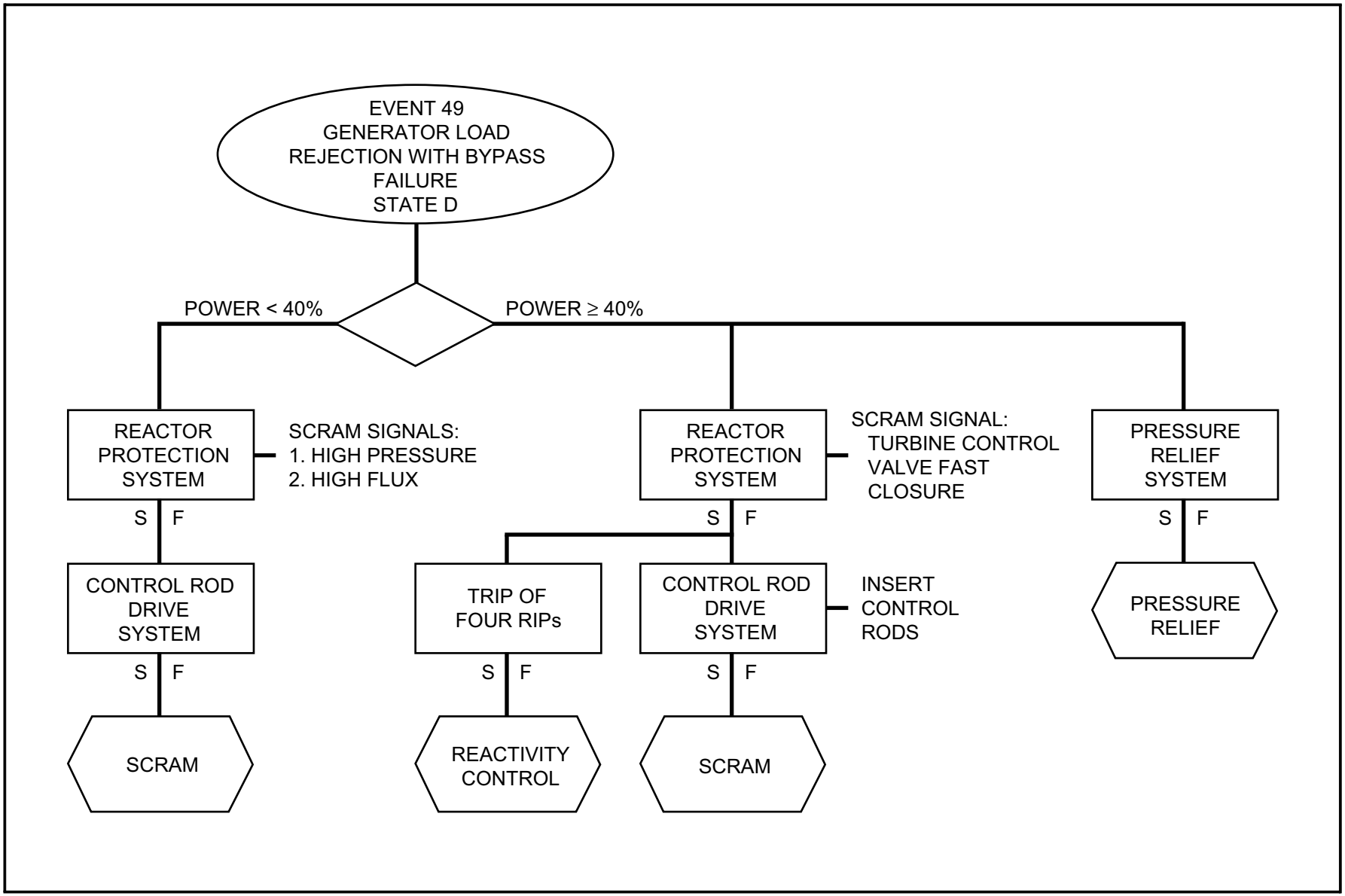


Figure 15A-56 Protection Sequences Main Generator Load Rejection—with Bypass Failure

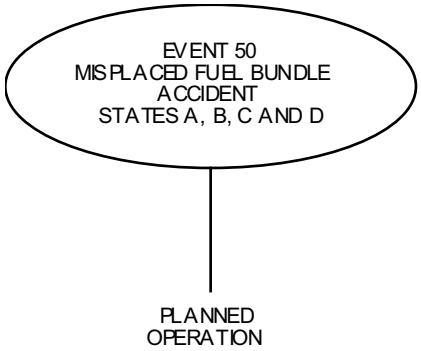


Figure 15A-57 Protection Sequence for Misplaced Fuel Bundle Accident

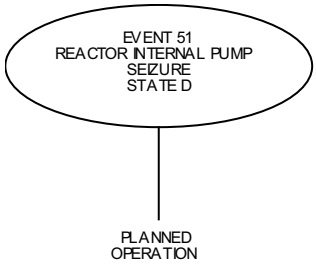


Figure 15A-58 Protection Sequence for Reactor Internal Pump Seizure

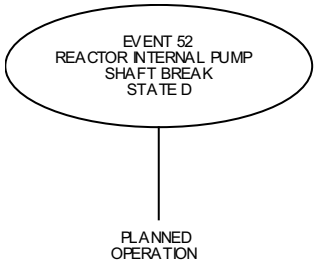


Figure 15A-59 Protection Sequence for RIP Shaft Break

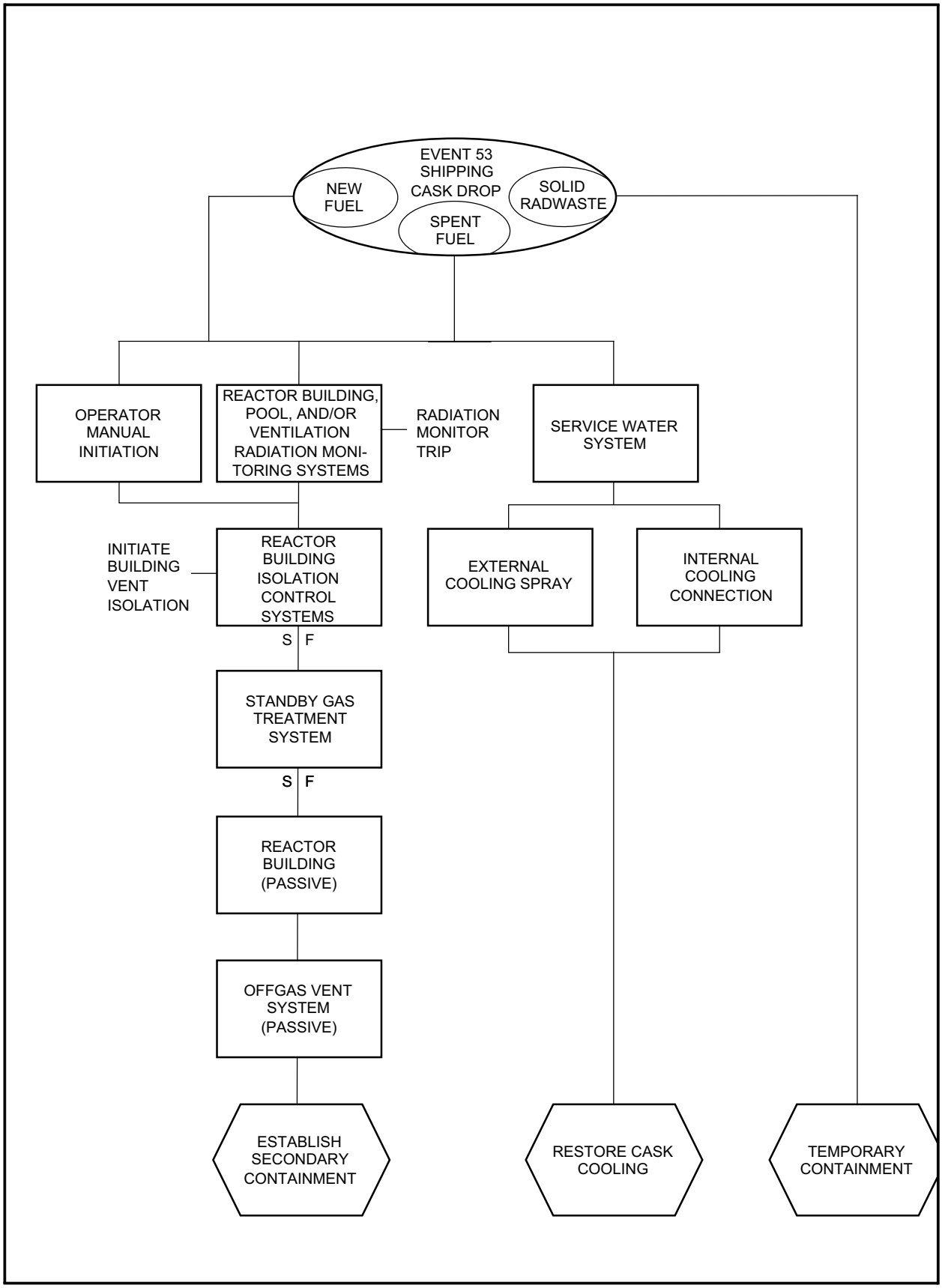


Figure 15A-60 Protection Sequence for Shipping Cask Drop

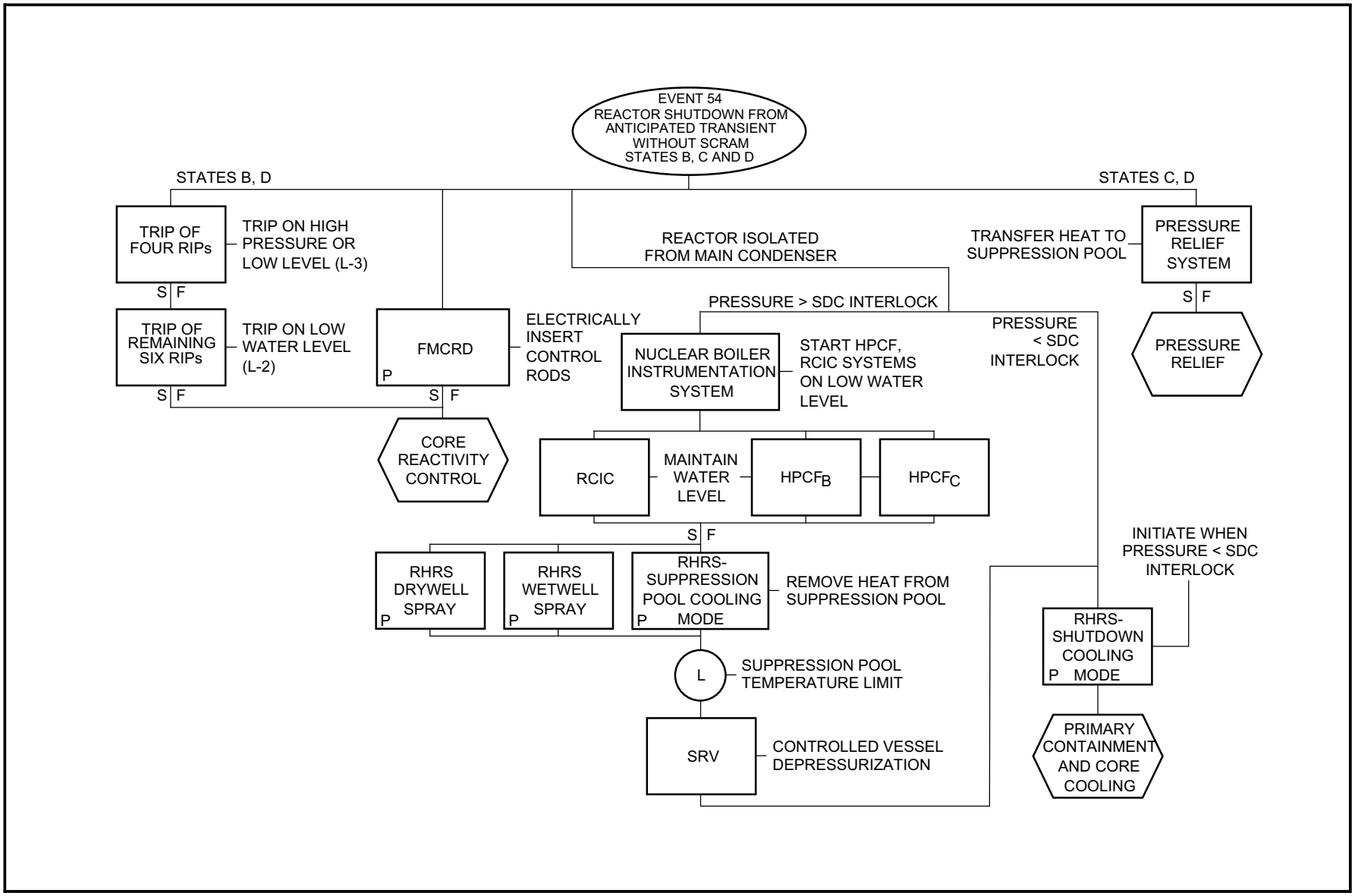


Figure 15A-61 Protection Sequence for Reactor Shutdown—from Anticipated Transient Without Scram

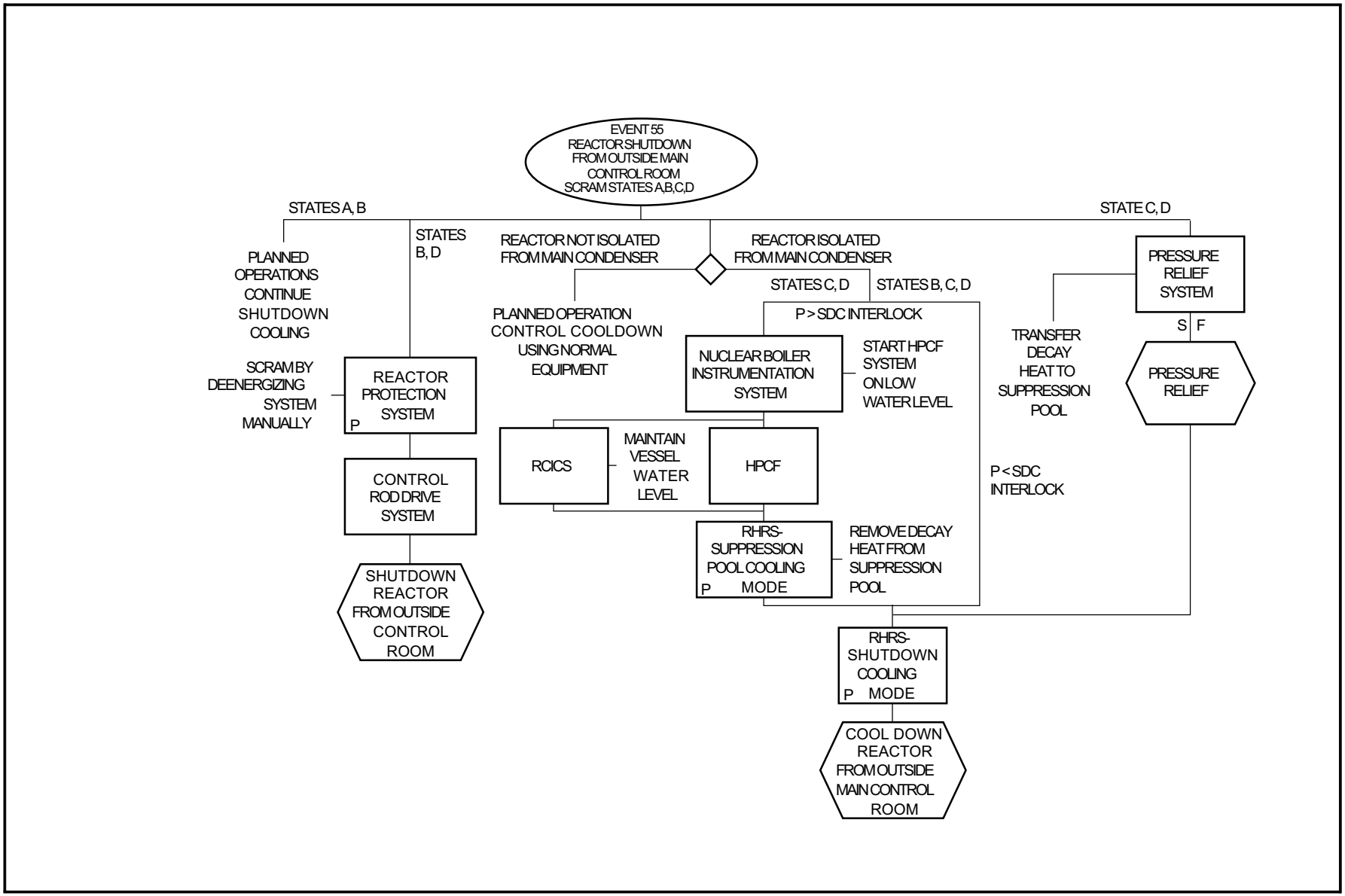


Figure 15A-62 Protection Sequence for Reactor Shutdown—from Outside Main Control Room

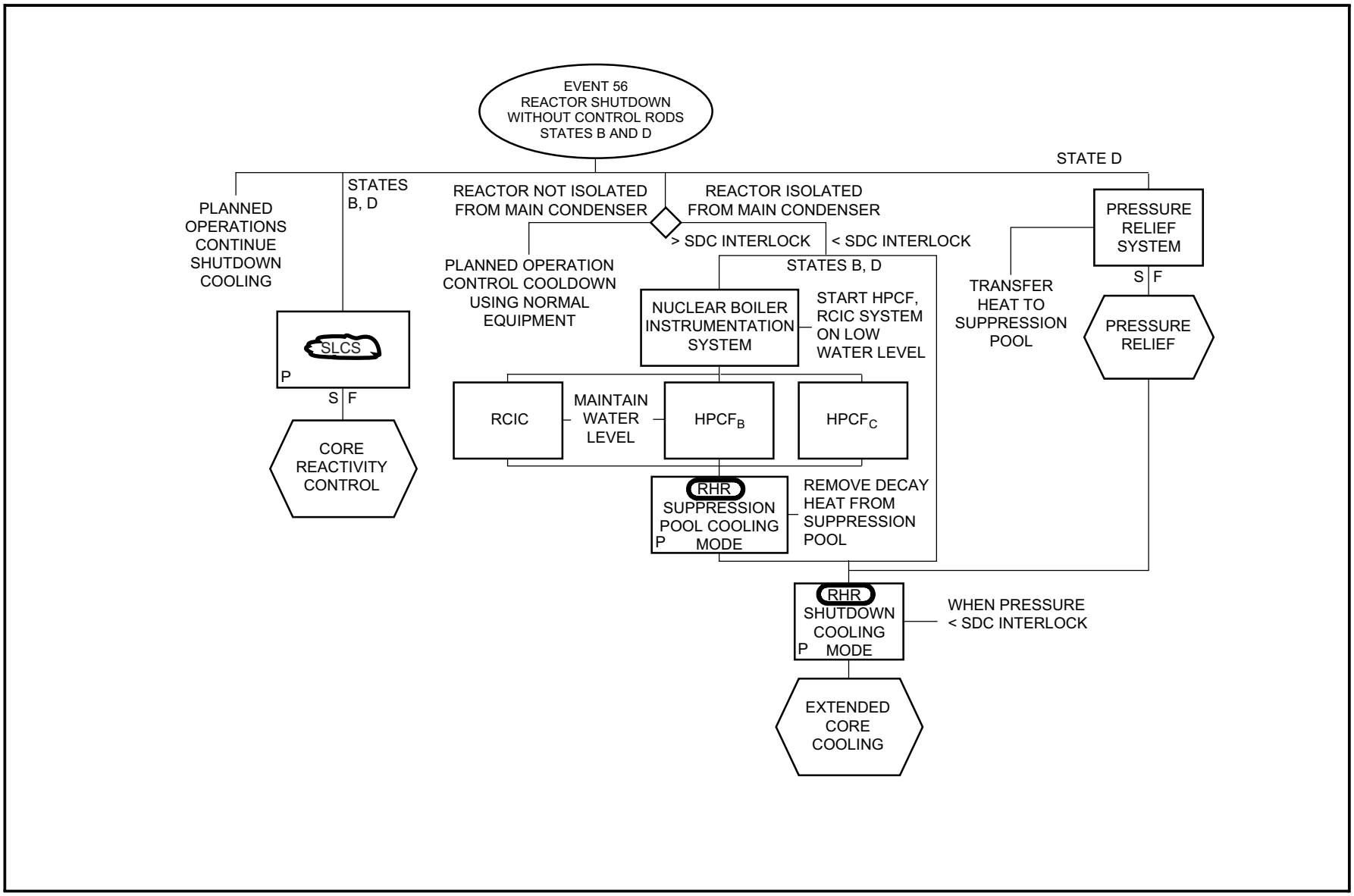


Figure 15A-63 Protection Sequence for Reactor Shutdown—Without Control Rods

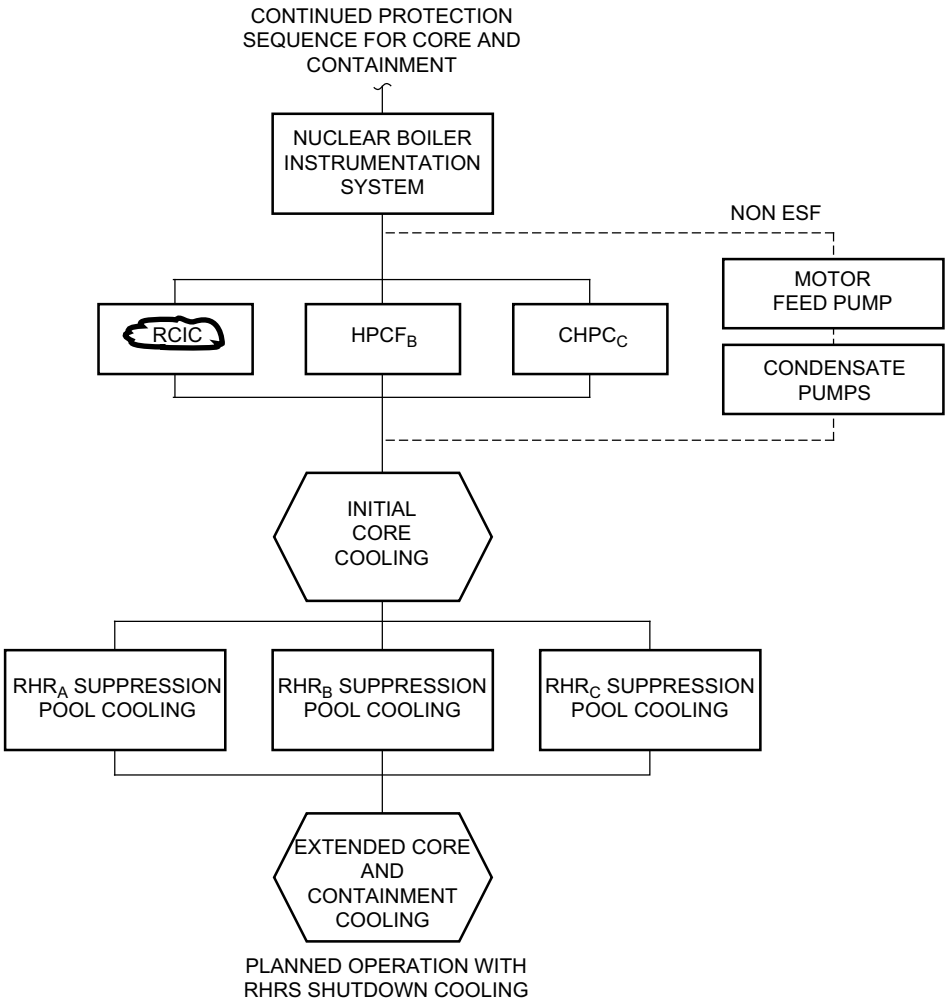


Figure 15A-64 Protection Sequence for Core and Containment Cooling for Loss of Feedwater and Vessel Isolations

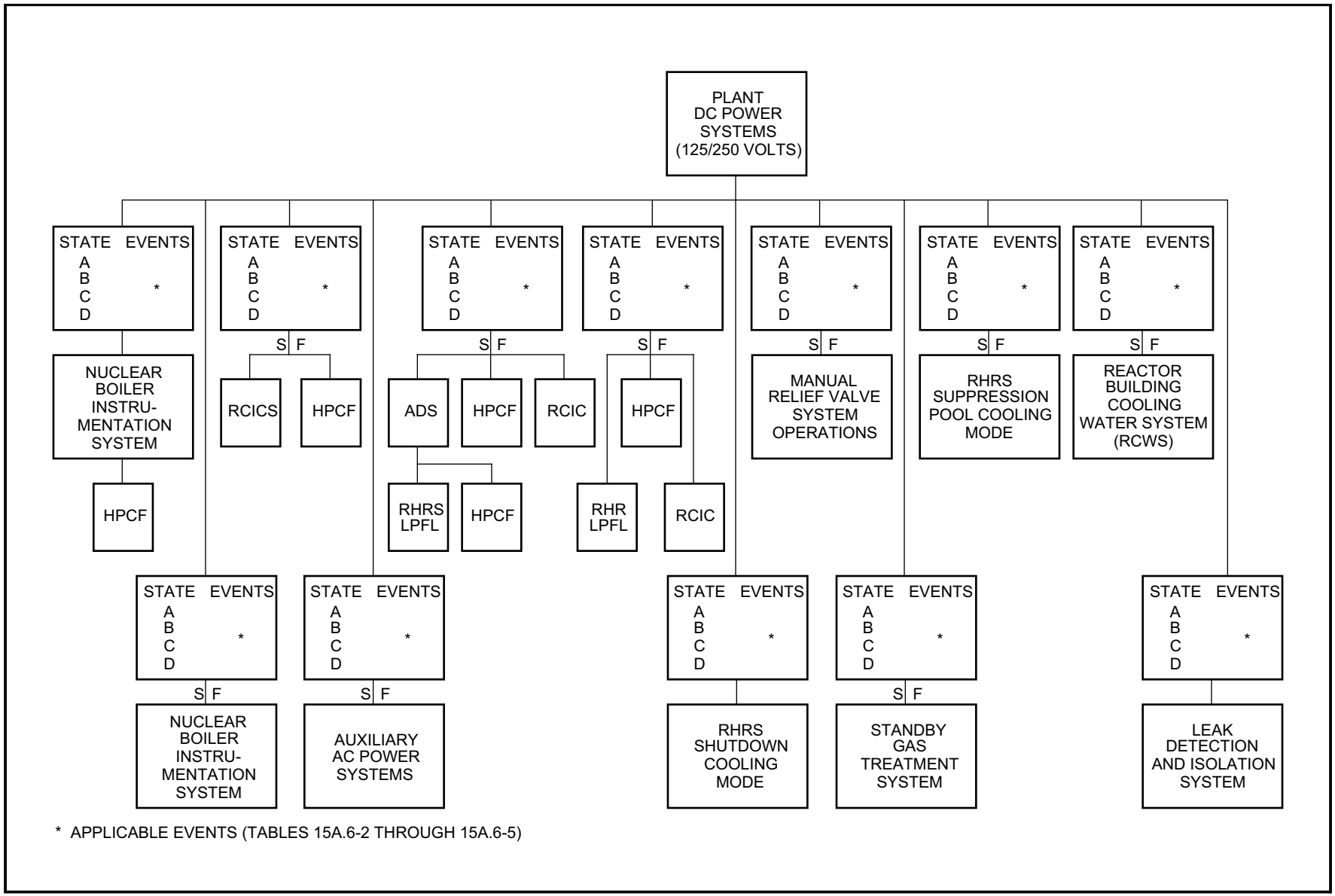


Figure 15A-65 Commonality of Auxiliary Systems—DC Power Systems (125/250 Volts)

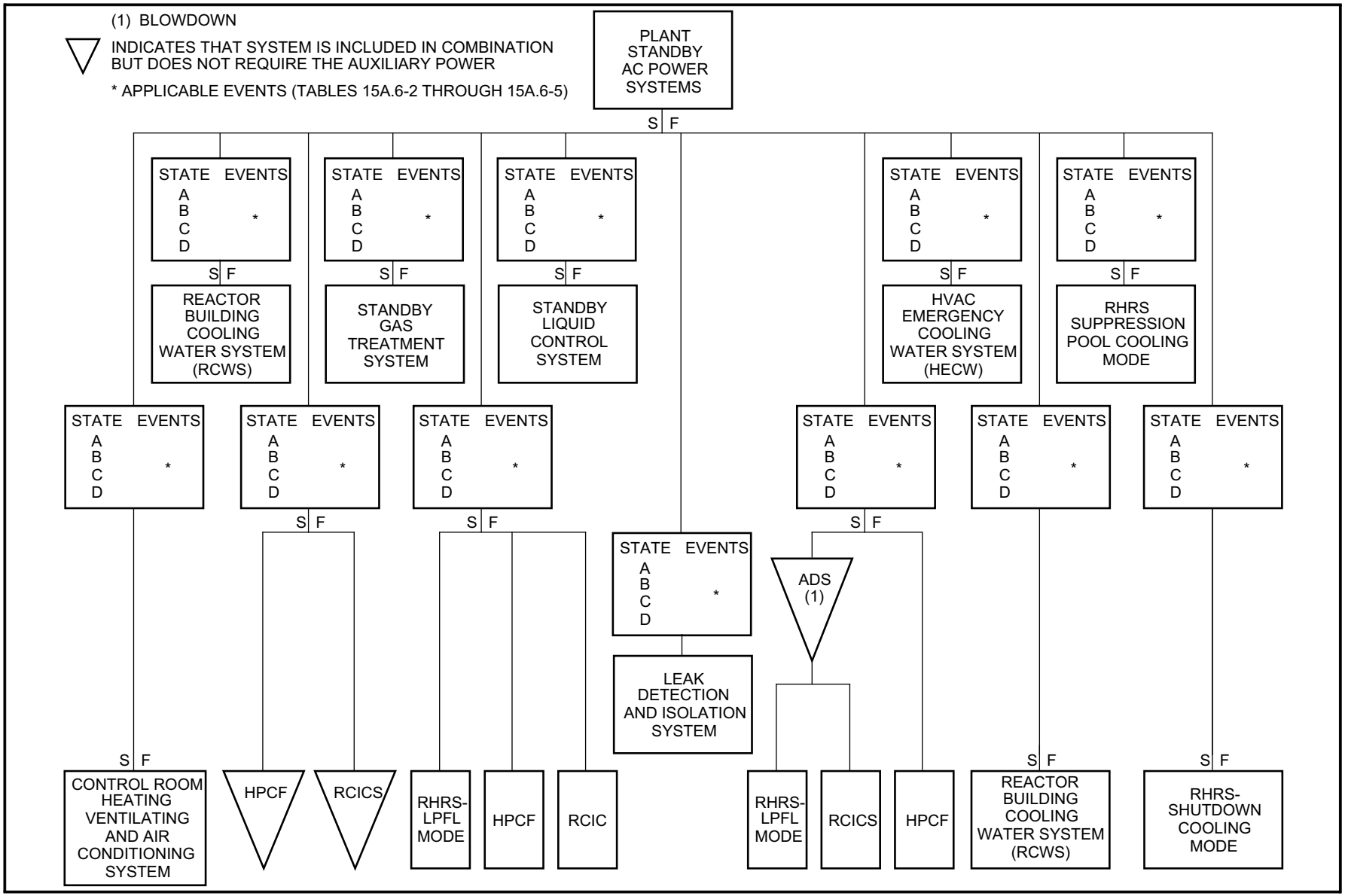


Figure 15A-66 Commonality of Standby AC Power Systems (120/480/6900 Volts)

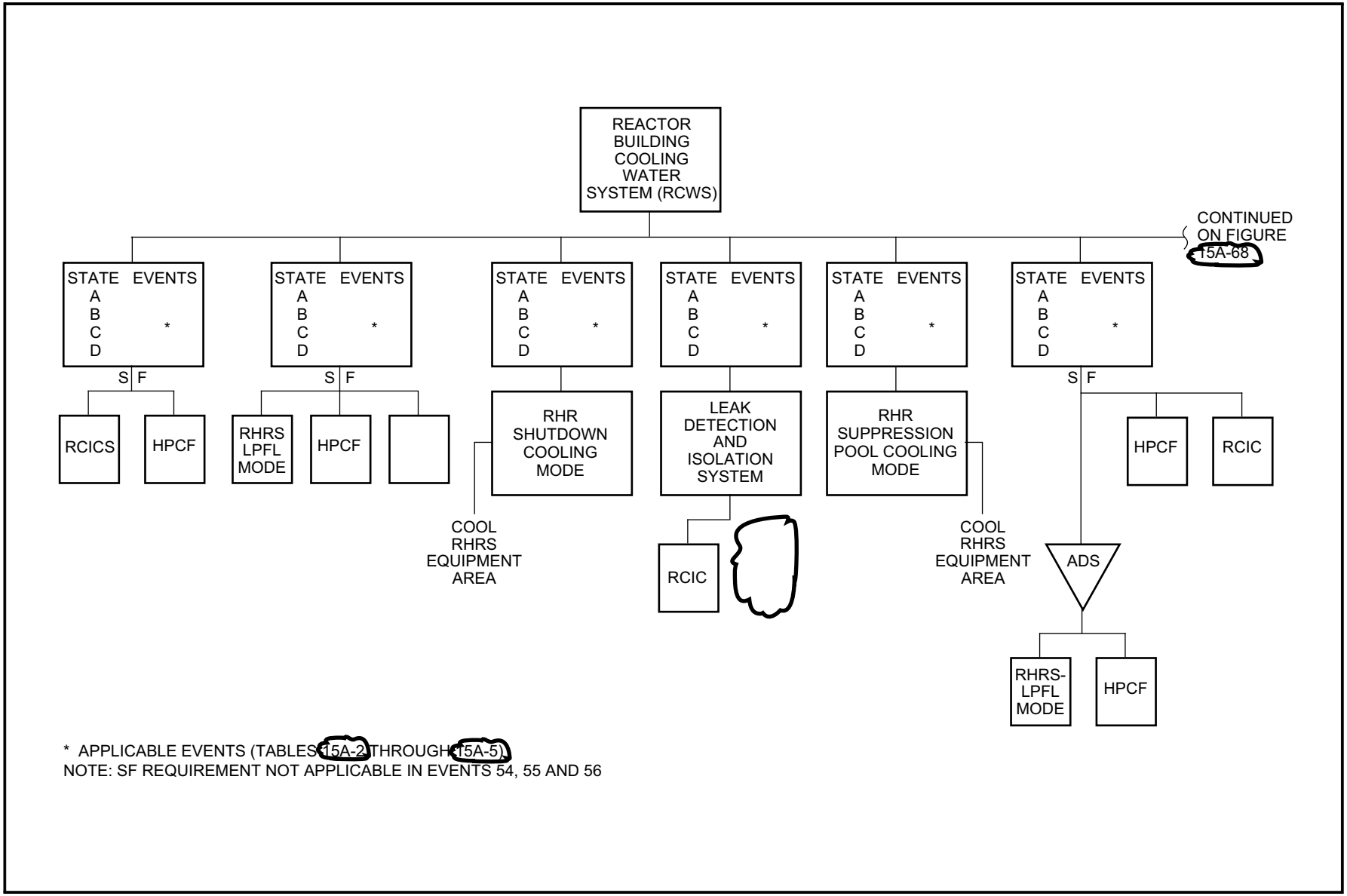


Figure 15A-67 Commonality of Auxiliary Systems—Reactor Building Cooling Water System (RCWS)

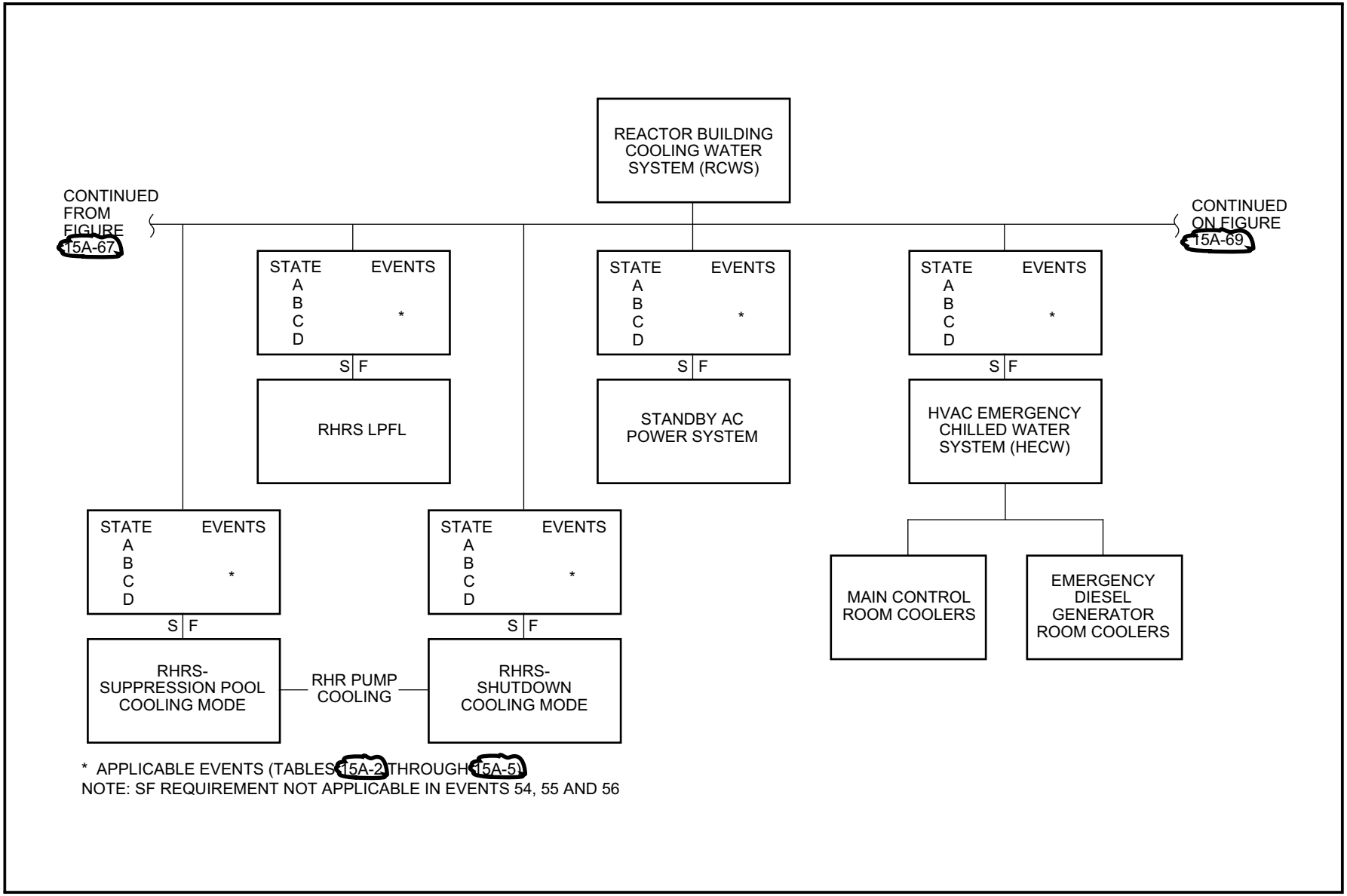
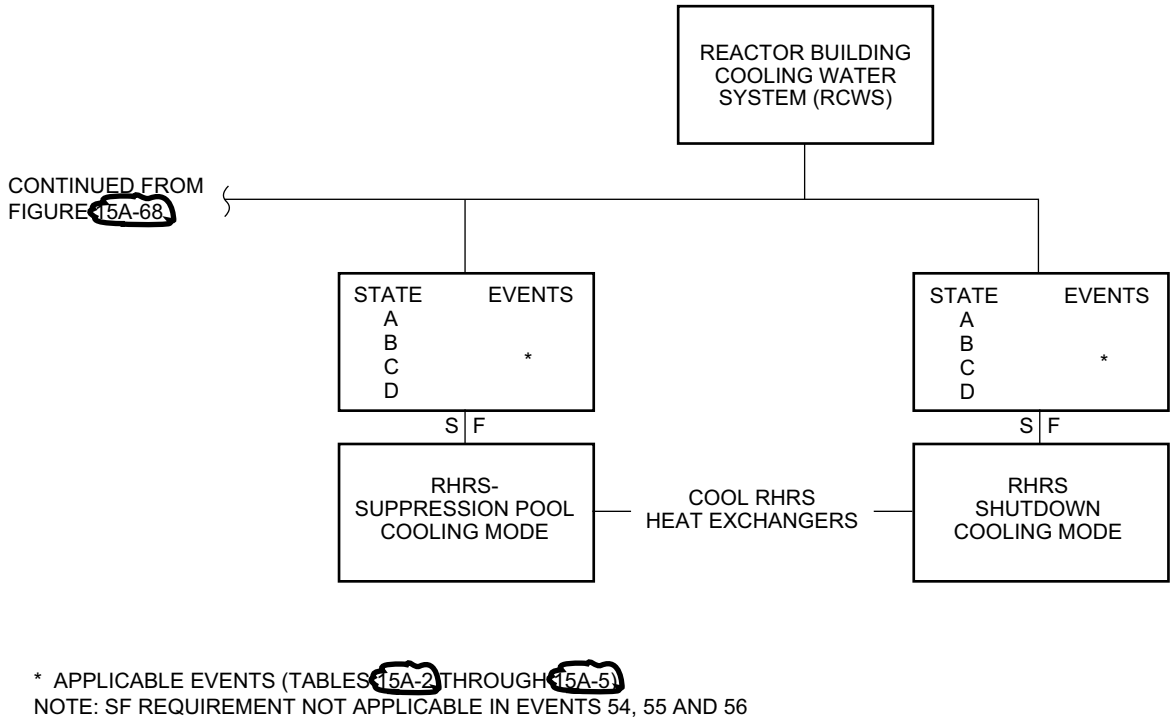


Figure 15A-68 Commonality of Auxiliary Systems—Reactor Building Cooling Water System (RCWS) (Continued)



* APPLICABLE EVENTS (TABLES 15A-2 THROUGH 15A-5)
NOTE: SF REQUIREMENT NOT APPLICABLE IN EVENTS 54, 55 AND 56

Figure 15A-69 Commonality of Auxiliary Systems—Reactor Building Cooling Water System (RCWS) (Continued)

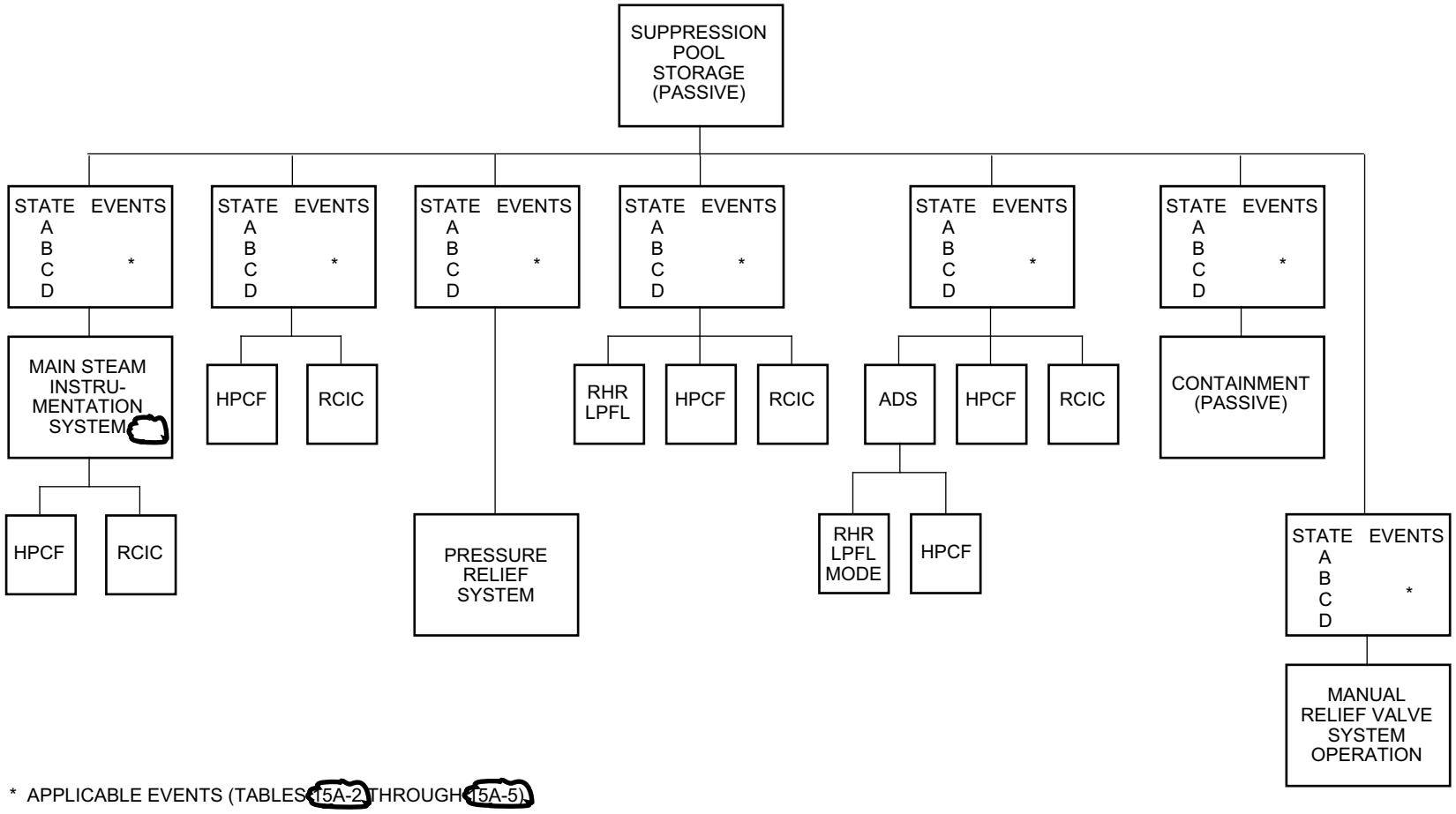


Figure 15A-70 Commonality of Auxiliary Systems—Suppression Pool Storage