ARKANSAS POWER & LIGHT COMPANY
POST OFFICE BOX 551 LITTLE ROCK, ARKANSAS 72203 (501) 371-4000

November 7, 1979

1-119-6

Director of Nuclear Reactor Regulation
ATTN: Mr. R. W. Reid, Chief
Operating Reactor Branch #4
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Subject: Arkansas Nuclear One-Unit 1
Docket No. 50-313
License No. DPR-51
Abnormal Transient Operating
Guidelines Program
(File: 1510.1)

Gentlemen:

Pursuant to a verbal request by Mr. Tom Novak of the NRC staff in a meeting in Lynchburg, Virginia on October 15, 1979, and later confirmed via a telephone conversation between your Mr. R. Capra and our Mr. D. Mardis, the following information as it relates to the Abnormal Transient Operating Guidelines (ATOG) Program for Arkansas Nuclear One - Unit 1 is provided.

Narrative Description of the ATOG Program Technique entitle "Safety Function and Protection Sequence Analysis", by R. A. Fortney et al (5 copies).	Attachment 1
Explanation of the Role of Safety Sequence and System Auxiliary Diagram in the Development of Abnormal Transients Operating Guidelines (5 copies).	Attachment 2
Excessive Feedwater Safety Sequence Diagram for Arkansas Nuclear One-Unit 1 (1 copy) - preliminary version without review.	Attachment 3

716 306

7911160 542

We note a copy of the Excessive Feedwater Event Tree was provided to the NRC staff at the Lynchburg meeting. Also, the program has not progressed to the point where draft guidelines are available.

From our discussion with the B&O Task Force, we understand this information will be used to evaluate the ATOG Program prior to a meeting with the B&W Owner Group.

Very truly yours,

John M. Griffin for

David C. Trimble
Manager, Licensing

DCT/DGM/ew

SAFETY FUNCTION AND PROTECTION SEQUENCE ANALYSIS

Authored by

R. A. Fortney
J. T. Snedeker

of
EDS Nuclear

and

J. E. Howard
W. W. Larson

of
Boston Edison Company

presented at
American Nuclear Society
Winter Meeting
November 11-16, 1973
San Francisco, California

Safety Function and Protection Sequence Analysis

Abstract

Today's complex nuclear plant safety requirements demand a planned and systematic engineering approach to identify the functional design requirements of the nuclear plant systems. This systems engineering concept is required to ensure that the nuclear plant design satisfies the various federal regulations and industry standards. The Safety Function and Protection Sequence Analysis provides such a systematic design verification process. The plant safety functions essential to achieving acceptable consequences following postulated accidents and transients are first carefully identified, and then the sequence of prime system responses that form redundant success paths to the safety functions are diagrammed as Safety Sequence Diagrams (SSD). Systems that act as essential auxiliaries in supporting the prime safety systems are functionally diagrammed on Safety Systems Auxiliary Diagrams (SSAD). When complete, the SSD's and SSAD's form the basis for comprehensive design review of all safety related systems. Because the full range of plant conditions is considered in evaluating each postulated event, the true design criteria and requirements are easily derived and documented for each safety related system, structure and component; the Quality Assured Items List is established; and redundancy and separation criteria are set. The SSD's and SSAD's also facilitate the identification of Seismic Category I equipment and structures. Systematic criteria are established for protection against pipe whip, jet impingement, fire and flooding. The information on the SSD's and SSAD's also forms the basis for the development of operating technical specifications. The concentrated effort required to perform the Safety Function and Protection Sequence Analysis is repaid many times over through the resulting benefits the analysis brings to today's nuclear project.

Introduction

Developments over the past decade in nuclear plant safety technology have given birth to numerous technically complex nuclear plant design and operational requirements. The proper application of the AEC requirements and industry codes and standards offers a significant challenge to nuclear plant engineers, managers and operators alike. The overall effect of the Safety Function and Protection Sequence Analysis is to systematize the identification of the functional design requirements to the nuclear power plant design. Developed as a systematic approach to the nuclear safety aspects of the Pilgrim Unit 2 design, the Safety Function and Protection Sequence Analysis (SFPSA) identifies the necessary and sufficient functional design requirements of the nuclear power station to ensure protection of the public health and safety.

The SFPSA provides the following specific benefits for a nuclear project:

1. A complete response to Section 15.1 of the AEC's *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.*
2. A systematic and consistent identification of all systems, structures and components that must be on the Quality Assured Items List and subjected to a Quality Assurance Program satisfying the requirements of 10CFR50, Appendix B.
3. A systems level design verification process satisfying, in part, the design control requirements of 10CFR50, Appendix B.

4. A systems level failure modes and effects analysis which assists in the identification of the necessary inputs for the development of functional, physical and electrical separation criteria.
5. A systems level, single failure analysis as required by IEEE-279, IEEE-379 and Regulatory Guide 1.53.
6. A documented basis for establishing operating plant technical specifications for inclusion in Chapter 16.0 of the Safety Analysis Report.
7. A documented basis for the preparation and review of those plant operating procedures which address abnormal and accident conditions.
8. A learning and training aid for engineers and operators to facilitate understanding of the integrated plant response to various plant abnormal and accident conditions.

TABLE I

EVENTS CLASSIFICATION FOR PILGRIM 2

SFPSA EVENT CATEGORY	EVENT FREQUENCY	10CFR50, APP. A EVENT CATEGORY	10CFR50, APP. I EVENT CATEGORY	ANSI 18.2 EVENT CATEGORY
Planned Operation	Routine	Normal Operation	Normal Reactor Operation	Condition I; Normal Operation
Expected Operational Occurrences	$\geq$ 1/year	Anticipated Operational Occurrences	Expected Operational Occurrences	Condition II; Incidents of Moderate Frequency
Infrequent Operational Occurrences	1/40 yrs $\leq$ f $<$ 1/yrs	Anticipated Operational Occurrences	Expected Operational Occurrences	Condition III; Infrequent Incident
Accident	$<$1/40 yrs	———	———	Condition IV; Limiting Faults

Development of the Safety Function and Protection Sequence Analysis

The fundamental objective of the nuclear plant design is to develop the functional requirements of the plant's safety systems to prevent the occurrence of specified unacceptable results during a postulated event. To achieve this proper plant design, a consistent systems engineering analysis must be developed. The Safety Function and Protection Sequence Analysis, the development of which is described in the following paragraphs, is an example of this required systems engineering analysis.

Event Classification and the Unacceptable Results

The first task in the analysis is to categorize the postulated events and to select the unacceptable results for each event category. The postulated events are grouped into event categories based upon some common event initiating characteristic, such as expected frequency of occurrence or the event initiating mechanism (e.g., pipe breaks). Event categories are not based upon event consequences because such categorization would involve circular reasoning. The event consequences are dependent upon the plant safety systems for which the design requirements are sought. Consideration is given to the various event classifications set forth in such regulatory and industry literature as 10CFR50 and its appendices and ANSI N18.2. Table I lists the event categories used in the Boston Edison Pilgrim 2 SFPSA and compares them to the event classifications used in other industry publications. Expected frequency of occurrence was used as the basic event classification characteristic.

After classifying the events into categories, the specific unacceptable results applicable to each category are defined. To define the unacceptable results the specific design limits associated with the proposed nuclear plant are identified. For the Boston Edison Pilgrim 2 analysis these limits were selected from the design criteria for the plant and included consideration of the AEC's Federal Regulation, Safety and Regulatory Guides, Interim Acceptance Criteria and Interim Policy Statement on Emergency Core Cooling; and the ASME codes and IEEE standards. Because the unacceptable results must be specific and measurable to be useful in the SFPSA, certain key plant variables or parameters are associated with the specific design limits of the plant, and thus with the unacceptable results. Examples of these plant parameters are fuel centerline temperature, site boundary dose, and containment structure stress. The unacceptable results are developed from the design limits using these key plant variables. Table II lists the unacceptable results used in the Pilgrim 2 analysis.

Safety Functions

Having defined the unacceptable results for each event category, the plant safety functions must be identified and developed. These safety functions are the functional means whereby the important plant variables are controlled or limited following a postulated event to avoid the unacceptable results. The development of the safety function is one of the major steps in the SFPSA. As a safety function is developed, the initial functional design requirements of the nuclear plant systems are established. For example, the safety function "Trip Reactivity Control" establishes the functional requirement for the rapid insertion of negative reactivity into the reactor core to prevent a certain plant parameter, DNBR, from exceeding its design limit.

The development of the safety functions is complete when it establishes all the functional design requirements essential to avoid the unacceptable results for all the event categories. To assist in developing all the required safety functions, a matrix is used to relate the safety functions to the unacceptable results. This enables the plant analyst to gain a functional overview of the safety functions and their effects. Table III lists the safety functions identified for the Pilgrim 2 unit. Table IV is the matrix showing the correspondence between the safety functions and the unacceptable results for the Pilgrim 2 SFPSA.

TABLE II

UNACCEPTABLE RESULTS FOR PILGRIM 2 SFPSA

EXPECTED OPERATIONAL OCCURRENCES

A. Radioactive Material Release

1. Radioactive material release to the environment exceeding the limits of 10CFR50, proposed Appendix I.

B. Fuel Limits

1. DNBR < 1.3 (W-3 correlation)

2. Fuel centerline temperature ≥ UO_2 melting temperature

C. Reactivity Limits

1. Inability to achieve a shutdown margin at no load reactor coolant temperature immediately following automatic reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted.

2. Inability to achieve and maintain a shutdown margin following the event.

D. Primary System Stress

1. Primary system stress in excess of that for which the primary system is designed, as determined by the following:

   a. Primary system pressure > 2750 psia when reactor coolant system temperature is ≥ LST.

   b. Primary system pressure > allowable when reactor coolant system temperature < LST.

   c. Primary system thermal transients in excess of those considered in the primary system design.

E. Secondary System Stress

1. Secondary system stress in excess of that for which the secondary system is designed, as determined by the following:

   a. Secondary system pressure > 1320 psia.

   b. Secondary system thermal transients in excess of those considered in the secondary system design.

F. Plant Environmental Conditions

1. Uninhabitability of the control room and other plant locations where manual actions are essential.

INFREQUENT OPERATIONAL OCCURRENCES	ACCIDENTS
A. Radioactive Material Release 1. Radioactive material release to the environment exceeding the limits of 10CFR20.	A. Radioactive Material Release 1. Radioactive material release to the environment that would result in exceeding the guideline values of 10CFR100.
B. Fuel Limits 1. DNBR < 1.3 (W-3 correlation) 2. Fuel centerline temperature ≥ UO_2 melting temperature	B. Fuel Limits 1. Fuel centerline temperature ≥ UO_2 melting temperature. 2. Peak fuel cladding temperature in excess of 2200° F. 3. Oxidation of fuel cladding at any location in excess of 17%. 4. Metal-water reaction generating more H_2 than 1% of the H_2 that would be generated if all cladding reacted.
C. Reactivity Limits 1. Inability to achieve a shutdown margin at no load reactor coolant temperature immediately following automatic reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted. 2. Inability to achieve and maintain a shutdown margin following the event.	C. Reactivity Limits 1. Inability to achieve a shutdown margin at no load reactor coolant temperature immediately following automatic reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted. 2. Inability to achieve and maintain a shutdown margin following the event.
D. Primary System Stress 1. Primary system stress in excess of that for which the primary system is designed, as determined by the following: a. Primary system pressure > 2750 psia when reactor coolant system temperature is ≥ LST. b. Primary system pressure > allowable when reactor coolant system temperature < LST. c. Primary system thermal transients in excess of those considered in the primary system design.	D. Primary System Stress 1. Primary system stress in excess of that for which the primary system is designed, as determined by the following: a. Primary system pressure > 2750 psia when reactor coolant system temperature is ≥ LST. b. Primary system pressure > allowable when reactor coolant system temperature < LST. c. Primary system thermal transients in excess of those considered in the primary system design.
E. Secondary System Stress 1. Secondary system stress in excess of that for which the secondary system is designed, as determined by the following: a. Secondary system pressure > 1320 psia. b. Secondary system thermal transients in excess of those considered in the secondary system design.	E. Secondary System Stress 1. Secondary system stress in excess of that for which the secondary system is designed, as determined by the following: a. Secondary system pressure > 1320 psia. b. Secondary system thermal transients in excess of those considered in the secondary system design.
F. Plant Environmental Conditions 1. Uninhabitability of the control room and other plant locations where manual actions are essential.	F. Containment Stress 1. When containment is required, containment stress in excess of that for which the containment is designed, as determined by the following: a. Containment pressure > 60 psig. b. Thermal transients affecting either containment concrete or liner plate in excess of those considered in the containment design. c. Existence of a flammable or explosive mixture of hydrogen and oxygen (i.e. > 4% H_2 with ≥ 5% O_2 or > 5% O_2 with ≥ 4% H_2) in areas of the plant where safety systems are located which are required in response to the originating accident.
	G. Plant Environmental Conditions 1. Exposure of station personnel in the control room in excess of 5 Rem whole body, 15 Rem skin, and 30 Rem thyroid over the duration of the accident. 2. Uninhabitability of the control room and other plant locations where manual actions are essential.

TABLE III

SAFETY FUNCTIONS FOR PILGRIM 2 SFPSA

Safety Function *	Functional Description
Trip Reactivity Control	Rapid insertion of negative reactivity into the core to produce subcritically immediately following an evaluated event.
Transient Reactivity Control	Insertion of negative reactivity into the core sufficient to compensate for cooldown of the reactor coolant system.
Long Term Reactivity Control	Establishment of a sufficient boron concentration in the core such that the reactor is maintained subcritical following the event.
Emergency Core Cooling - Injection Phase	Provision of coolant to the reactor core immediately following an accident and prior to the time that manual action can be taken.
Emergency Core Cooling- Recirculation Phase	Provision of coolant to the reactor core some time after the accident has occurred and at a time when manual action can be taken and in such a way that the core coolant is recirculated back into the primary system after it leaks out.
Reactor Heat Removal	Cooling of the core by other than injection of coolant directly to the core.
Pressure Control - Primary System	Maintenance of primary system pressure within allowable pressure limits and ensuring that the primary steam bubble remains in the pressurizer.
Pressure Control - Secondary System	Maintenance of secondary system pressure within allowable pressure limits.
Pressure Control - Containment	Maintenance of containment pressure within allowable pressure limits when containment is required.
Temperature Control - Containment	Maintenance of containment temperature within allowable temperature limits when containment is required.

* Where appropriate, safety function descriptions are modified with such phrases as "initial", "long term", "above LST", etc.

Safety Function *	Functional Description
Combustible Gas Control	Conditioning of post-accident atmosphere or treatment of accident-generated flammables to prevent formation of flammable or explosive mixtures.
Radioactive Material Treatment	Mechanical or chemical treatment of radioactive materials to reduce the quantity that escape or are discharged to the environs.
Establish Containment	Trapping of radioactivity inside the containment to prevent escape to the environs.
Primary System Isolation	Isolation of all or part of the primary system to prevent coolant loss or radioactivity discharge.
Secondary System Isolation (blowdown)	Isolation of all or part of the secondary system to prevent or reduce the discharge of secondary system coolant into the containment, so that containment temperature and pressure are maintained within allowable limits.
Secondary System Isolation (heat sink)	Isolation of all or part of the secondary system to prevent or reduce the discharge of secondary coolant, so that at least one steam generator can function as a heat sink for primary system energy.
Secondary System Isolation (radioactivity)	Isolation of all or part of the secondary system to prevent the discharge of radioactive materials to the environs.
Steam Generator Inventory Control	Maintenance of a proper level in at least one steam generator for use as a primary system heat sink and prevention from injecting cold feedwater into a dry and hot steam generator.
Control Station Habitability	Conditioning of the post-event control station (Control room and other locations where manual actions are essential) atmosphere to ensure habitability and control of personnel radiation exposure.

TABLE IV

SAFETY FUNCTIONS AND UNACCEPTABLE RESULTS MATRIX FOR PILGRIM 2 SFPSA

Safety Functions	Fuel Limits	Reactivity Limits	Primary System Stress	Secondary System Stress	Containment Stress
Trip Reactivity Control	Acc: B.1 EOO: B.1-2 IOO: B.1-2	Acc: C.1 EOO: C.1 IOO: C.1	Acc: D.1.a EOO: D.1.a IOO: D.1.a		
Transient Reactivity Control		Acc: C.2 EOO: C.2 IOO: C.2			
Long Term Reactivity Control		Acc: C.2 EOO: C.2 IOO: C.2			
Emergency Core Cooling - Injection Phase	Acc: B.1-4				
Emergency Core Cooling - Recirculation Phase	Acc: B.1-4				
Reactor Heat Removal	Acc: B.1,2 EOO: B.2 IOO: B.2				
Pressure Control - Primary System			Acc: D.1.a,b EOO: D.1.a,b IOO: D.1.a,b		
Pressure Control - Secondary System				Acc: E.1.a EOO: E.1.a IOO: E.1.a	
Pressure Control - Containment					Acc: F.1.a

Alphanumeric references refer to unacceptable results as listed on Table II

SAFETY FUNCTION	Radiological Release	Fuel Limits	Primary System Stress	Secondary System Stress	Containment Stress	Environmental Conditions
Temperature Control - Containment					Acc: F. 1. b	
Combustible Gas Control					Acc: F. 1. c	
Radioactive Material Treatment	Acc: A. 1 EOO: A. 1 IOO: A. 1					
Establish Containment	Acc: A. 1					
Primary System Isolation	Acc: A. 1					
Secondary System Isolation (blowdown)					Acc: F. 1. a, b	
Secondary System Isolation (heat sink)		Acc: B. 1-4 EOO: B. 1-2 IOO: B. 1-2				
Secondary System Isolation (Radioactivity)	Acc: A. 1					
Control Station Habitability						Acc: G. 1-2 EOO: F. 1 IOO: F. 1
Steam Generator Inventory Control		Acc: B. 1-4 EOO: B. 1-2 IOO: B. 1-2	Acc: D. 1. a, b, c EOO: D. 1. a, b, c IOO: D. 1. a, b, c	Acc: E. 1. a, b EOO: E. 1. a, b IOO: E. 1. a, b		

Legend: Acc = Accident
EOO = Expected Operational Occurrences
IOO = Infrequent Operational Occurrences

Operating States

Because each postulated event must be evaluated over the full range of normal plant conditions in which the event is possible, it is convenient to identify and define various plant operating states. The analyst can then more easily evaluate each event over the range of plant conditions within each operating state. The operating states to be used for the analysis of a specific plant are dependent upon the plant design. Table V defines the operating states used for the Pilgrim 2 unit, a two-loop pressurized water reactor.

TABLE V

PLANT OPERATING STATES FOR PILGRIM 2

Operating State	Reactivity Control Status	Primary System Status	Reactor Power
A - Refueling	All CEA's may be withdrawn *	0 psig T < 210° F	Nil
B - Cold Shutdown	< 1 shutdown group withdrawn; all others inserted ****	0 psig T < 210° F	Nil
C - Shutdown Cooling	< 1 shutdown group withdrawn; all others inserted ****	210° F < T < 350° F pressure per allowable ***	Nil
D - Heatup/Cooldown	< 1 shutdown group withdrawn; all others inserted ****	350° F < T < 556° F pressure per allowable ***	Nil
E - Hot Shutdown	< 1 shutdown group withdrawn; all others inserted **	2250 psia 556° F	Nil
F - Hot Standby	Any allowable CEA positions **	Temp/pressure per allowable	< 15%
G - Power	Any allowable CEA positions **	Temp/pressure per allowable	15 - 100%

* Reactor boron concentration such that reactor would have at least a 5% shutdown margin with all CEA's fully withdrawn.

** Reactor boron concentration such that reactor would have at least a 2% shutdown margin at no load reactor coolant temperature following reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted.

*** Pressure-temperature limits applicable during heatup and cooldown of reactor coolant system.

**** Reactor boron concentration such that reactor would have at least a 2% shutdown margin with all CEA's fully inserted.

Event Analysis

With the placement of each postulated event in its category, and with the unacceptable results and safety functions identified for event category, the analysis of each specific event can be performed.

The analysis of an event begins with the complete definition of the event. This includes the identification of the event (e.g., steamline break inside containment), the range of plant process variables which apply to the event (e.g., 350°F to 580°F for average reactor coolant temperature), and the listing of the applicable plant operating states (e.g., power operation, hot shutdown). After the event is completely defined, the analyst selects a specific set of initial plant process parameters (e.g., 100% power, rated temperature) to begin the event analysis. With this set of initial parameters, each unacceptable result associated with the event's category is examined to determine which unacceptable results could or could not occur as a result of the event. For example, the analyst determines that the unacceptable result concerning the existence of a flammable or explosive mixture of hydrogen and oxygen could not occur for a steamline break accident occurring outside containment.

Having determined which unacceptable results could occur for the event, a matrix such as that shown in Table IV is used to determine the safety functions associated with the specific set of initial parameters. To achieve these safety functions the specific plant safety systems and their required responses, or safety actions, are identified. A safety system is a system, active or passive, which must furnish the safety action as a result of a postulated plant event.

After identification of the required safety systems and their safety actions, the sensed variables are identified that cause or require the special system responses. In cases where the system does not automatically respond, the operator action required to initiate the safety system (e.g., starting the pump locally from the control room) is identified. As the safety systems and their actions are identified, they are arranged in functional order forming success paths, or protection sequences, leading to the required safety function. The arrangement of success paths becomes the Safety Sequence Diagram for the event. The Safety Sequence Diagram (SSD) becomes the analyst's major output in the SFPSA. Figure 1 is the format of the SSD's developed for the Boston Edison Pilgrim 2 analysis.

To depict the level of redundancy in the plant design on the SSD, a sufficient number of independent parallel paths is developed for each safety function such that no single component failure can prevent the achievement of the required safety function. Because many of the Pilgrim 2 systems (e.g., engineered safety features) have been designed with functional redundancy, certain safety functions require only one success path, i.e., no single active component failure can prevent the safety systems in the success path from achieving their special responses. If the analysis reveals a safety function for which functional redundancy does not exist, either with a parallel independent success path or safety system redundancy, then the plant design, configuration or functional response must be changed to achieve this redundancy.

The analysis of the postulated event is continued for its entire duration including post-event activities until some planned operation is resumed or the plant achieves a stable condition. A planned operation is considered resumed when the actions taken are identical to those described by normal operating procedures.

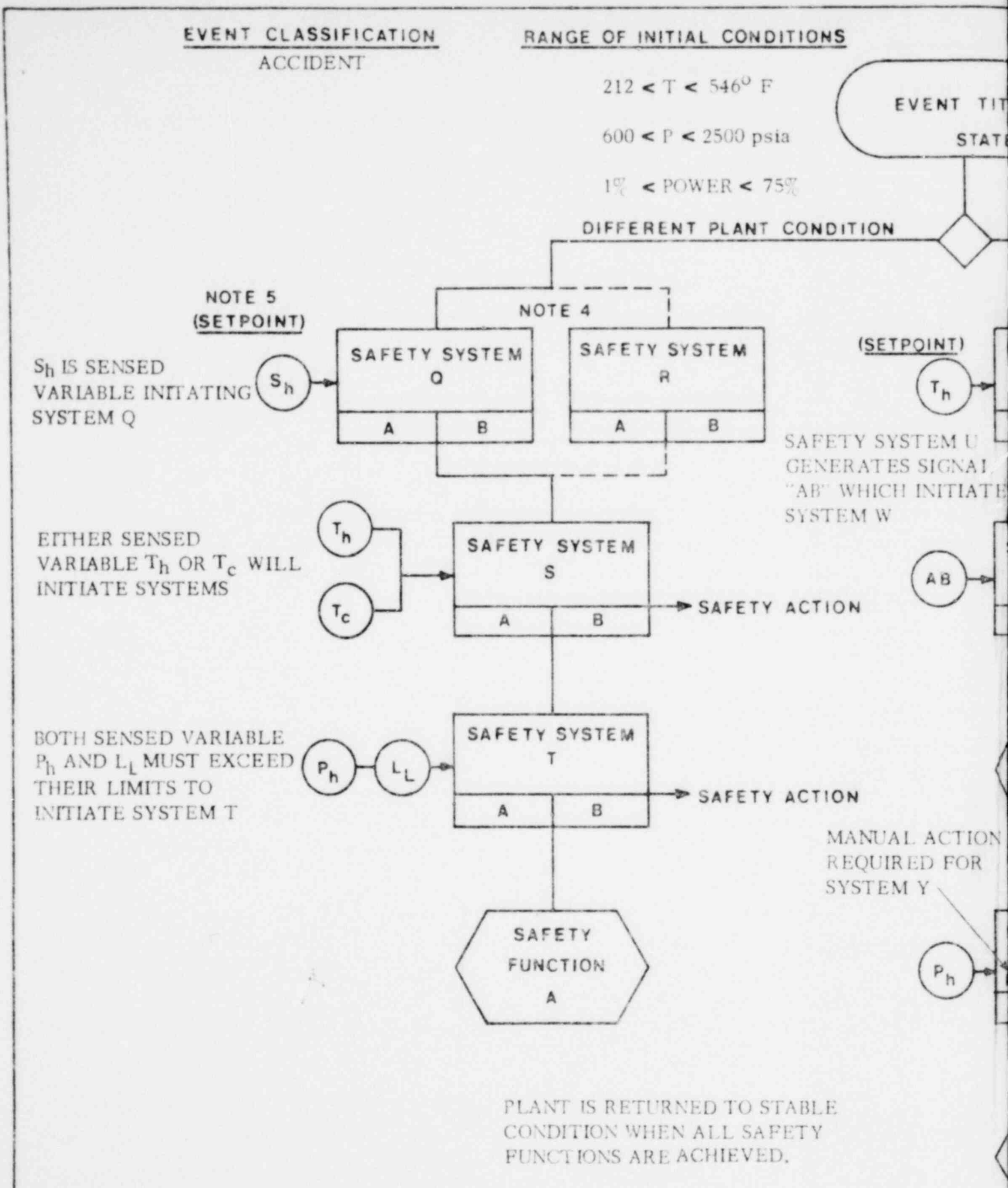
After the success paths and safety functions required for the initial set of plant conditions have been identified and illustrated on the Safety Sequence Diagram, the analyst will vary each plant process parameter from its initial condition value throughout its entire range for the event. During this parameter variation process, the analyst ensures that all required safety functions have been identified. If any additional required safety functions are identified, their required success paths must be determined in the same manner as done for the initial set of plant conditions. Additionally, as the parameters are varied, the analyst also determines which of the "initial condition" safety functions are still required. Each of these required safety functions is reviewed to ensure that the safety systems in the success path will provide their required safety actions under the different plant conditions. During this process, if any new success paths are discovered, they are diagrammed on the Safety Sequence Diagram with appropriate notation as to the specific conditions under which they are required. Also, where the event mechanism itself is variable (e.g., size and location of a pipe break), the variable characteristic is considered over its full range to assure that all success paths are identified.

This parameter variation analysis for each safety sequence enables the analyst to identify the limiting set of parameters for each success path and each safety system. This type of systematic analysis is used to demonstrate the plant's ability to safely respond to any postulated event. The historical concept of the "worst case" is an unusable concept for a systems analysis of a nuclear power plant. Considering the number of systems and components which must function during an accident, no single set of initial conditions can possibly describe the most limiting set for all systems. Rather than any one "worst case" condition, there exists a spectrum of "worst cases" which must be analyzed on a systems basis to properly design a nuclear power station.

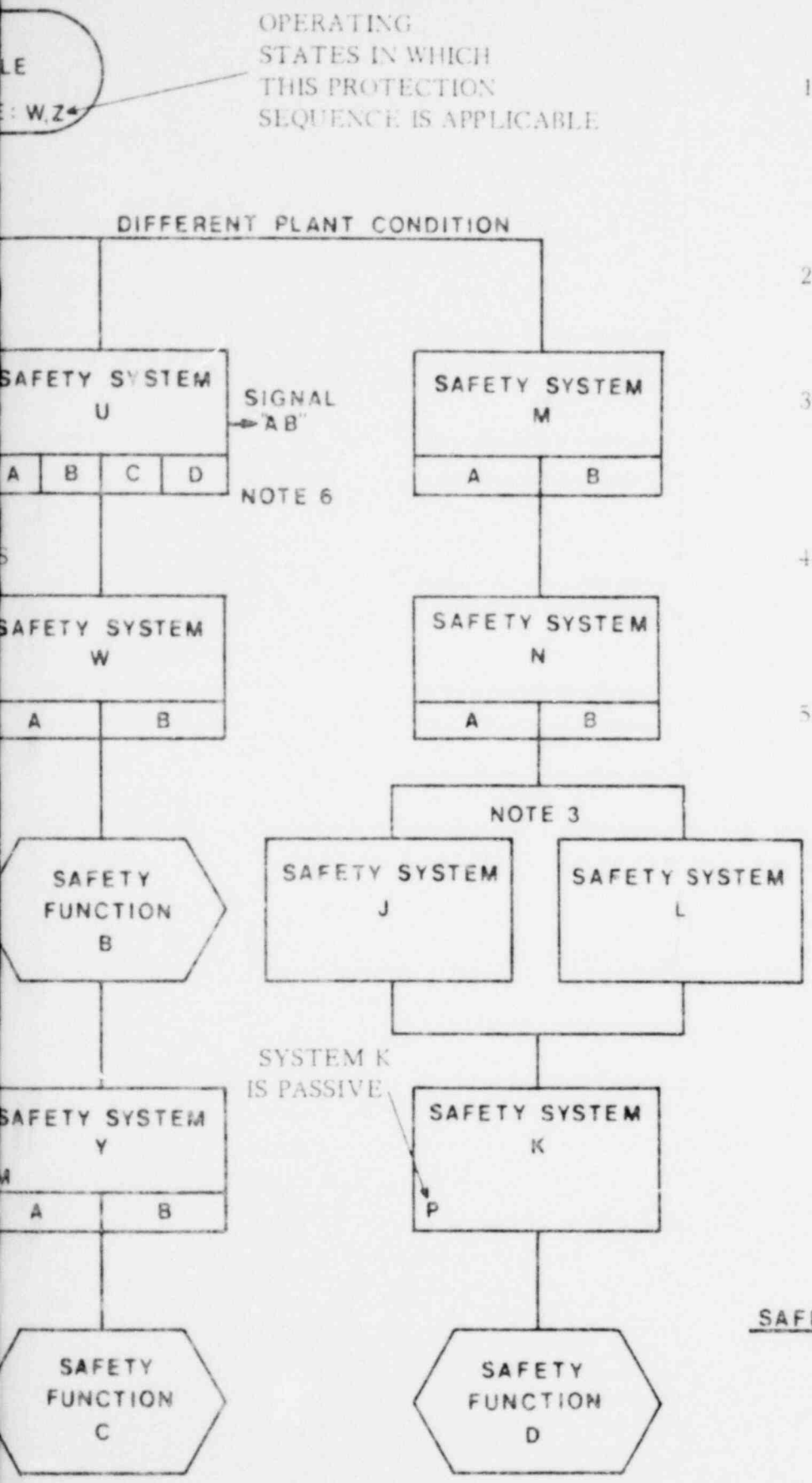
6 319

Safety Sequence Diagram

When all the plant process parameter variations have been considered, the Safety Sequence Diagram (SSD) for the particular event is completed. The SSD displays those prime, or major, plant safety systems whose responses are essential to providing the safety actions required for the postulated event. The SSD shows these safety systems in their functional (not necessarily chronological) sequences following the postulated event. In addition, the SSD shows which plant process variables are monitored or sensed by these safety systems as initiating signals. Figure 2 is an example of the Safety Diagram for the accident "Steamline Break Inside Containment", as developed for the Pilgrim 2 unit.


EVENT CLASSIFICATION
ACCIDENT
RANGE OF INITIAL CONDITIONS
212 < T < 546° F
600 < P < 2500 psia
1% < POWER < 75%
EVENT TIT
STATE
DIFFERENT PLANT CONDITION
NOTE 5
(SETPOINT)
NOTE 4
Sh IS SENSED VARIABLE INITATING SYSTEM Q
SAFETY SYSTEM Q
A
B
SAFETY SYSTEM R
A
B
(SETPOINT)
Th
SAFETY SYSTEM U GENERATES SIGNAL "AB" WHICH INITIATE SYSTEM W
AB
EITHER SENSED VARIABLE Th OR Tc WILL INITIATE SYSTEMS
Th
Tc
SAFETY SYSTEM S
A
B
SAFETY ACTION
BOTH SENSED VARIABLE Ph AND LL MUST EXCEED THEIR LIMITS TO INITIATE SYSTEM T
Ph
LL
SAFETY SYSTEM T
A
B
SAFETY ACTION
MANUAL ACTION REQUIRED FOR SYSTEM Y
Ph
SAFETY FUNCTION A
PLANT IS RETURNED TO STABLE CONDITION WHEN ALL SAFETY FUNCTIONS ARE ACHIEVED.

7 6 52P



GENERAL NOTES

1. Although not shown for all systems on this format diagram, unless safety system is passive a sensed variable is required for either manual or automatic system action.

2. The safety action for each system is to be shown aside the arrow pointed away from the system (——→).

3. System "J" and "L" together satisfy independent functional redundancy. Parallel solid paths indicate this condition.

4. System "R" action is not essential to achieve safety function A. Due to plant conditions system R may operate. Dashed path indicates this condition.

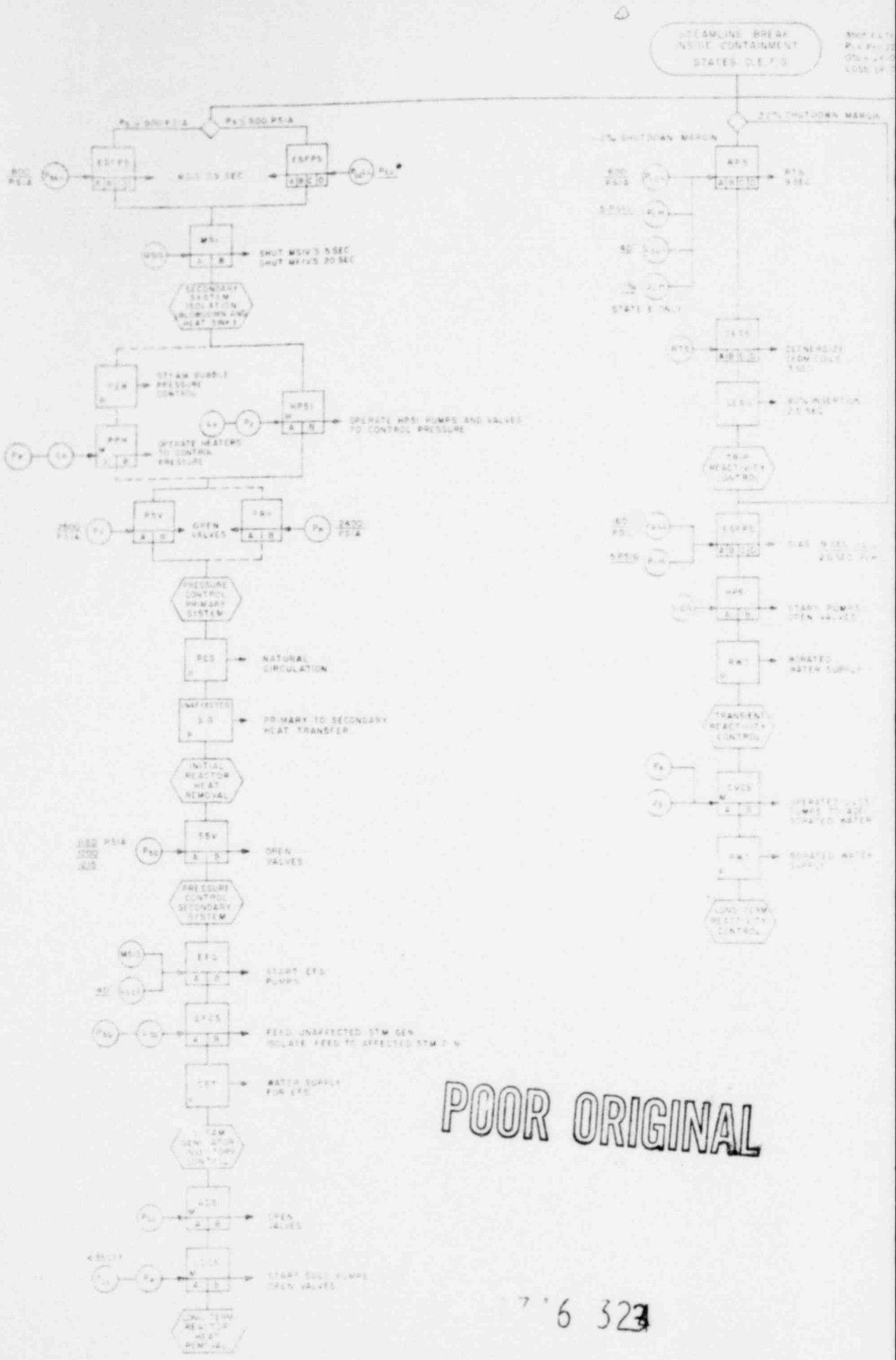
5. (Setpoint) indicates the value of the sensed variable at which the syste is initiated.

6. [A][B] or [A][B][C][D] indicates number of independent, functionally redundant system channels or components.

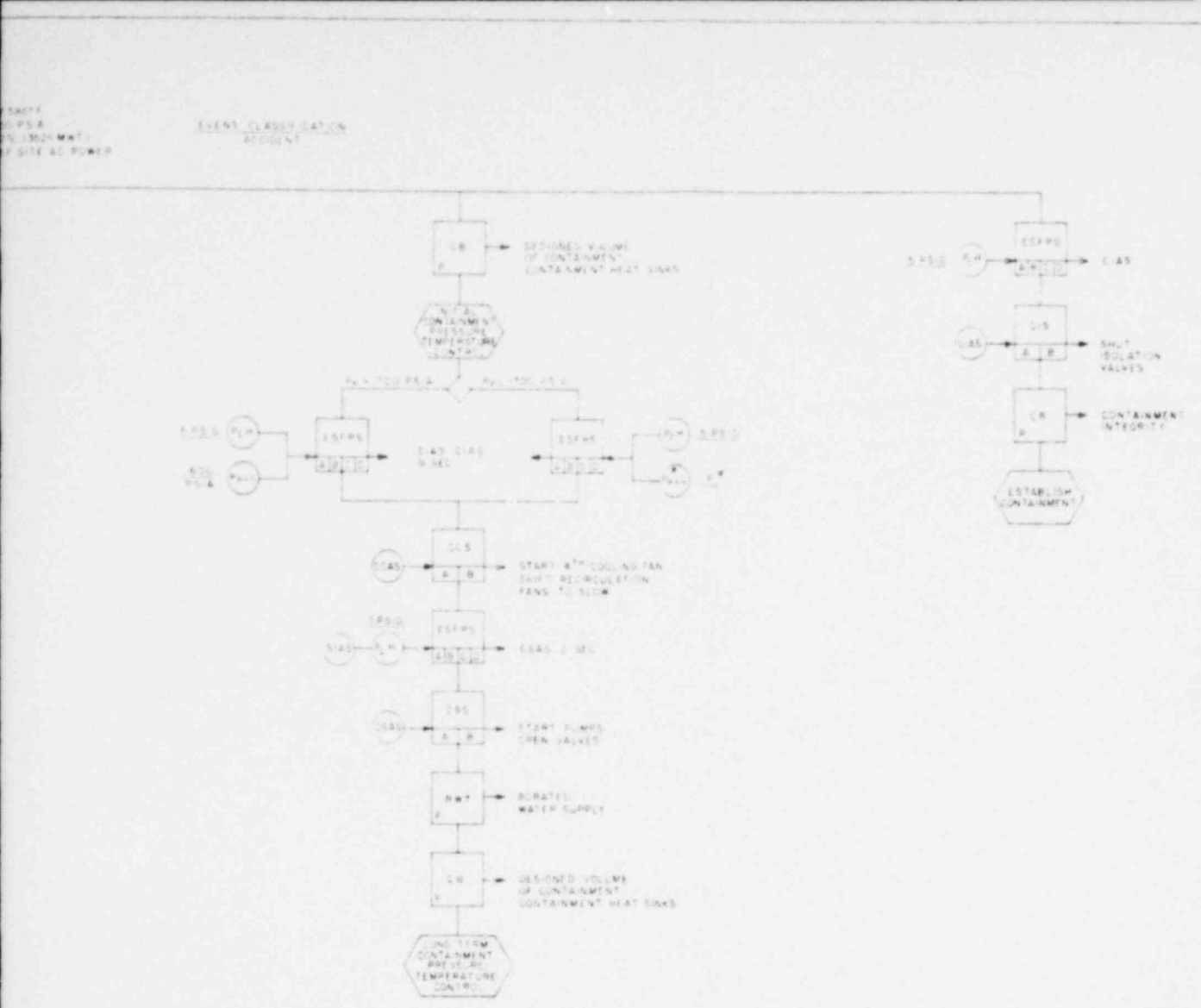
SAFETY SEQUENCE DIAGRAM FORMAT

FIGURE 1

776 522



POOR ORIGINAL



POOR ORIGINAL

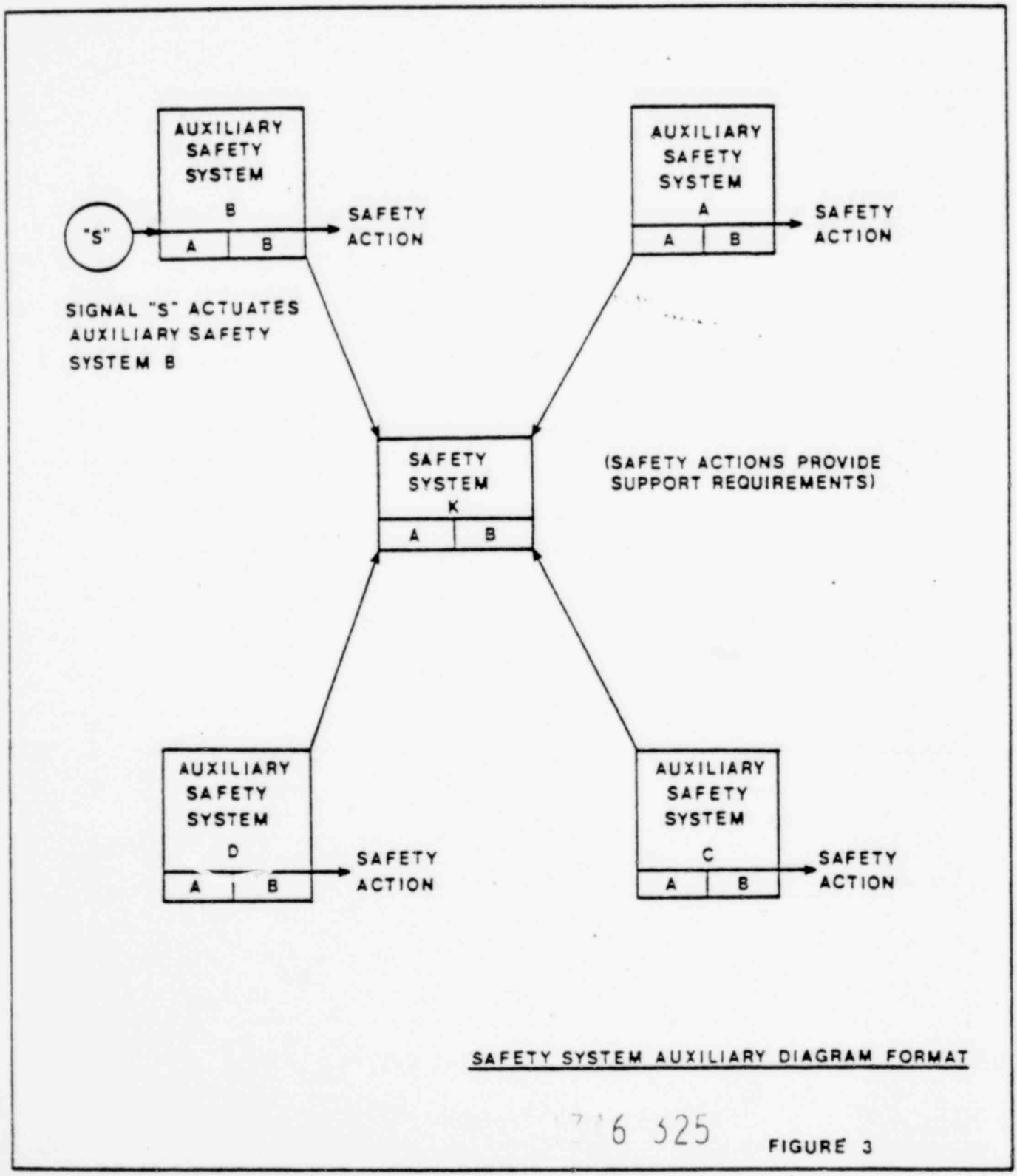
NOTE:
REFER TO TABLE XI FOR DEFINITION OF ABBREVIATIONS

STEAM LINE BREAK INSIDE CONTAINMENT
SAFETY SEQUENCE DIAGRAM

Figure 2

Safety System Auxiliary Diagram

After completion of the SSD for a postulated event, each safety system displayed on the SSD is analyzed to determine the specific support requirements necessary to produce its safety action. Examples of these support requirements are electric power, component cooling, or instrument air supply. The analyst refers to the SSD to determine every sequence in which a safety system is required, thereby ensuring all support requirements are identified. After identification of the support requirements, the plant systems that provide these support requirements are identified. These systems are the Auxiliary Safety Systems. A Safety System Auxiliary Diagram is then prepared on which the prime safety system and its auxiliary safety systems are displayed. Figure 3 is the format for a Safety System Auxiliary Diagram as used in the Boston Edison Pilgrim 2 analysis.



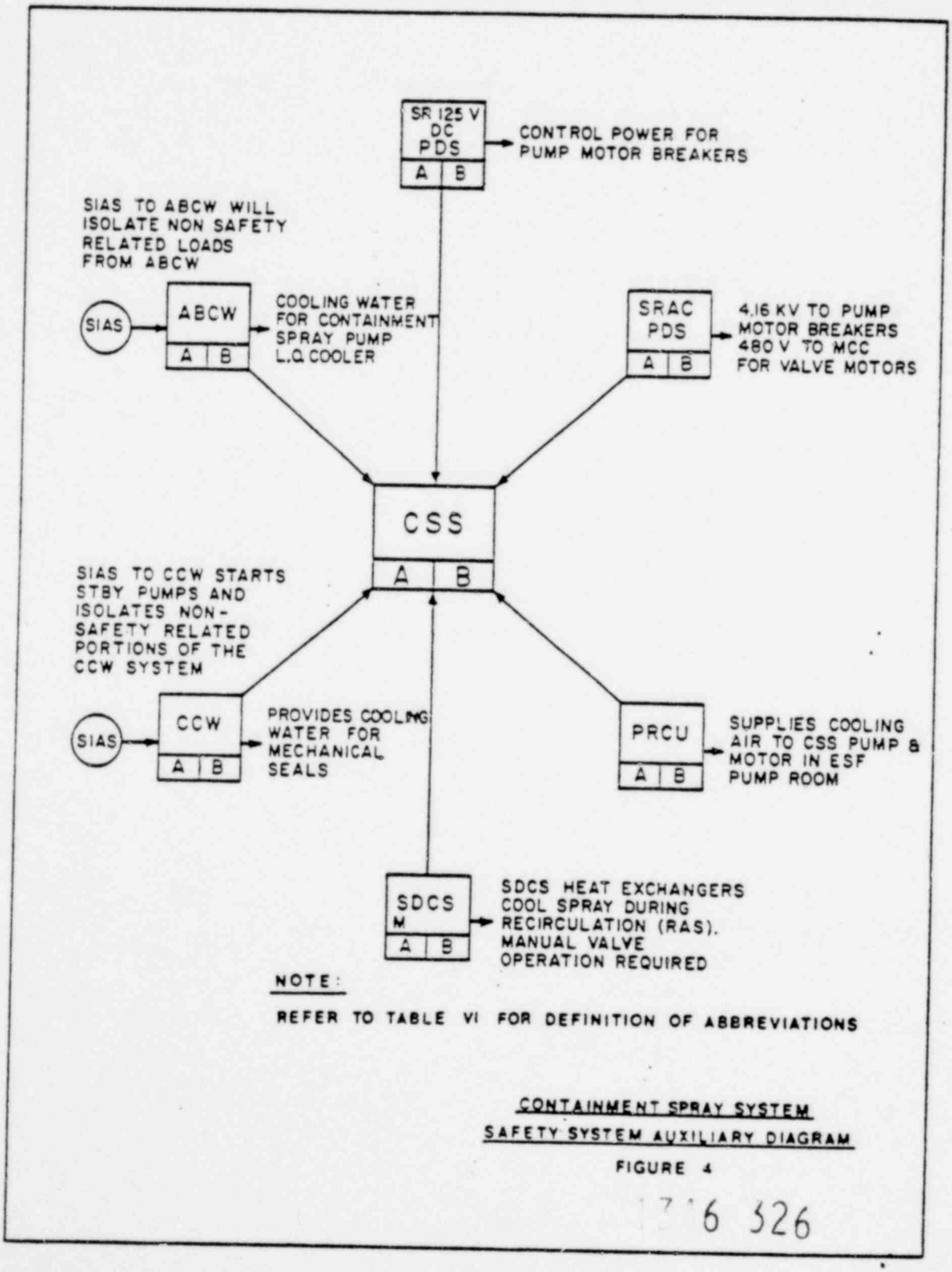
SAFETY SYSTEM AUXILIARY DIAGRAM FORMAT

6 525

FIGURE 3

In developing the Safety System Auxiliary Diagram the analyst ensures that each support requirement is functionally redundant by developing design information about the plant sufficient to positively identify the auxiliaries essential to the required response of the safety system, and by identifying plant design changes so that the auxiliary systems can support their safety system with the needed level of redundancy.

To complete any Safety System Auxiliary Diagram the analyst must review the Safety Sequence Diagrams for all the postulated events to identify all safety sequences in which the subject safety system appears. Figure 4 is the Safety System Auxiliary Diagram for the Containment Spray System of the Boston Edison Pilgrim 2 nuclear unit.



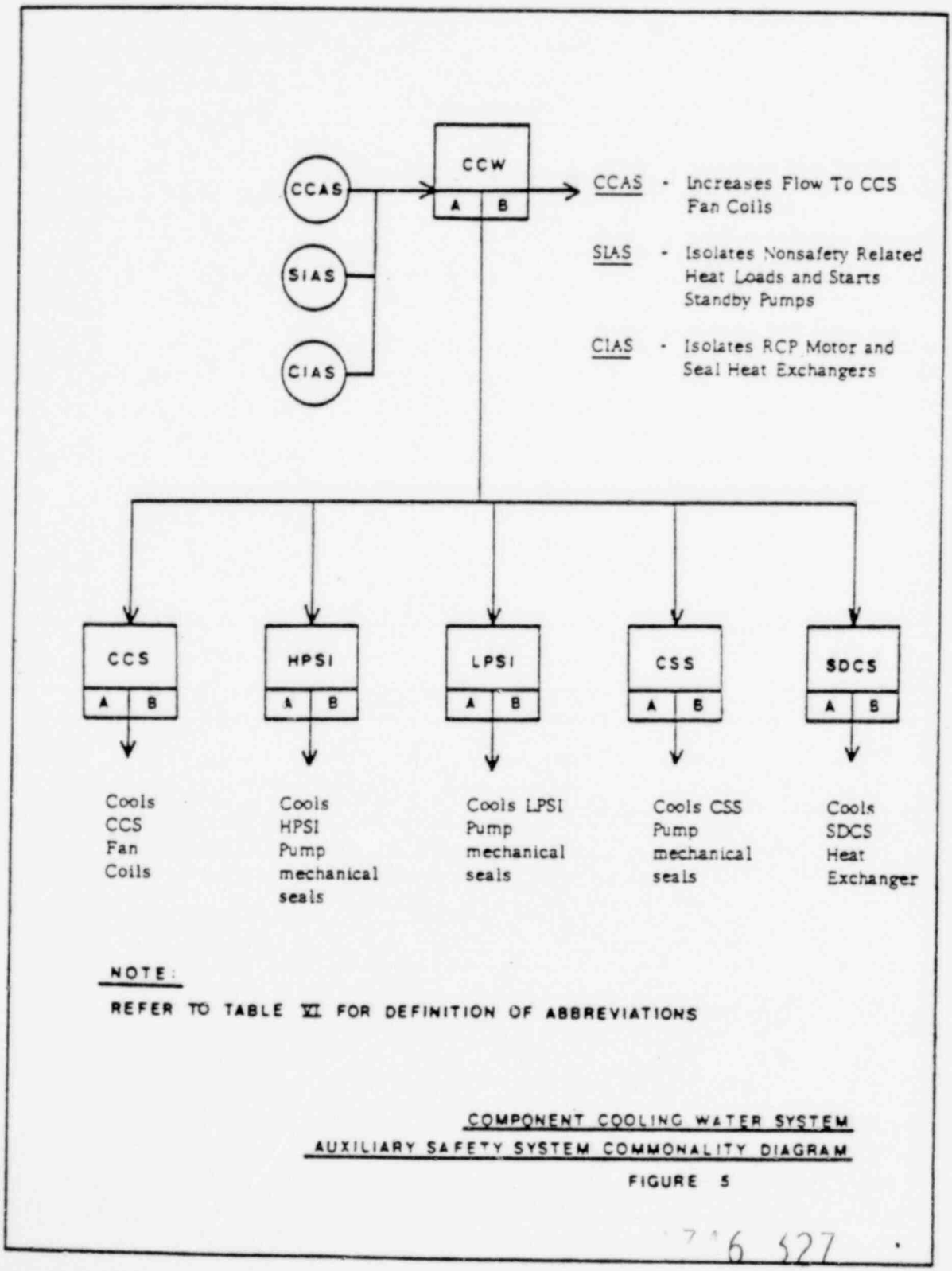
CONTAINMENT SPRAY SYSTEM
SAFETY SYSTEM AUXILIARY DIAGRAM

FIGURE 4

6 326

Auxiliary Safety System Commonality Diagram

After completion of the Safety Sequence Diagrams for each postulated event and the Safety System Auxiliary Diagrams, the Auxiliary Safety System Commonality Diagram (ASSCD) for each Auxiliary Safety System is developed. This diagram indicates all the safety systems that a given Auxiliary Safety System supports. ASSCD is developed mainly as an information diagram, rather than a primary design review diagram. ASSCD allows evaluation of the overall plant response to the operations of each Auxiliary Safety System, considering such effects as that of a single active failure to the component cooling water system. Figure 5 is the ASSCD for the Component Cooling Water System of the Pilgrim 2 station.



COMPONENT COOLING WATER SYSTEM
AUXILIARY SAFETY SYSTEM COMMONALITY DIAGRAM
FIGURE 5

7 6 527

TABLE VI

ABBREVIATIONS USED ON SFPSA DIAGRAMS

ABCW	Auxiliary Building Cooling Water
ADS	Atmospheric Steam Dump System
CB	Containment Structure
CCAS	Containment Cooling Actuation Signal
CSS	Containment Cooling System
CCW	Component Cooling Water
CEA	Control Element Assemblies
CETS	Control Element Trip System
CIAS	Containment Isolation Actuation Signal
CIS	Containment Isolation System
CSAS	Containment Spray Actuation Signal
CSS	Containment Spray System
CST	Condensate Storage Tank
CVCS	Chemical and Volume Control System
EFCS	Emergency Feed Control System
EFS	Emergency Feed System
ESFPS	Engineered Safety Features Protection System
HPSI	High Pressure Safety Injection
LPSI	Low Pressure Safety Injection
MFIV	Main Feed Isolation Valves
MSI	Main Steam Isolation System
MSIS	Main Steam Isolation Signal
MSIV	Main System Isolation Valves
PPH	Pressurizer Proportional Heaters
PRCU	Pump Room Cooling Unit
PRV	Power Relief Valves
PSV	Primary Safety Valves
PZR	Pressurizer
RCS	Reactor Coolant System
RPS	Reactor Protection System
RTS	Reactor Trip System
RWT	Refueling Water Tank
SDCS	Shutdown Cooling System
SG	Steam Generator
SIAS	Safety Injection Actuation Signal
SRPDS	Safety Related Power Distribution System
SSV	Secondary Safety Valves

$J_L H$	High Logrithmic Power
J_S	Startup Neutron Flux Level
L_P	Pressurizer Level
L_{SG}	Steam Generator Level
$L_{SG}L$	Low Steam Generator Level
$P_C H$	High Containment Pressure
P_P	Pressurizer Pressure
$P_P L$	Low Pressurizer Pressure
$P_P LL$	Low-Low Pressurizer Pressure
P_S	Steam Pressure
$P_{SG}L$	Low Steam Generator Pressure
$P_{SG}LL$	Low-Low Steam Generator Pressure
T_{CL}	Cold Leg Temperature

The Role of SFPSA in the Design Process

Under the requirements of 10CFR50, systems, structures and components important to nuclear plant safety must be identified and designed to ensure that they will perform reliably in service. This requirement is satisfied by subjecting all such safety related items to a quality assurance program conforming to the requirements of 10CFR50, Appendix B. The systematic process employed by the SFPSA, as shown on the resulting SSD's and SSAD's, makes it possible to easily identify and classify the various systems, structures, and components of the plant in relation to safety. In particular, the SSD's and SSAD's become a key tool or mechanism to satisfy the design verification requirements of a nuclear quality assurance program under Criterion III (Design Control) of 10CFR50, Appendix B. The following paragraphs describe how the SFPSA results are used in the design process.

The Quality Assured Items List

Each system, component, and structure required to mitigate the consequences of a nuclear plant accident must be subjected to the Nuclear Quality Assurance Program and must be listed on the Quality Assured Items List. Upon completion of the required Safety Sequence Diagrams (SSD's) and Safety System Auxiliary Diagrams (SSAD's), the process of identifying these quality assured items and placing them on the Quality Assured Items List is simple and systematic. Each accident SSD and the associated SSAD's is reviewed. Because the prime safety systems and their supporting auxiliary systems required to achieve the safety functions are diagramed on the SSD's and SSAD's, the task of quality assured system identification is complete. To identify the specific components and structures within the plant systems and larger structures that must be quality assured, each safety system and auxiliary safety system is examined to determine the specific components of these systems that must function to produce the required system responses. The structures in which the systems and components are located, including passive structures shown on the SSD (e.g., the containment, or the refueling water tank), are identified as structures to be quality assured.

The significant amount of analytical effort expended to perform the SFPSA has made the development of the sometimes controversial Quality Assured Items List easy and systematic.

Seismic Design Review

The SFPSA facilitates the identification of the systems, components and structures that must be classified Seismic Category I under the requirements of AEC Regulatory Guide 1.29. In a manner similar to the identification of quality assured items, the accident SSD's are reviewed, and sufficient systems, components and structures are classified Seismic Category I to provide at least one success path for each required safety function. The SSAD for each safety system in the success path is reviewed to identify those auxiliary systems required to support the Category I safety systems. Such auxiliary safety systems are also classified Seismic Category I.

To identify the specific components and structures to be Seismic Category I, each prime safety system and auxiliary safety system is studied in detail, as done in the Quality Assured Items List study. The specific components and structures which must function to produce the safety actions of these systems are classified as Seismic Category I.

Redundancy and Separation

During the development of the SSD's and SSAD's, success paths are determined for each safety function. Each success path represents a sequence that is capable of achieving its safety function given any single active component failure. This capability is shown with either physical redundancy (e.g., two independent trains of the Safety Injection System) or functional redundancy (e.g., either the High Pressure Safety Injection System or the Chemical & Volume Control System supplying borated water). Thus, with the SSD's and SSAD's finished, the complete systems level redundancy of the plant is shown diagramatically.

During the review of the safety system design of the plant, the information on the SSD's and SSAD's is used to ensure that the designs do reflect the required redundancy shown on the diagrams. The design reviewer refers to the SSD's and SSAD's as he tests the designs for susceptibility to single failures. During review of physical arrangement drawings, the SSD's and SSAD's are used to check the adequacy of physical separation, thus ensuring that the plant is properly designed against the effects of pipe whip, jet impingement, flooding, fire, etc.

Effects of Pipe Breaks

Because an SSD has been developed for every pipe break that must be postulated in plant design considering the various plant systems and the various sizes of breaks, the specific systems and structures that must respond to each specific pipe break can be easily identified. During the analysis of a particular pipe break the information on the SSD's and SSAD's is used to identify the specific systems, components and structures that must be protected for that particular break. Pipe whip restraints and jet deflectors are located to protect those specific systems, components and structures, whereas damage to other plant equipment is acceptable. For example, if a particular two inch pipe break in the reactor coolant system does not require the use of the Chemical & Volume Control System (CVCS), there is no reason to protect the CVCS piping following that two inch reactor coolant system pipe break, and no pipe whip restraints or jet deflectors would be specified for this purpose. However, if the High Pressure Safety Injection System is required for this rupture, it will be protected from damage due to pipe whip and jet impingment. Thus, all the items which must be protected are systematically identified and protected, but the number of pipe restraints and deflectors is minimized.

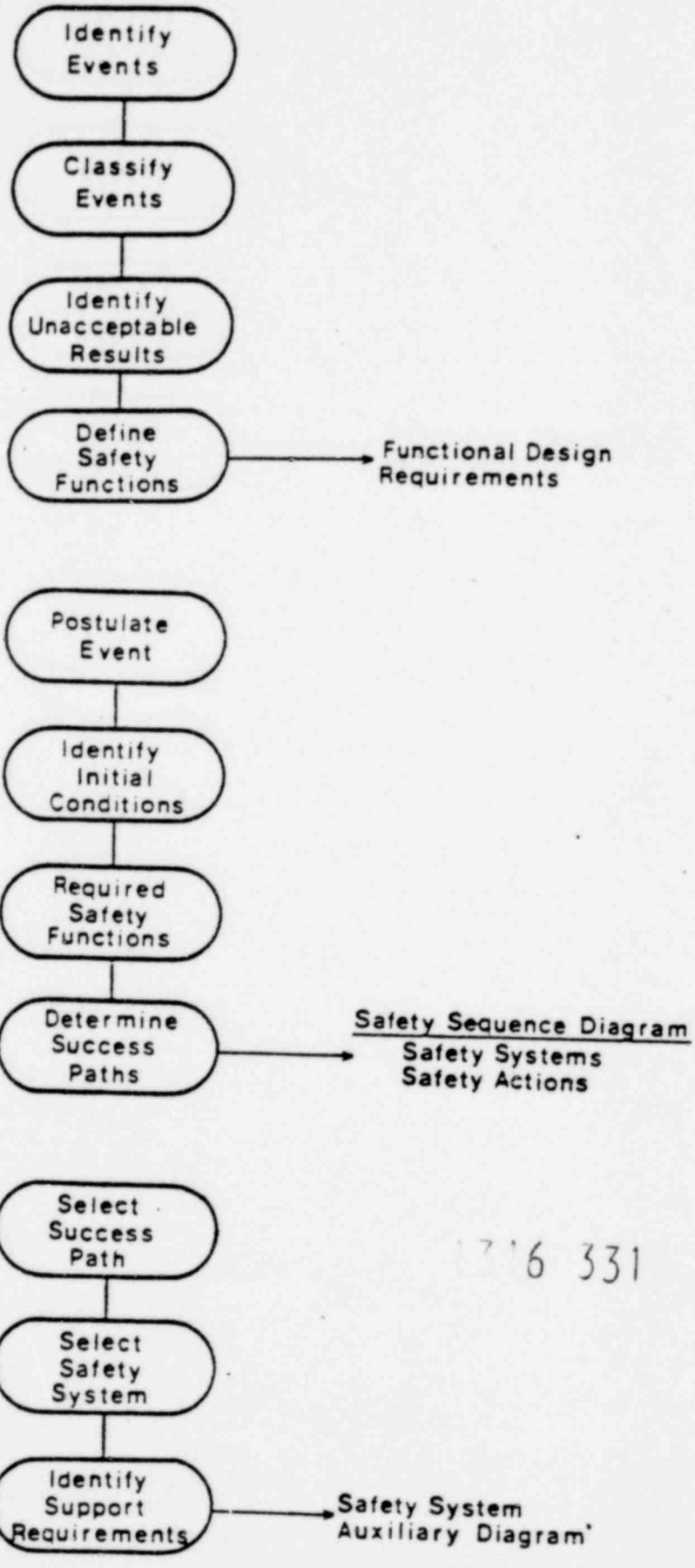
Summary

The systematic approach of the SFPSA provides assurance that each system, component or structure required for safety is identified and designed in accordance with all applicable requirements.

When the SFPSA is complete, each required safety function that must be achieved is clearly identified; the time sequence in which the necessary safety actions must occur is delineated; the degree of redundancy provided in plant design is established; and the need for station design to provide intelligence for operator manual control is defined. The SFPSA distinguishes between those plant systems that are required for the public health and safety and those that are required only for equipment protection. The SFPSA is the mechanism whereby each safety system receives a complete and consistent design review. The SFPSA helps to ensure that no one safety system has been "over designed" at the expense of another.

When performed early in the design process of a nuclear project, the SFPSA operates to greatly reduce, or even eliminate, design changes later in the project, when such changes would be much more costly. Because the SFPSA is a continuing analysis throughout the design phase of the project, it becomes the most useful and meaningful comprehensive representation of the plant safety system design, illustrating on easily understood diagrams the practical results of large volumes of engineering drawings, specifications, and design information.

SAFETY FUNCTION AND PROTECTION SEQUENCE ANALYSIS



ATTACHMENT 1

Application of Safety Sequence and System Auxiliary Diagrams to the Development of Abnormal Transients Operating Guidelines

Application of Safety Sequence and System Auxiliary Diagrams to the Development of Abnormal Transients Operating Guidelines.

The objective of the B&W Abnormal Transients Operating Guidelines (ATOG) Program is to provide the operators of 177 fuel assembly plants with operating guidelin s based on a thorough understanding of many possibl event sequences. Event trees will be const ucted and computer simulations completed to provide the technical basis for the guidelines. Guidelines will be prepared specifically for each of seven plants.

Development of the event trees and guidelines will require a large amount of plant specific data. EDS Nuclear will collect and present this information using the Safety Sequence Diagram (SSD) and System Auxiliary Diagram (SAD) formats. The purpose of the SSDs will be to provide information about systems designed to perform safety functions mitigating transient consequences. The SADs will provide information about systems necessary for operation of other prime systems, which directly affect plant response. (Conversely, they will provide information about the causes of prime system failure.) The SSDs will provide input data for preparation of the event trees (and, to some extent, the guidelines). The SADs will provide direct input data for preparing the guidelines. The SSDs and SADs will also achieve certain secondary objectives: provide training devices; cross check event trees; and identify possible design deficiencies.

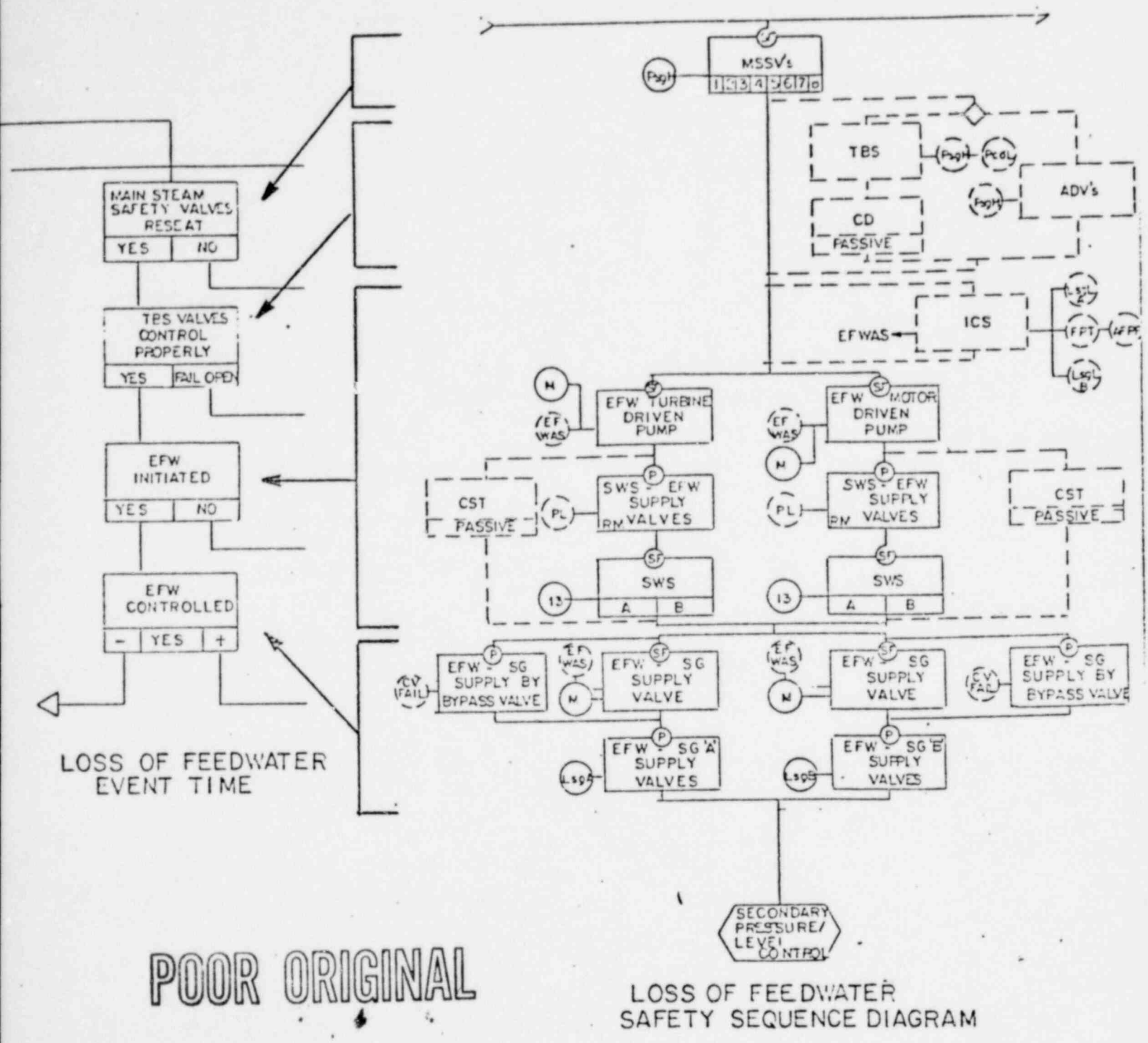
The SSD and SAD formats were chosen for several reasons. They contain sufficient data for preparation of event trees or for establishing corrective actions. They provide information in a logical and easily understood form.

EDS Nuclear has a number of people trained in this method of representing system response; use of this method will facilitate the use of EDS staff personnel in order to complete the ATOG Program in a timely manner.

Safety sequence diagrams are prepared by first carefully identifying the plant safety functions (reactor heat removal, primary pressure and level control, etc.) essential to achieving acceptable consequences during transients. Then the sequence of prime system responses forming redundant success paths are diagramed. The information listed in Table 1 is also added to the diagram. Safety Function and Protection Sequence Analysis, "Transactions of the ANS", November 1973, by R. A. Fortney, et. al., (Attachment 2) is a good general discussion of the SSD and SAD. The EDS Administrative and Technical Procedures for the ATOG Program (Attachment 3) are more current and more detailed descriptions of the methods which will be used to prepare SSDs and SADs.

Figure 1 illustrates the relationship of event trees and SSDs. On the left of Figure 1 is a segment of the preliminary version of the Arkansas Nuclear One Unit 1 (ANO-1) Loss of Feedwater (LOFW) event tree. On the right is one success path from a preliminary version of the ANO-1 LOFW SSD (Attachment 4). The detailed information provided on the SSD is essential to the analyst's understanding of the ANO-1 response to a LOFW. That understanding is needed for development of the event sequences represented on the event tree and for simulation of the event sequence. The data and nomenclature presented can also be used to develop the guidelines.

A sample SAD is provided as Attachment 5. Table 2 summarizes the information presented on the SAD. The importance of the SAD in developing corrective actions and training new operators is apparent.



POOR ORIGINAL

Figure 1 Relationship of Safety Sequence Diagrams and Event Trees

TABLE 1

SAFETY SEQUENCE DIAGRAM

INFORMATION SUMMARIZED

- ALL SYSTEMS INVOLVED IN ACHIEVING A SAFETY FUNCTION
- SYSTEM MAJOR COMPONENTS
- COMPONENT ACTUATION LOGIC
- SETPOINTS
- REDUNDANCY
- PARAMETERS MONITORED
- COMPONENT FUNCTIONAL INTER-RELATIONSHIPS
- PLANT SPECIFIC TERMINOLOGY
- INPUT REFERENCES
- OPERATOR ACTIONS

TABLE 2

SYSTEM AUXILIARY DIAGRAM

INFORMATION SUMMARIZED

- SUPPORTING SYSTEMS AND INTERDEPENDENCE
- POWER SUPPLIES
- ACTUATION PARAMETERS AND INSTRUMENTATION
- VALVES ACTUATED (INCLUDING FAILURE POSITION)
- LOGIC AND SETPOINTS
- SAFETY QUALIFICATIONS
- REQUIRED OPERATOR ACTIONS
- VERIFICATION INSTRUMENTATION
- OUTPUT ACTIONS AND SIGNALS
- REFERENCES