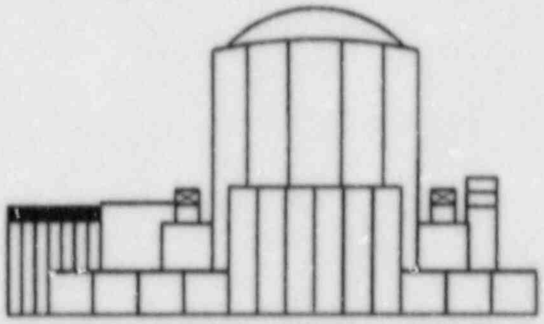
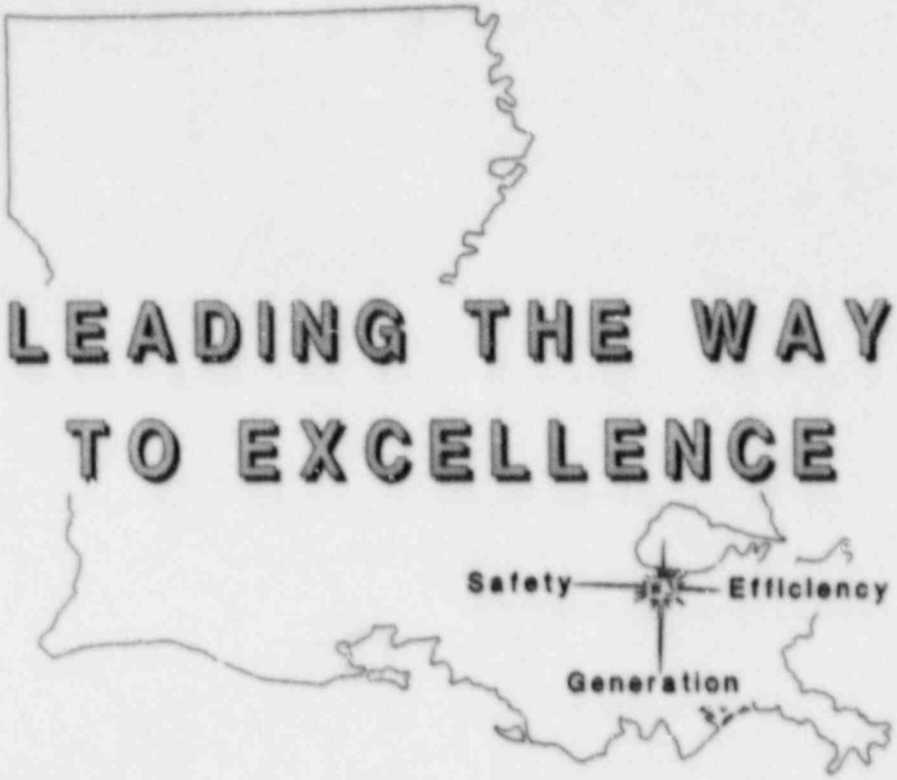
LOUISIANA P&L
MIDDLE SOUTH
UTILITIES SYSTEM



WATERFORD SES - UNIT 3

NUCLEAR OPERATIONS

LEADING THE WAY TO EXCELLENCE



COMPLIANCE WITH 10CFR50.62

REDUCTION OF RISK from ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS) EVENTS

OCTOBER, 1988

WATERFORD STEAM ELECTRIC STATION - UNIT NO. 3

COMPLIANCE WITH 10CFR50.62
REDUCTION OF RISK FROM ANTICIPATED
TRANSIENTS WITHOUT
SCRAM EVENTS

OCTOBER, 1988

ABSTRACT

Title 10 of the Code of Federal Regulations Section 50.62 requires that Waterford 3 have a diverse scram system (DSS), a diverse turbine trip (TT) and diverse equipment to automatically initiate the emergency feedwater actuation system (EFAS) under conditions indicative of an anticipated transient without scram (ATWS) event. These systems are to be diverse from the existing reactor trip system (RTS) to the extent reasonable and practicable.

This submittal describes the design and functioning of these systems for Waterford 3 and establishes that Waterford 3 will have the equipment necessary to mitigate an ATWS event without undue risk to the health and safety of the public. A request for exemption from the EFAS diversity requirements is submitted as an Appendix to this report.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AC	Alternating Current
AOO	Anticipated Operational Occurrence
ASSY	Assembly
ATWS	Anticipated Transient Without Scram
C	Centigrade
CE	Combustion Engineering
CEA	Control Element Assembly
CEDM	Control Element Drive Mechanism
CEDMCS	Control Element Drive Mechanism Control System
CMF	Common Mode Failure
CPC	Core Protection Calculator
DC	Direct Current
DSS	Diverse Scram System
EFAS	Emergency Feedwater Actuation System
EM	Electro-Mechanics
ESFAS	Engineered Safety Features Actuation System
HPP	High Pressurizer Pressure
MSL	Mean Sea Level
PPS	Plant Protection System
PRZ	Pressurizer
QA	Quality Assurance
QSPDS	Qualified Safety Parameters Display System
RCS	Reactor Coolant System
RMS	Root Mean Square
RPS	Reactor Protection System

LIST OF ABBREVIATIONS
(Cont'd)

RTD	Resistance Temperature Detector
RTS	Reactor Trip System
SGLL	Steam Generator Low Level
TT	Turbine Trip
UV	Under Voltage
VAC	Volts Alternating Current
VDC	Volts Direct Current

LIST OF FIGURES

1.0 INTRODUCTION

In order to reduce the probability of core damage and mitigate the release of fission products to the environs which could result from a severe anticipated transient without scram (ATWS) event, the NRC issued 10CFR50.62, commonly known as the ATWS Rule. The following report documents LP&L's plans for compliance with the ATWS rule for Waterford 3.

The ATWS Rule requires installation of a diverse scram system (DSS) and equipment to initiate the emergency feedwater system (EFAS) and a turbine trip (TT) under conditions indicative of an ATWS. These systems are to be diverse from the reactor trip system (RTS) to preclude the possibility of common mode failures (CMFs).

Waterford 3 will install a DSS that is designed to meet the requirements of 10CFR50.62 during the third refueling outage. The combination of existing equipment and the DSS results in a diverse turbine trip. While Waterford 3 feels that the existing EFAS incorporates sufficient diversity to the extent reasonable and practicable under the ATWS Rule, an explicit exemption to the EFAS requirements of 10CFR50.62 is requested.

2.0 DIVERSE SCRAM SYSTEM

The DSS for Waterford 3 is designed to initiate a reactor trip for conditions indicative of an ATWS by monitoring pressurizer pressure.

Pressurizer pressure increases as more energy is deposited in the coolant. The DSS generates a signal when the pressure setpoint is reached, interrupting the power supply that maintains the control rod position. Once the power field is interrupted, the control rods, no longer suspended, drop into the core halting the reaction.

The Waterford 3 DSS employs two parallel paths of circuitry, each consisting of the pressure sensor, a bistable, a bistable relay, and a trip relay (see Figures 1 and 1a). The pressure sensor is a Barton diaphragm - type sensor. The sensor monitors pressurizer pressure generating a signal proportional to the existing pressure. This signal is compared to a setpoint by the bistable. If the setpoint has been exceeded, the bistable switches state, thereby generating a trip signal. This trip signal is sent through the bistable relay to the trip relay. The bistable relay provides for the voltage change between the bistable and the trip relay. When the trip relay receives the signal, the electric field of the motor-generator set is interrupted (see Figure 4). This removes the power supply for the control element drive mechanism control system (CEDMCS) without actuating the reactor trip breakers. Once the CEDM power to the CEDMCS is removed, a scram occurs.

Operating status of the DSS will be provided to the control room operators through an ATWS display which will be incorporated into the qualified safety parameters display system (QSPDS). A full description of the QSPDS is provided in Appendix 1.9A of the Waterford 3 FSAR. The QSPDS is "human-factor" engineered to provide operators with clear, concise data from the inadequate core cooling instrumentation. As part of the QSPDS, the ATWS display will be quality controlled. The QSPDS will provide continuous monitoring through alarms which will inform the operators of a high pressure state. The ATWS display will be available to operators during both normal and abnormal conditions. Consequently, its use as a part of the QSPDS will be integrated into operator training. Additionally the main control room annunciators will provide indication of an ATWS trip or system bypass/trouble state. Locally (at the motor-generator sets), red and green lights will provide ATWS trip indication and amber lights will indicate system bypass.

2.1. GUIDANCE REGARDING SYSTEM AND EQUIPMENT SPECIFICATIONS FOR DSS

Supplementary information (49FR26043, 26044) is provided with the Federal Register notification of the ATWS rule which includes guidance concerning the degree of diversity from the RTS required of the DSS and mitigating systems. The guidance states that equipment diversity to minimize the potential for CMF is required from sensor out[illegible] and including the components used to interrupt control rod power [illegible] the DSS. Therefore all DSS instrument channel components (excluding sensors and signal conditioning equipment upstream of the bistables) and logic channel components, and all DSS actuation devices must be diverse from the RTS. Areas of guidance are as follows.

1. Safety Related (1EEE - 279)
2. Redundancy
3. Diversity from the RTS
4. Electrical Independence from existing RTS
5. Physical Separation from existing RTS
6. Environmental Qualification
7. Seismic Qualification
8. Quality Assurance for Test, Maintenance, and Surveillance
9. Safety Related (1E) Power Supply
10. Testability at Power
11. Inadvertent Actuation

In these areas the NRC establishes the criteria for such things as diversity, testability, etc. for a DSS design that they feel will comply with 10CFR50.62. Though not formally required, these guidelines are integrated into the design for the Waterford 3 DSS as discussed below.

2.1.1. SAFETY RELATED (1EEE - 279)

Staff Position - Not required but the implementation must be such that the existing protection system continues to meet all applicable safety related criteria.

Though not required to satisfy 1EEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, the DSS designed for Waterford 3 will use components demonstrating a high level of quality assurance. While the DSS as a system will not be classified as safety-related, all of the components except for the power supply for Potter Brumfield power relay and the power relay itself will be safety class 1E. This power relay will be powered by a non-1E DC vital bus that is available during a loss of offsite power event.

To avoid jeopardizing the existing level of safety for the RTS, the design for the DSS is such that there is no interaction with the RTS. This is done by locating the equipment in separate cabinets on a different elevation. Additionally, the DSS is electrically isolated from the RTS using qualified components. Physical and electrical isolation of the DSS from the RTS maintains the integrity of the RTS and, consequently, does not invalidate the safety classification of the RTS.

2.1.2. REDUNDANCY

Staff Position - Not required.

Redundancy alone does not preclude CMF occurrences. Consequently, the NRC placed no requirements on redundancy of the DSS. Regardless, the DSS designed for Waterford 3 employs two parallel paths based on a two out of two logic, in order to provide increased reliability and accuracy over that provided by a single channel system.

2.1.3 DIVERSITY FROM EXISTING REACTOR TRIP SYSTEM

Staff Position - Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failure is required from the sensors to and including the components used to interrupt control rod power. Circuit breakers from different manufacturers alone is not sufficient to provide the required diversity for interruption of control rod power. The sensors need not be of a diverse design or manufacturer. Existing protection system instrument-sensing lines may be used. Sensors and instrument-sensing lines should be selected such that adverse interactions with existing control systems are avoided.

Figure 1 represents the circuits for the RTS and the DSS. The first components for these systems are the sensors. The Waterford 3 RTS and DSS share a common process card and power supply (not shown in figure) for the sensors. These are considered part of the sensor and as such do not violate diversity requirements. However, a certain level of diversity does exist between these sensors. The RTS sensor element uses a Rosemount capacitance capsule type sensor where the DSS employs a Barton diaphragm type sensor. This not only provides diversity of manufacturers but also of operational principle. The Rosemount sensor is a capacitor, two plates on either side of a dielectric, where a change in pressure results in a change in the capacitance of the system. The Barton sensor operates on a bellows principle where deflection of the bellows caused by a change in pressure results in a change of tension across a strain gauge. The change in strain gauge resistance indicates the pressure change. The Barton sensors had no previous RTS function, and since diversity exists between the other elements of the DSS and the RTS, interactions at the sensor level are minimized.

The second component in the DSS is the NAL Bistable card. The bistable in the DSS is diverse from the RTS bistables in manufacturer (Westinghouse for the DSS versus Electro-Mechanics for the RTS and Gould for the CPCs), and power supply. The CPCs provide an auxiliary trip in the RTS on high pressurizer pressure using digital processing. The DSS Westinghouse bistable is diverse from both the Electro-Mechanics bistable and CPC Gould digital processor in the RTS system. The power supply for the DSS is a Westinghouse power supply which provides 26 VDC with a 24 VDC source as backup should the 26 VDC fail. The RTS power supply is a Power Mate supply which provides 12 VDC. The CPC power supply is 16 VDC Lambda supply. Thus, the DSS NAL bistable card has nearly ideal diversity from the RTS bistable, and CPC auxiliary trip.

The third component in the DSS is the NAI bistable relay card. Similar diversity exists between the bistable relays as between the bistables; that is, they are diverse in manufacturer (Westinghouse designed the NAI card in the DSS and Electro-Mechanics designed the bistable relay in the RTS), design principle (analog for the DSS NAI card versus digital for the

RTS), and power supply. Like the bistables, the bistable relays are powered such that those in the DSS circuitry receive 26 VDC from a Westinghouse power supply (with a 24 VDC backup source should the 26 VDC fail), and those in the RTS circuitry receive 12 VDC from a Power Mate power supply. Thus, the DSS NAI bistable relay card has nearly ideal diversity from the RTS bistable relay.

The final component of the DSS is a Potter Brumfield power relay. The parallel device for the RTS is not a relay and is powered by a 1E vital bus as opposed to the non-1E vital bus used for the DSS relay, so diversity is well established between these components. However, there are other relays in the RTS circuitry. With the exception of one, all of the RTS relays are diverse from the DSS Potter Brumfield power relay in manufacturer. The exception is a Potter Brumfield rotary relay. This is a different model though, with different specifications. See table below.

DESIGN PARAMETER	RTS	DSS
	MDR-170-1	PRD11DHO
Operational Principal	Rotary	Toggle
Input Voltage	115 VDC	110 VDC
Coil Current (amps)	0.620	0.020
DC Coil Resistance (ohms)	8.4	6050.
Steady State Power (watts)	17.0	2.0

Also, the above two relays operate on different principles. The coil for the DSS Potter Brumfield relay is oriented such that when energized and deenergized, the relay toggles. No other relay in the RTS operates on this exact same toggle mechanism. The coils for the Potter Brumfield rotary relay in the RTS are shaped as two semicircles. When energized and deenergized, these coils spin the relay rather than toggle it. Therefore, diversity on operational principle exists. Power supply diversity exists, as well. The DSS relay receives its power from a 125 VDC vital bus where the RTS relays (including the Potter Brumfield rotary relay) receive power from either a 120 VAC vital bus or a 12 VDC Power Mate power supply. Although there is a common manufacturer for one of the RTS relays and the DSS relay, no other similarities exist in the power supply systems. As such, sufficient diversity is established for the actuation device in the DSS to meet the requirements.

The ATWS Rule requires diversity to exist from (but not including) the sensors to (but not including) the final actuation device. Though not required, additional limited diversity exists between the sensors for the DSS and RTS. As such, the design of the Waterford 3 DSS meets the requirements of the staff position on diversity.

2.1.4. ELECTRICAL INDEPENDENCE FROM EXISTING REACTOR TRIP SYSTEM

Staff Position - Required from sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits.

The power supplies for the non-safety related circuits of the DSS are to be electrically isolated from the safety related circuits of the RTS by a series of circuit breakers and fuses (see Figure 3), which are qualified as 1E. This prevents the possibility of a failure of one power supply to affect the operation of the other power supplies.

The RTS and the DSS are designed such that a CMF producing an overvoltage or undervoltage condition will not compromise both the RTS and ATWS prevention/mitigation functions. During an undervoltage occurrence, an alarm is generated if the voltage on the AC vital bus drops to between 115 and 116 volts. Since the Westinghouse power supplies are operable down to 112 volts, the operation of the NAL card and NAI card are assured during undervoltage conditions of which the operator has no knowledge. Likewise, the Potter Brumfield relay will remain operable down to 75% of its input voltage, long after an undervoltage alarm would have occurred. Therefore, the ATWS circuitry will provide continuous protection during undervoltage occurrences prior to voltage lowering to the alarm setpoint.

During an overvoltage occurrence, a regulator on the output of the RTS power supplies maintains a steady supply to the components. Should the overvoltage state continue to worsen, the operator is notified by an alarm when the input voltage to the power supplies reaches a setpoint between 129 and 130 volts. Likewise, if the output voltage of the Power Mate supplies increases to 14 volts (the RTS components are still operable at this voltage), the power supply overvoltage protection device automatically drops the output voltage to zero. When any of the two auctioneered power supplies in a channel drop to zero, a reactor trip will be generated.

2.1.5. PHYSICAL SEPARATION FROM EXISTING REACTOR TRIP SYSTEM

Staff Position - Not required, unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated.

Although not required, physical separation from the existing RTS is provided for the DSS. Separate cabinets will house the electronics associated with the DSS. This equipment will be located on the +21 MSL elevation. Similar equipment for the RTS is located on the +46 MSL.

2.1.6. ENVIRONMENTAL QUALIFICATION

Staff Position - For anticipated operational occurrences only, not for accidents.

In Title 10 of the Code of Federal Regulations, Section 50.49(c), a mild environment is defined as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences". All materials that operate as part of the DSS will, as a minimum, meet the qualifications for a mild environment.

2.1.7. SEISMIC QUALIFICATION

Staff Position - Not required.

Though the NRC's equipment qualification guidance states that the DSS does not require seismic qualification, it must not jeopardize the qualification of the existing RTS. The components of the DSS from the sensor output to the final actuation device will be removed from the RTS in separate cabinets. Therefore, the DSS will not violate the seismic qualification of the existing RTS.

2.1.8. QUALITY ASSURANCE FOR TEST, MAINTENANCE, AND SURVEILLANCE

Staff Position - The Commission has released a Generic Letter (85-06, April 16, 1986) in which is provided the explicit Quality Assurance (QA) guidance required by 10CFR50.62. While Appendix B is viewed as a useful reference in which to frame the staff's guidance for non-safety related ATWS equipment, it does not meet the intent of the ATWS QA program. The equipment encompassed by 10CFR50.62 is not required to be safety related, therefore, less stringent QA guidance is acceptable. This letter incorporates a lesser degree of stringency by eliminating requirements for involving parties outside the normal line organization and requirements for a formalized program and detailed record keeping for all quality practices.

LP&L has included in its Nuclear Operations Management Manual, a chapter that defines the quality program for non-safety related ATWS equipment. This non-Appendix B program addresses 10CFR50.62 and incorporates the guidance provided by Generic Letter GL-85-06.

Testing will be performed prior to installation and operation to demonstrate that the ATWS equipment conforms to design specifications. Additionally, ATWS equipment will be periodically tested to ensure that the test requirements have been satisfied. Measuring and test equipment used to determine the acceptability of work or process status will be controlled and calibrated or adjusted at specific intervals in accordance with reviewed and approved procedures.

LP&L has considered the applicability of Technical Specifications to the DSS. It is our understanding that current NRC policy dictates that requirements should not be added to either the Standard Technical Specifications or individual plant Technical specifications unless they are consistent with the Commission Interim Policy Statement on Technical Specification Improvement - basically, requirements necessary to prevent or mitigate design basis accidents or transients. Because the DSS will be a non-safety related system for which no credit is taken in plant analyses, the necessary criteria are not met for including the DSS in the Waterford 3 Technical Specifications.

2.1.9. SAFETY-RELATED (1E) POWER SUPPLY

Staff Position - Not required, but must be capable of performing safety functions with loss of offsite power. Logic power must be from an instrument power supply independent from the power supplies for the existing reactor trip system. Existing RTS sensor and instrument channel power supplies may be used provided the possibility of common mode failure is prevented.

The RTS is composed of four channels A, B, C and D. Each channel possesses circuitry identical to the RTS circuitry represented in Figure 1. Channels A and C are powered from the "A" battery, and Channels B and D are powered from the "B" battery. The DSS will be composed of only two channels, A and B, each identical to the circuitry shown in Figure 1. The 26 VDC power supplies (shown in Figure 1) will receive power from the "A" battery for Channel A, and from the "B" battery for Channel B. These 26 VDC power supplies will all be 1E safety-related supplies. The 125 VDC vital bus in each channel will receive power from the "AB" battery. This will be a non-1E vital bus. However, all power supplies for the DSS, including the 125 VDC vital buses, will be independent from existing RTS power supplies (as stated above), and will be functional during a loss of offsite power.

2.1.10. TESTABILITY AT POWER

Staff Position - Required.

LP&L has made provisions to permit periodic testing of process equipment, bistable, and logic for the DSS when the reactor is operating at power. The level of testing is comparable to present reactor protection system requirements; that is, a combination of simultaneous and overlapping tests of components and subsystems will be performed to insure full system functional capability. Because the RTS would be redundant and independent of the DSS, the RTS would provide the trip functions during the periodic testing of the DSS.

To test the DSS circuitry at power, the Potter Brumfield power relay (Figure 1) is bypassed by an identical Potter Brumfield power relay placed in parallel. This bypass state is indicated in the control room by an audible alarm and a bypass indication light on the local panel display. Once the power relay is bypassed, a test signal consistent with an ATWS occurrence is sent to the NAL card. A successful test will trip the power relay switching a red light to a green light on the local panel designating actuation of the DSS circuitry and a main control room annunciator.

2.1.11. INADVERTENT ACTUATION

Staff Position - The design should be such that the frequency of inadvertent reactor trip and challenges to other safety systems is minimized.

LP&L will employ a DSS that includes the use of two channels operating on a two out of two logic, reliable power supplies and testing to support a satisfactory level of reliability. These design features are sufficient to minimize the frequency of inadvertent actuation and challenges to other safety systems.

2.2. DSS CONCLUSION

As required, the Waterford 3 DSS design establishes diversity from the sensors to and including the components used to interrupt control rod power to the extent reasonable and practicable to minimize the potential for common cause failure. Compared to the RTS, the Waterford 3 DSS incorporates components from different manufacturers with different operating specifications. This design meets or exceeds the NRC suggested guidelines for ATWS Rule implementation.

3.0 DIVERSE TURBINE TRIP (TT) SYSTEM

Under normal operation, the turbine trip is initiated in response to the RTS trip signal. During an ATWS event, the failure of a RTS scram will result in the omission of a turbine trip signal. The diverse TT for Waterford 3 assures initiation of a turbine trip during an ATWS event.

The existing TT system initiates on a signal from the existing RTS. By implementing a DSS, an inherent diverse TT system is provided. (See Figures 1 and 4.) When the DSS causes a reactor scram, power is interrupted to the control element drive mechanism coils upstream of the rod power bus undervoltage relays in the CEDMCS. The deenergizing of these undervoltage relays actuates the turbine trip circuitry. Therefore in defining a DSS (as was done in the previous section), the existing TT is also diverse due to the diversity between the DSS and the existing RTS.

Basically the system works via three-phase power separately input to each of two CEDMCS undervoltage circuits, housed in separate cabinets. Each circuit has the three phase power input monitored for an undervoltage condition by two redundant undervoltage relays, which are part of an Undervoltage and Auxiliary Relay Assembly. Each assembly, two per CEDM power bus, contains an undervoltage relay and two interconnected auxiliary relays. Instrument bus power is used to energize the auxiliary relays.

Each undervoltage relay provides local indication of an undervoltage condition. Remote annunciation is provided by auxiliary relays, each of which is controlled by its interconnected undervoltage relay. A second auxiliary relay is provided for testing each undervoltage/auxiliary relay combination.

If the line-to neutral voltage of any phase drops to 111 ± 15 Vac input to the undervoltage relays, the relays de-energize. De-energizing the undervoltage relays also de-energizes their interconnected auxiliary relays, which causes the associated turbine trip solenoid to energize resulting in a turbine trip.

This dependence of the diverse TT upon the DSS means the operating status of the DSS will reflect the operating status of the diverse TT. The control room annunciators and the QSPDS ATWS displays will similarly relay the status of the diverse TT status.

3.1. GUIDANCE REGARDING SYSTEM AND EQUIPMENT SPECIFICATIONS FOR DIVERSE TT

The diverse TT system is an extension of the DSS. There are no new components associated with the diverse TT system that did not exist previously as part of the DSS. In this regard, the same level of acceptability to each of the 11 areas of guidance for the DSS in Section 2.1 directly applies to the diverse TT.

3.2. DIVERSE TT CONCLUSION

As required by the ATWS Rule, the Waterford 3 diverse TT establishes diversity from the sensors to, but not including, the final actuation device to the extent reasonable and practicable to minimize the potential for common cause failure. The diversity of the DSS was detailed in Section 2. Since the circuitry for the diverse TT is essentially the DSS, component diversity for the TT is inferred. Additional diversity is provided by the different methods through which the DSS and RTS trip the turbine. Like the DSS design, the Waterford 3 diverse TT design meets or exceeds the guidelines suggested by the NRC. Therefore adequate diversity between the diverse TT and the RTS exists in compliance with the ATWS Rule.

4.0 DIVERSE EMERGENCY FEEDWATER ACTUATION SYSTEM (EFAS)

The function of the diverse EFAS is to ensure emergency feedwater activation such that a sufficient supply of cooling water to the steam generators exists to limit the peak reactor coolant system pressure experienced during an ATWS.

Section 10.4.9B.1 of the Waterford 3 FSAR summarizes a reliability study that was done on the Waterford 3 EFAS. The intent of this study was to assess the system availability to function on demand. The results demonstrated that the existing EFAS is highly reliable.

The Waterford 3 EFAS has two parallel paths of circuitry each consisting of a steam generator level sensor, a bistable operational amplifier, a bistable relay, a matrix relay, an initiation relay and the final actuation device (see Figure 2). If pressure and level is low for a steam generator, a break is indicated and emergency feedwater will not be delivered to that steam generator. If the pressure is above the value indicating a break, and a low steam generator level signal is generated, the actuation device opens the emergency feedwater isolation valves enabling the delivery of emergency feedwater to both steam generators.

In November of 198[illegible], the CE Owners Group prepared CEN-349, Response to the NRC's Evaluation of CEN-315 for SONGS 2 & 3, ANO-2 and Waterford 3. CEN-349 provided detailed information about the diversity between the EFAS and RTS for ANO-2, SONGS 2 & 3, and Waterford 3. In evaluating EFAS diversity, CEN-349 considered the three RTS functions (i.e., high pressurizer pressure trip, core protection calculators, and steam generator low level trip) which would have to fail in order for an overpressure ATWS to occur. It demonstrated that all of the EFAS components except for the bistable and matrix relays were diverse from their counterparts in the RTS.

CEN-349 stated, however, that the design of the PPS provides a degree of protection against common mode failures of bistable relays disabling both the EFAS and RTS that is comparable to the protection which would be provided by diverse components. At a minimum, the right combination of 24 out of 48 bistable relays or 24 out of 72 matrix relays in the EFAS and the RTS functions of interest (high pressurizer pressure trip, core protection calculators, and steam generator low level trip) would have to fail in the no trip state to prevent both reactor trip and EFW actuation. Due to the nature of the PPS logic, for some failure combinations up to 44 out of 48 bistable relays and 62 out of 72 matrix relays could simultaneously fail in the no trip condition without causing a failure of both the reactor to trip and the EFW to actuate.

CEN-349 stated that, although the EFAS and RTS power supplies are not independent, their design also protects against common mode failures. All PPS power supplies have two circuits, one providing power and the other supplying overvoltage protection, that are diverse and independent of one another. It would require the simultaneous occurrence of two different types of common mode failure, one causing an overvoltage condition on the power circuit and the other causing a failure of the overvoltage protection circuit, in order for a power supply failure to cause both a failure of the RTS to trip the reactor and a failure of the EFAS to actuate EFW.

The NRC Staff's response to CEN-349 stated that ANO 2, SONGS 2&3, and Waterford 3 did not satisfy the ATWS rule requirement for EFAS diversity because the bistable relays and matrix relays in the EFAS are identical to their counterparts in the RTS. In addition, the power supplies in the EFAS and RTS are not independent. The Staff therefore concluded that either:

(1) diversity and independence must be provided in the areas where they are lacking, or

(2) an exemption from the ATWS rule must be requested in accordance with the provisions of 10 CFR 50.12.

After evaluating the above options, LP&L has concluded that the most prudent choice, considered in conjunction with ATWS risk reduction, is to seek an exemption. Therefore, an exemption is requested from the requirement to have equipment diverse and independent from the RTS to automatically initiate the emergency feedwater system under ATWS conditions. Included as the Appendix to this submittal is CEN-380, dated September 1988, entitled "ATWS Rule 10CFR50.62 Request for Exemption For Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3, and Waterford Steam Electric Unit 3," which is the detailed request for this exemption. Also included as part of the Appendix in support of the exemption request is CEN-380 Supplement 1, dated September 1988, entitled "Evaluation of ATWS Rule 10CFR50.62 Risk Reduction To Support Request For Exemption for Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3 and Waterford Steam Electric Station Unit 3." The Staff's expeditious review of CEN-380 and CEN-380 Supplement 1 is requested.

The following discussions present LP&L's position that adequate diversity from the RTS exists for the presently installed EFAS, to the extent reasonable and practicable. Although an exemption is being requested to the diverse EFAS requirements of 10CFR50.62, LP&L feels it worthwhile to reiterate our original position for completeness of the record, and for a more extensive review of the EFAS design features.

4.1. GUIDANCE REGARDING SYSTEM AND EQUIPMENT SPECIFICATIONS FOR EFAS

The supplemental information provided with the Federal Register notification of the ATWS rule (49 FR 26043, 26044), gives guidance to establish the level of diversity between the EFAS and the RTS required by the ATWS rule (10 CFR 50.62). The guidance suggests that equipment diversity to minimize the potential for CMF between the EFAS and the RTS is necessary from sensor output to but not including the final actuation device. The same eleven areas of guidance applied to the DSS and TT will also be applied to verify the acceptability of the EFAS.

4.1.1. SAFETY-RELATED (IEEE-279)

Staff Position - Not required but the implementation must be such that the existing protection system continues to meet all applicable safety related criteria.

The EFAS at Waterford 3 is a subsystem of the engineered safety features actuation system (ESFAS). The Waterford 3 FSAR (Section 7.1.2.1.1a) states that IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, was used as part of the design basis for the ESFAS. Therefore, though not required in the staff position, the EFAS conforms to this IEEE standard. Additionally, the EFAS is already installed at Waterford 3 so it can not effect a change in any applicable safety criteria of the RTS.

4.1.2. REDUNDANCY

Staff Position - Not required.

As in the case for the DSS, the staff does not require redundancy for the EFAS, since it does not preclude CMF occurrences. The existing EFAS employs two parallel circuitry paths based on a two out of four logic. This redundancy provides appropriate reliability and accuracy.

4.1.3. DIVERSITY FROM EXISTING REACTOR TRIP SYSTEM

Staff Position - Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failures is required from the sensors to, but not including, the final actuation device (e.g., existing circuit breakers may be used for auxiliary feedwater initiation). The sensors need not be of a diverse design or manufacturer. Existing protection system instrument sensing lines may be used. Sensors and instrument sensing lines should be selected such that adverse interactions with existing control systems are avoided.

The first components in the trip path are the sensors. The existing RTS sensors which measure parameters indicative of an ATWS include the resistance temperature detectors (RTDs), pressurizer pressure sensors, and steam generator level sensors. Of these ATWS indicating sensors, the RTDs provide nearly ideal diversity from the level sensors used by the EFAS. The RTDs provide core inlet temperature input to the core protection calculator (CPC) for use in the RTS. The steam generator level sensors used by the EFAS are diverse from the RTDs used by the RTS in design principle. The EFAS level sensors are the Rosemount capacitance capsule type sensors mentioned in Section 2.1. These level sensors use a Westinghouse process card. The RTDs (RTS) are manufactured by Weed and Rosemount. They use wheatstone bridges manufactured by Rosemount.

The second components in the trip path are the bistables. The bistables used by the EFAS are diverse from the RTS CPC bistables in manufacturer (Electro-Mechanics for the EFAS versus Gould-Systems Engineers Laboratory for the CPCs) and des[illegible] principle (analog for the EFAS versus digital for the CPCs). Thus [illegible] steam generator level bistables have nearly ideal diversity from t[illegible] bistables.

The third compon[illegible]e trip path are the bistable relays. The bistable relays used by [illegible]re identical to those used by the CPC, steam generator low l[illegible]) and the high pressurizer pressure (HPP) trips. They are electromechanical devices manufactured by Electro-Mechanics using the same design principle and having the same model number. These components, however were custom designed and custom built for the Plant Protection System (PPS). As such, it would not be "reasonable or practicable" to replace them with diverse components, as qualified, diverse replacements would be extremely difficult or impossible to obtain.

The design of these bistable relays provides protection against a CMF that disables both the RTS and the EFAS. The operating history of these bistable relays indicates that they are not vulnerable to a CMF. CMFs fall into three classes: (1) those due to a common manufacturing defect, (2) those due to an external fault that causes multiple failures of like components, and (3) those due to common operating history. These relays do not appear to be vulnerable to a common manufacturing defect, as they have been used for a number of years in C-E plants with only isolated, random failures of individual relays. Protection against external fault CMFs is furnished through adherence to the other ATWS guidance criteria (e.g. environmental qualification, seismic qualification, etc.). The third class, a CMF due to common operating history, is considered to be a very low probability occurrence, as it would have to affect a large number of components in several separate channels, and separate functions at the same time. An investigation of the bistable logic supports this. The Appendix (CEN-380 and CEN-380 Supplement 1) to this sumbittal provides further justification for not replacing these components.

The different PPS functions of interest to EFAS are the CPC, HPP, and SGLL trip paths, and the EFAS function. Each PPS function has four channels, and each channel has three bistable relays. Thus, there are 48 bistable relays of interest. A trip of any bistable relay causes a trip in its associated coincident logic matrix. Since the PPS uses a two-out-of-four coincident logic, a minimum of 24 out of 48 relays would have to simultaneously fail in the no trip state to prevent both a reactor trip and actuation of the emergency feedwater system. As many as 44 out of 48 bistable relays could simultaneously fail in the no trip state without preventing either a reactor trip or actuation of the emergency feedwater system. LP&L is unaware of a failure of safety system electrical components of this order ever occurring in the commercial nuclear power industry.

The fourth components in the trip path are the matrix relays. The matrix relays used by the EFAS are electromechanical devices manufactured by Electro-Mechanics. They use the same design principle and have the same model number as the matrix relays used by the CPCs and the HPP trip in the RTS. Like the bistable relays, these components were custom designed and custom built for the PPS. As previously mentioned and further discussed in the Appendix (CEN-380 and CEN-380 Supplement 1) to this submittal, it would not be "reasonable or practicable" to replace them with diverse components, as qualified, diverse components would be extremely difficult or impossible to obtain.

Much like the bistables, the matrix relays provide protection against a CMF that disables both the RTS and the EFAS. The operating history of these relays indicate that they too are reliable and not likely to suffer any of the three types of CMF previously mentioned. Common manufacturing defects have not been shown to be credible. The successful operating history of these relays in CE plants reveals only isolated, random failures of individual relays. External fault CMFs are unlikely since adherence to the other ATWS guidance criteria (e.g. equipment qualification, seismic qualification, etc.) protects against this. Common operating history CMFs are considered a very low probability occurrance. As with the bistables, a large number of components in several, separate channels, and functions would have to be affected at the same time.

There are six matrices associated with the RTS and twelve matrices associated with the EFAS function. Since each matrix has four relays, there are a total of 72 relays of interest. A minimum of twelve out of the 24 RTS matrix relays and twelve out of the 48 EFAS matrix relays would have to simultaneously fail in the no trip state to prevent both a reactor trip and actuation of the EFAS. As many as 22 of the 24 RTS matrix relays and 40 out of the 48 EFAS matrix relays could simultaneously fail in the no trip state without preventing either a reactor trip or actuation of the EFAS. LP&L is unaware of a failure of safety system electrical components of this order ever occurring in the commercial nuclear power industry.

The fifth components in the trip path are the initiation relays. The initiation relays used by both the EFAS and the RTS are solid state, DC input relays manufactured by Teledyne. However, the electrical characteristics of the relays for the two systems are very different as shown below.

PARAMETER	RTS RELAYS	EFAS RELAYS
Input Voltage Range	3 to 28 VDC	3 to 50 VDC
Capacitance	10 Picofarads	2 Picofarads
Turn-on Time	3 Milliseconds	50 Microseconds
Turn-off Time	5 Milliseconds	30 Microseconds
Isolation Resistance	10^9 Ohms (minimum)	10^{11} Ohms (minimum)
Dielectric Strength	1500 VAC	1000 VDC
Output Voltage	120 VAC	60 VDC
Output Current Rating	10 Amp AC	10 Amp DC (Resistive)
Temperature Range	-30°C to 80°C	-55°C to 110°C

Differences also exist in turn-on/turn-off current, overvoltage, leakage, and power dissipation. Due to the differences in electrical characteristics, the physical characteristics of these relays also differ. Therefore, the EFAS initiation relays are diverse from these of the RTS.

The sixth components in the trip path are the actuation devices. The actuation devices used by the EFAS are diverse from those used by the RTS in manufacturer (Potter-Brumfield for the EFAS and General Electric for the RTS), and design principle (electromechanical rotary relays with multiple contacts for the EFAS vs mechanical circuit breakers for the RTS). The actuation devices used by the EFAS are 28 volt devices powered by 36 VDC power supplies. The actuation devices used by the RTS are 125 volt devices powered by 125 VDC power supplies. Both the EFAS and RTS actuation devices are "deenergize to trip" devices. However, the RTS actuation devices have a redundant "energize to trip" feature (the shunt trip coils). Thus, the EFAS actuation devices have nearly ideal diversity from the RTS actuation devices.

The rotary relays in the RTS are used as a post-initiation device where the EFAS rotary relays act as the actuation device. Both are Potter-Brumfield, however, substantial diversity exists between the EFAS rotary relays and the RTS relays. The rotary relays used in the EFAS are powered by 36 VDC power supplies while the rotary relays used in the RTS are powered by the 120 VAC power supplies. The EFAS relays differ from the RTS rotary relays in voltage, current, DC resistance, coil power, and operate time as shown below. These relays also differ in physical construction. The EFAS MDR 136-1 is physically smaller than the MDR 170-1 (i.e., Potter-Brumfield small frame versus a medium frame). In addition, the windings in the EFAS rotary relays (MDR 7032, 7033, 7034) have special coil lead routing while the RTS rotary relays use the standard Potter-Brumfield construction. Additional design details are provided below to demonstrate the high level of diversity between the EFAS relays and the RTS relays.

DESIGN PARAMETER	RTS	EFAS			
	MDR-170-1**	MDR 7032*	MDR 7033*	MDR 7036*	MDR 136-1**
Relay Frame Size	medium	medium	medium	medium	small
Input Voltage	115 VAC	28 VDC	28 VDC	28 VDC	28 VDC
Contact Arrangement	16 Form C	12 Form C 3 Form Y	24 Form C	16 Form C	8 Form C
Coil Current (amps)	0.620	0.667	0.667	0.667	0.362
DC Coil Resistance (ohms)	8.4	42	42	42	8.76

DESIGN PARAMETER	RTS	EFAS			
Steady State Power (watts)	17.0	18.7	18.7	18.7	10.0
Breakdown Voltage (VAC RMS)	1230	1310	1310	1310	1308
Deck Arrangement	4 decks	6 decks	6 decks	4 decks	2 decks

* special construction coils and coil power leads and deck/contact arrangement

** off the shelf type relays, i.e., normal catalog items

Of the components shown for the EFAS and the RTS in Figure 2, only two, the bistable relays and the matrix relays, fail to exhibit an obvious diversity between the two systems. As previously stated, these components were custom designed and custom built for the PPS at Waterford 3. Therefore, it would not be "reasonable or practicable" to replace these since qualified, diverse replacements would be extremely difficult or impossible to obtain. Additionally, it was pointed out that the prevention of a reactor trip and automatic actuation of emergency feedwater resulting from a failure of these relays could only be from the unlikely, simultaneous failure of a large number of bistable relays or matrix relays in different functions and physically separate channels. Therefore, replacing these components would not significantly reduce the probability of a CMF which might result in an ATWS. As such, the design of the PPS provides a level of protection against CMFs comparable to that which might be provided by an EFAS comprised entirely of components that satisfy the criteria for component diversity. Therefore, LP&L considers the existing level of diversity of the EFAS acceptable.

The DSS to be installed at Waterford 3 will be completely diverse from the existing RTS and EFAS functions. As such, the DSS will ensure the diversity between the EFAS and the new RTS (i.e., the existing RTS and the DSS). This will further reduce the chance that a CMF would prevent both a reactor trip and actuation of the emergency feedwater.

4.1.4. ELECTRICAL INDEPENDENCE FROM EXISTING REACTOR TRIP SYSTEM

Staff Position - Required from sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits.

As stated on page 2 of Enclosure A of SECY-83-293, Reference (3), the RTS includes power sources. Page 21 of Reference (2), however, states that power supply diversity is not required. Reference (2) further states, "power supply independence is required such that faults within the [EFAS] diverse actuation circuitry can not degrade the reliability/integrity of the existing RTS below an acceptable level, and that a common mode failure mechanism affecting the RTS power distribution system (including degraded voltage conditions such as overvoltage and undervoltage) can not compromise both the RTS and the [EFAS] diverse actuation functions". Features have been incorporated into the Waterford 3 EFAS to provide protection against a CMF mechanism that could affect the RTS power distribution system such that both the RTS and EFAS diverse actuation functions can not be simultaneously compromised.

Power supplies are presently shared between the RTS and the EFAS. All of the PPS power supplies have two circuits that are diverse from and independent of one another. One circuit provides power while the other provides overvoltage protection. It would require the simultaneous occurrence of two different types of CMFs one failing the overvoltage protection and the other causing an overvoltage condition on the same circuits, to produce the failure of both the RTS and diverse EFAS actuation circuitry due to an overvoltage condition. Upon a loss of power to any component with shared power (i.e., bistable relay or initiation relay) the affected channel will fail in the trip condition. In the event of an undervoltage condition which failed one of these relays, that relay would fail tripped. Hence, the existing EFAS complies with the ATWS Rule requirement of electrical independence.

4.1.5 PHYSICAL SEPARATION FROM EXISTING REACTOR TRIP SYSTEM

Staff Position - Not required unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated.

Physical separation from the RTS is provided for the EFAS. Separate cabinets house the EFAS electronics. This equipment is located on the +21 MSL elevation. Similar equipment for the RTS is located on the +46 MSL.

4.1.6. ENVIRONMENTAL QUALIFICATION

Staff Position - For anticipated operational occurrences only; not for accidents.

The EFAS is relied upon to remain functional during and following design basis events to ensure the capability to shutdown the reactor and maintain it in a safe shutdown condition. As such, the equipment comprising the EFAS is included in the Waterford 3 Equipment Qualification Program and subject to the requirements under 10 CFR 50.49. Therefore, this level of qualification exceeds the staff position.

4.1.7. SEISMIC QUALIFICATION

Staff Position - Not required.

The EFAS is defined as a safety related system and therefore the EFAS equipment is required to be qualified to seismic class I. This qualification surpasses the staff's recommendation for the EFAS.

4.1.8. QUALITY ASSURANCE FOR TEST, MAINTENANCE, AND SURVEILLANCE

Staff Position - The Commission has released a generic letter (85-06, April 16, 1986) in which is provided the explicit Quality Assurance (QA) guidance required by 10CFR50.62. While Appendix B is viewed as a useful reference in which to frame the staff's guidance for non-safety related ATWS equipment, it does not meet the intent of the ATWS QA program. The equipment encompassed by 10CFR50.62 is not required to be safety related; therefore, less stringent QA guidance is acceptable. This letter incorporates a lesser degree of stringency by eliminating requirements for involving parties outside the normal line organization and requirements for a formalized program and detailed record keeping for all quality practices.

As the Waterford 3 EFAS is a safety-related system, the less stringent QA guidance mentioned above is not applicable. The EFAS system must conform to Appendix B requirements, and as such QA for testing, maintenance and surveillance exceeds the guidance given in Generic Letter 85-06.

4.1.9. SAFETY-RELATED (1E) POWER SUPPLY

Staff Position - Not required, but must be capable of performing safety functions with loss of offsite power. Logic power must be from an instrument power supply independent from the power supplies for the existing reactor-trip system. Existing RTS sensor and instrument channel power supplies may be used provided the possibility of common mode failure is prevented.

As described for the DSS, the RTS is composed of four channels, A, B, C and D. Each channel possesses circuitry identical to the RTS circuitry represented in Figure 2. Channels A and C are powered from the "A" battery, and Channels B and D are powered from the "B" battery. Likewise, the EFAS is composed of four channels, A, B, C and D, each channel identical to the EFAS circuitry shown in Figure 2. Channels A and C receive power from battery "A", and Channels B and D receive power from battery "B". The Waterford 3 EFAS is a safety-related system. Since power supplies for a system are considered part of that system, the power supplies for the Waterford 3 EFAS are 1E safety-related. They are functional during a loss of offsite power and are independent from the RTS power supplies as described above.

4.1.10. TESTABILITY AT POWER

Staff Position - Required.

Provisions are made to permit periodic testing of the EFAS. These tests cover the sensors' input through the actuation devices. The system test does not interfere with the protection function of the system and therefore can be performed at power.

4.1.11. INADVERTENT ACTUATION

Staff Position - The design should be such that the frequency of inadvertent reactor trip and challenges to other safety systems is minimized.

The EFAS operates on a two-out-of-four logic for each steam generator. Similarly, reliable power supplies are used and sufficient tests run to support a satisfactory level of quality assurance features. These design features are more than sufficient to meet the goal to minimize the frequency of inadvertent actuation and challenges to other safety systems.

4.2. EFAS CONCLUSION

Of the six major components in the EFAS, four are clearly diverse from the RTS. The remaining two are the bistable relays and the matrix relays. These components are custom designed and custom built. It would not be reasonable or practicable to replace these with diverse relays. The high reliability of these components, coupled with the physical separation of the RTS and the EFAS channels, and the large number of components which would have to fail in an adverse manner to disable both the EFAS and the RTS, provides a level of protection against CMFs comparable to that which would be provided by components that satisfy the staff's diversity criteria. As such, LP&L considers the diversity level of the EFAS acceptable.

5.0 SUMMARY

The ATWS rule requires that Waterford 3 be equipped with a DSS which is diverse from the existing RTS, a TT which is diverse from the RTS, and an EFAS which is diverse from the RTS. Based on the adherence to the staff guidelines as presented in this report, it is concluded that, with the addition of the DSS/TT circuitry, and the existence of the present EFAS, sufficient diversity will exist from the present RTS to the extent reasonable and practicable to meet the requirements of the ATWS rule. In that the NRC has concluded that some relays in the Waterford 3 EFAS do not meet the diversity requirements of the ATWS rule, a request for exemption to the EFAS requirements of 10CFR50.62 is submitted in the Appendix to this report.

6.0 REFERENCES

1. CEN-315, "Summary of the Diversity Between the Reactor Trip System and the Auxiliary Feedwater System for C-E Plants", September 1985.

2. D. M. Crutchfield (NRC) to R. W. Wells (CEOG), NRC Staff Evaluation of CEN-315, "Summary of the Diversity Between the Reactor Trip System and the Auxiliary Feedwater Actuation System", August 4, 1985.

3. W. R. Dirks, NRC Staff, to the Commissioners, Amendments to 10CFR50 Related to Anticipated Transient Without Scram (ATWS) Events, SECY-83-293, Dated July 19, 1983.

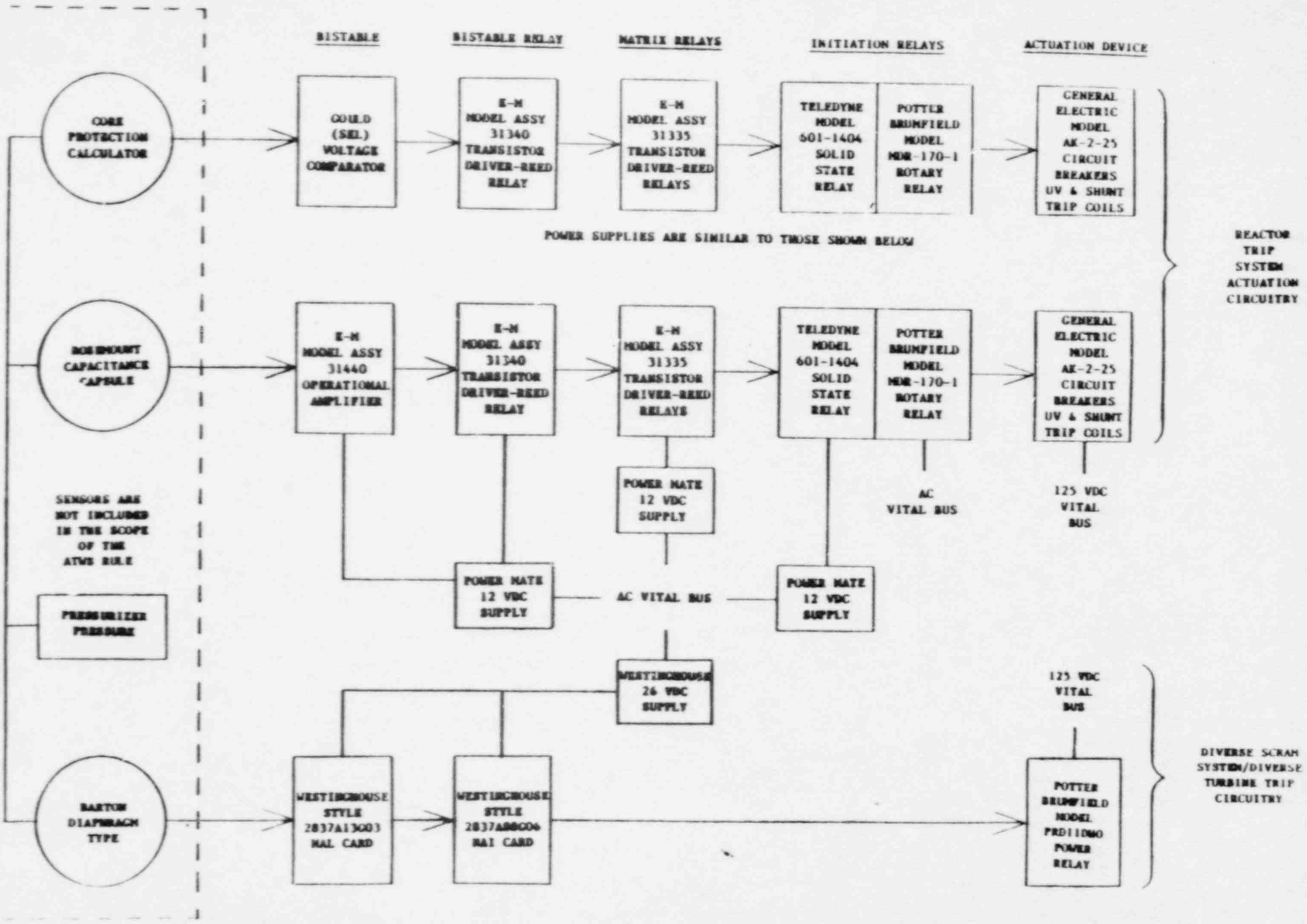
4. CEN-349, "Response to the NRC's Evaluation of CEN-315 for San Onofre Nuclear Generating Station Units 2 and 3, Arkansas Nuclear One Unit 2, and Waterford Steam Electric Station Unit 3", November 25, 1986.

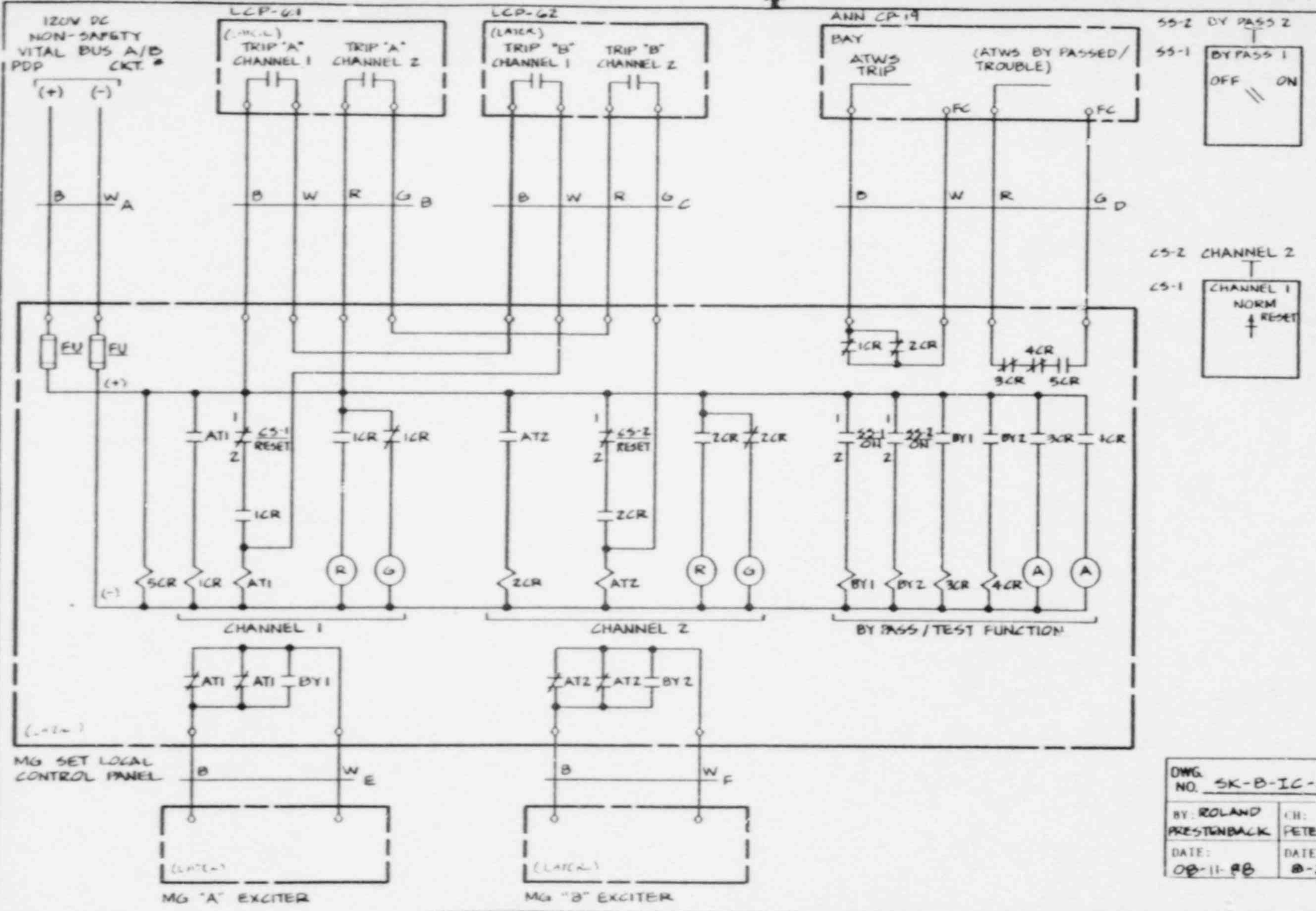
5. CEN-380, "ATWS Rule 10 CFR 50.62, Request For Exemption For Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3, and Waterford Steam Electric Station Unit 3", September, 1988.

6. CEN-380 Supplement 1, "Evaluation of Risk Reduction To Support A Request For Exemption From ATWS Rule 10 CFR 50.62 For Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3, and Waterford Steam Electric Station Unit 3", September, 1988.

FIGURES

DIVERSE SCRAM SYSTEM/DIVERSE TURBINE TRIP





SS-1, SS-2

CONTACTS	POSITION 10 1/2 OFF	POSITION 1 1/2 ON	CWD SH.
1-2		X	*
3-4	X		

TYPE PTK * THIS SHT.

MAINTAINED CONTACTS, KEY REMOVABLE IN OFF POSITION ONLY

CS-1, CS-2

CONTACTS	POSITION 12 NORM	POSITION 3 RESET	CWD SH.
1-2	X		*
3-4		X	

TYPE PTS

MAINTAINED CONTACTS IN NORM, SPRING RETURN FROM RIGHT

DWG. NO. SK-B-IC-0007		APPROVED
BY: ROLAND PRESTENBACK	CH: PETER KLEIN	DFTG SUPV:
DATE: 08-11-88	DATE: 8-23-88	DATE: 8-25-88

8				4			
7				3			
6				2			
5				1			
REV	DATE	BY	APPROVED	REV	DATE	BY	APPROVED

DIV I&C RSP

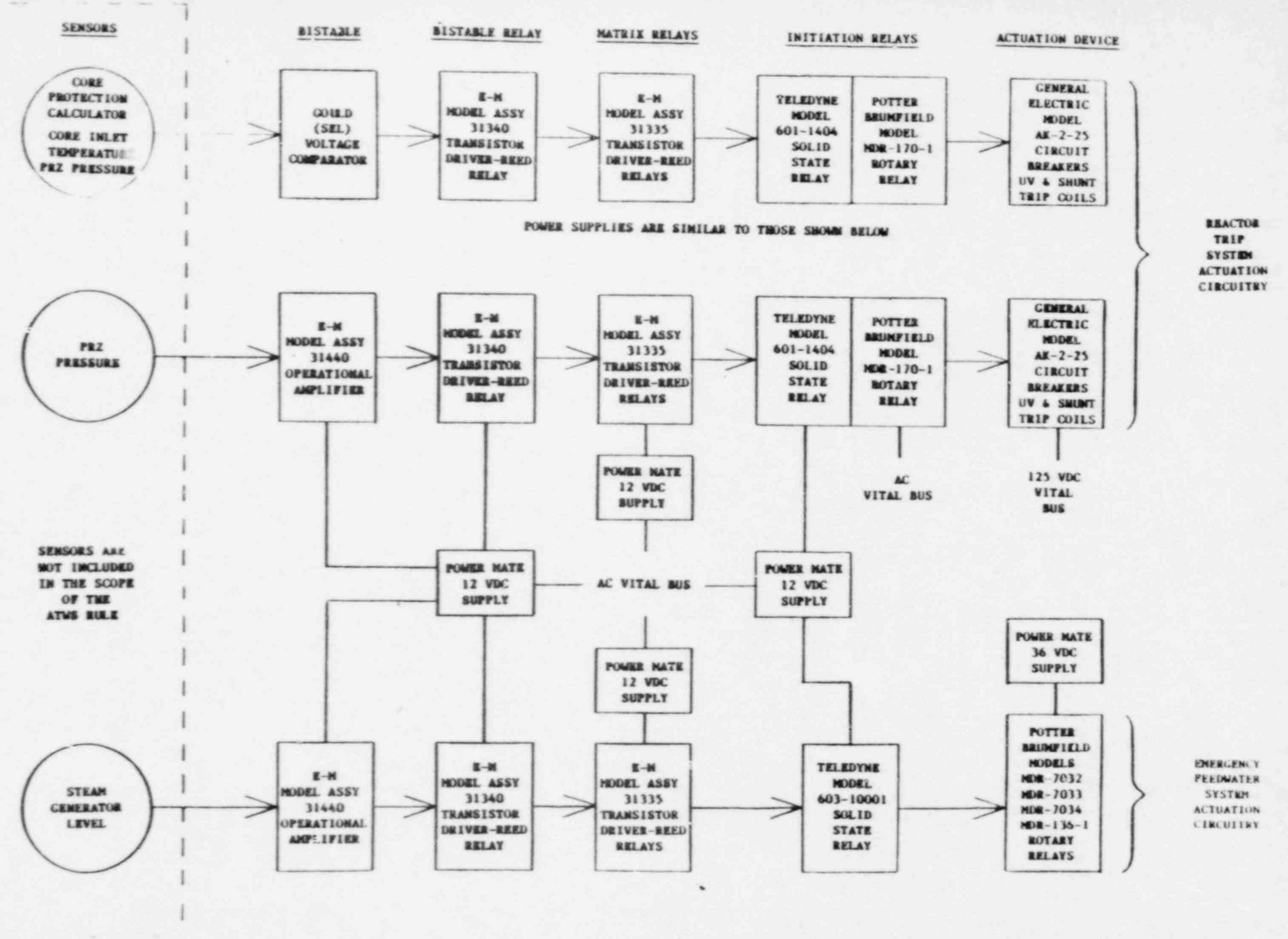
CH DRAFT. SUPV

APPROVED

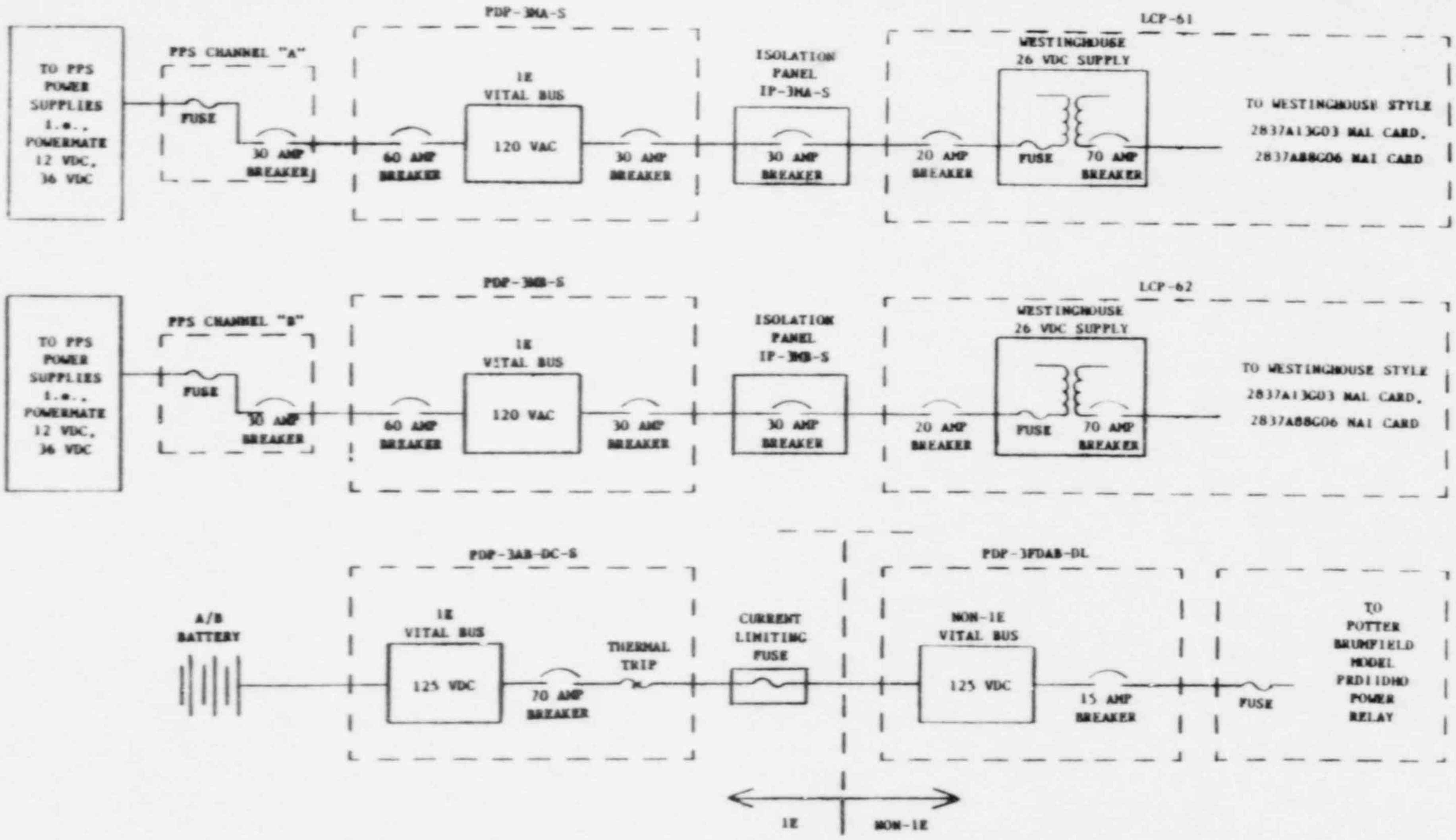
LOUISIANA POWER & LIGHT CO.
WATERFORD S. E. S. UNIT No.3
CONTROL WIRING DIAGRAM

ANTICIPATED TRANSIENT WITHOUT SCRAM

SMP'S INCORP. THIS REV.


SENSORS
BISTABLE
BISTABLE RELAY
MATRIX RELAYS
INITIATION RELAYS
ACTUATION DEVICE
CORE PROTECTION CALCULATOR
CORE INLET TEMPERATURE
PRZ PRESSURE
GOULD (SEL) VOLTAGE COMPARATOR
E-M MODEL ASSY 31340 TRANSISTOR DRIVER-REED RELAY
E-M MODEL ASSY 31335 TRANSISTOR DRIVER-REED RELAYS
TELEDYNE MODEL 601-1404 SOLID STATE RELAY
POTTER BRUMFIELD MODEL MDR-170-1 ROTARY RELAY
GENERAL ELECTRIC MODEL AK-2-25 CIRCUIT BREAKERS UV & SHUNT TRIP COILS
POWER SUPPLIES ARE SIMILAR TO THOSE SHOWN BELOW
REACTOR TRIP SYSTEM ACTUATION CIRCUITRY
PRZ PRESSURE
E-M MODEL ASSY 31440 OPERATIONAL AMPLIFIER
E-M MODEL ASSY 31340 TRANSISTOR DRIVER-REED RELAY
E-M MODEL ASSY 31335 TRANSISTOR DRIVER-REED RELAYS
TELEDYNE MODEL 601-1404 SOLID STATE RELAY
POTTER BRUMFIELD MODEL MDR-170-1 ROTARY RELAY
GENERAL ELECTRIC MODEL AK-2-25 CIRCUIT BREAKERS UV & SHUNT TRIP COILS
POWER MATE 12 VDC SUPPLY
AC VITAL BUS
125 VDC VITAL BUS
SENSORS ARE NOT INCLUDED IN THE SCOPE OF THE ATWS RULE
POWER MATE 12 VDC SUPPLY
AC VITAL BUS
POWER MATE 12 VDC SUPPLY
POWER MATE 12 VDC SUPPLY
POWER MATE 36 VDC SUPPLY
STEAM GENERATOR LEVEL
E-M MODEL ASSY 31440 OPERATIONAL AMPLIFIER
E-M MODEL ASSY 31340 TRANSISTOR DRIVER-REED RELAY
E-M MODEL ASSY 31335 TRANSISTOR DRIVER-REED RELAYS
TELEDYNE MODEL 603-10001 SOLID STATE RELAY
POTTER BRUMFIELD MODELS MDR-7032 MDR-7033 MDR-7034 MDR-136-1 ROTARY RELAYS
EMERGENCY FEEDWATER SYSTEM ACTUATION CIRCUITRY

FROM THE EXISTING REACTOR TRIP SYSTEM



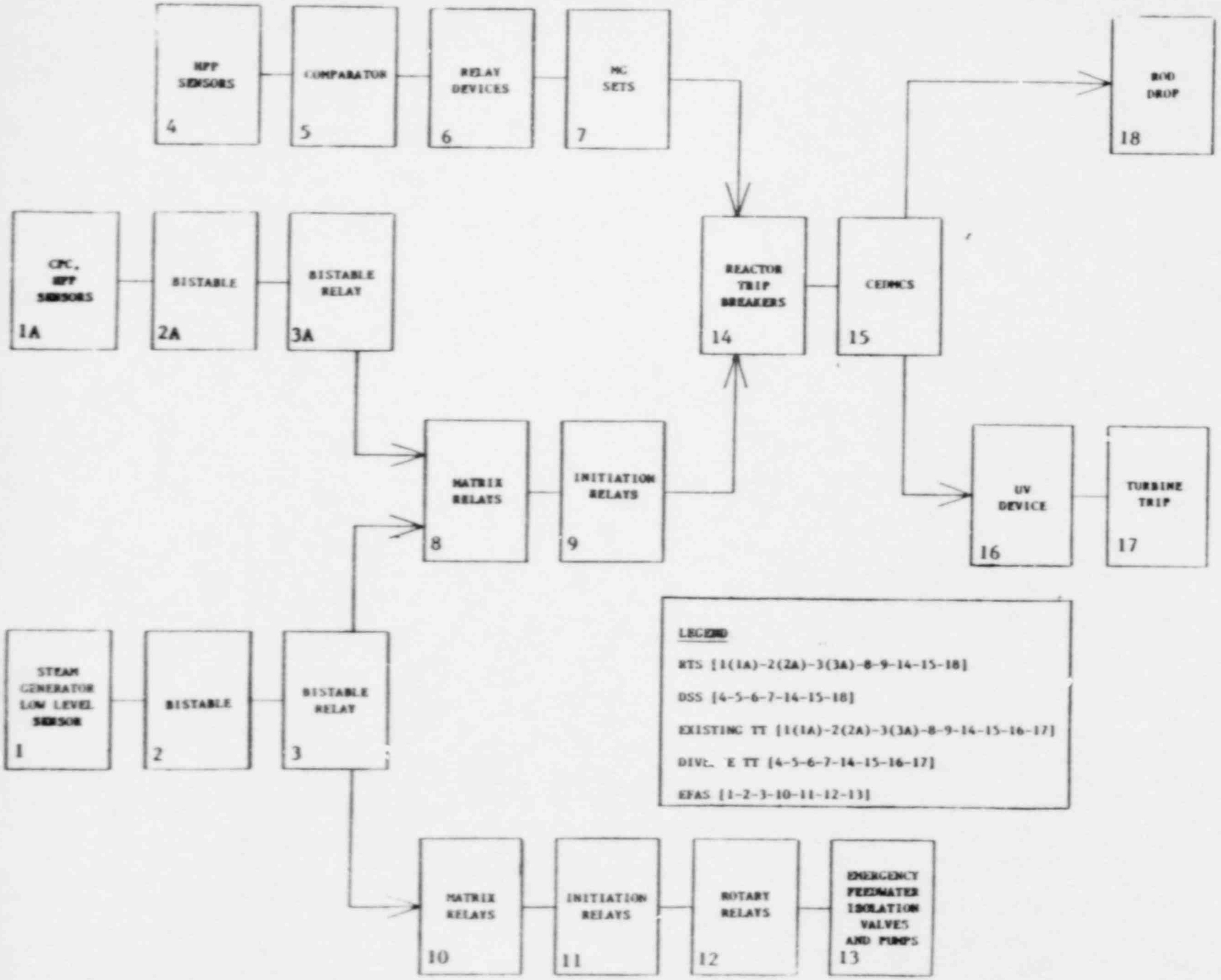
NOTES:

1) PDP-3MA-S AND 3MB-S ARE VITAL 1E BUSES WITH BATTERY BACKUP.

2) PDP-3AB-DC-S IS NOT CONNECTED TO THE PPS SYSTEM IN ANY CHANNEL.

3) VITAL BUSES SHOWN ARE ALL AVAILABLE ON LOSS OF OFF-SITE POWER.

4) A 24 VDC POWER SUPPLY ACTS AS BACKUP TO 26 VDC AND IS WIRED SIMILARLY IN LCP-61 AND LCP-62.


HPP SENSORS 4
COMPARATOR 5
RELAY DEVICES 6
MG SETS 7
ROD DROP 18
CPC, HPP SENSORS 1A
BISTABLE 2A
BISTABLE RELAY 3A
REACTOR TRIP BREAKERS 14
CEDMCS 15
MATRIX RELAYS 8
INITIATION RELAYS 9
UV DEVICE 16
TURBINE TRIP 17
STEAM GENERATOR LOW LEVEL SENSOR 1
BISTABLE 2
BISTABLE RELAY 3
LEGEND
RTS [1(1A)-2(2A)-3(3A)-8-9-14-15-18]
DSS [4-5-6-7-14-15-18]
EXISTING TT [1(1A)-2(2A)-3(3A)-8-9-14-15-16-17]
DIVERSE TT [4-5-6-7-14-15-16-17]
EFAS [1-2-3-10-11-12-13]
MATRIX RELAYS 10
INITIATION RELAYS 11
ROTARY RELAYS 12
EMERGENCY FEEDWATER ISOLATION VALVES AND PUMPS 13

[redacted]

APPENDIX

REQUEST FOR EXEMPTION

CEOG COMBUSTION ENGINEERING OWNERS GROUP

CEN-380

ATWS RULE 10 CFR 50.62
REQUEST FOR EXEMPTION

FOR

ARKANSAS NUCLEAR ONE UNIT 2
SAN ONOFRE NUCLEAR GENERATING
STATION UNITS 2 AND 3
AND
WATERFORD STEAM ELECTRIC STATION
UNIT 3

PREPARED FOR THE

C-E OWNERS GROUP

SEPTEMBER, 1988

COMBUSTION ENGINEERING, INC.

CEN-380
FINAL REPORT

ATWS RULE 10CFR50.62

REQUEST FOR EXEMPTION

FOR

ARKANSAS NUCLEAR ONE UNIT 2
SAN ONOFRE NUCLEAR GENERATING STATION UNITS 2 AND 3
AND
WATERFORD STEAM ELECTRIC STATION UNIT 3

SUBMITTED BY

ARKANSAS POWER AND LIGHT COMPANY
SOUTHERN CALIFORNIA EDISON COMPANY
AND
LOUISIANA POWER AND LIGHT COMPANY

September, 1988

Prepared by

C-E POWER SYSTEMS
COMBUSTION ENGINEERING, INC.

ABSTRACT

This submittal provides the basis and supporting documentation to request exemption from a requirement of Title 10 of the Code of Federal Regulations Section 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants" for Arkansas Nuclear One Unit 2 (ANO 2), San Onofre Nuclear Generating Station Units 2 and 3 (SONGS 2 & 3), and Waterford Steam Electric Station Unit 3 (WSES 3). The submittal will address the requirements of Title 10 of the Code of Federal Regulations Section 50.12 " Specific Exemptions", in terms of exemption from the ATWS Rule and address issues posed by the Nuclear Regulatory Commission Staff concerning a request for exemption from the ATWS rule. Arkansas Power and Light Company (AP&L), Southern California Edison Company (SCE), and Louisiana Power and Light (LP&L) propose to install at each of their respective plants, (ANO 2, SONGS 2 & 3, and WSES 3), a Diverse Scram System which is diverse from the existing Reactor Trip System. These modifications will also provide a turbine trip, as required by the ATWS rule, that is diverse and independent from the existing Reactor Trip System. The installation of this Diverse Reactor Trip System alone will be demonstrated to achieve ATWS risk reduction in a cost-effective manner, which is the underlying purpose of Title 10 of the Code of Federal Regulations, Section 50.62. AP&L, SCE, and LP&L are requesting in this submittal exemption from the portion of Title 10 of the Code of Federal Regulations Section 50.62 that requires equipment diverse from the reactor trip system to initiate the emergency feedwater system under conditions indicative of an ATWS.

MSIS	Main Steam Isolation System
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MTC	Moderator Temperature Coefficient
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
P ATWS	Probability of a Severe Anticipated Transient Without Scram
PSV	Primary Safety Valve
QA	Quality Assurance
QSPDS	Qualified Safety Parameters Display System
RCS	Reactor Coolant System
RPS	Reactor Protective System
RTS	Reactor Trip System
SCE	Southern California Edison Company
SDG&E	San Diego Gas and Electric
SONGS 2 & 3	San Onofre Nuclear Generating Station Units 2 and 3
SG	Steam Generator
SGLL	Steam Generator Low Level
TT	Turbine Trip
VIR	Value Impact Ratio
UPS	Uninterruptable Power Supply
WSES 3	Waterford Steam Electric Station Unit 3

LIST OF ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
AFAS	Auxiliary Feedwater Actuation System
AFS	Auxiliary Feedwater System
ANO 2	Arkansas Nuclear One Unit 2
ASME	American Society of Mechanical Engineers
AP&L	Arkansas Power and Light
AT	Anticipated Transients
ATWS	Anticipated Transients Without Scram
B&W	Babcock and Wilcox
CD	Core Damage
C-E	Combustion Engineering, Inc.
CEA	Control Element Assembly
CEDMCS	Control Element Drive Mechanism Control System
CEOG	Combustion Engineering Owners' Group
CFR	Code of Federal Regulations
CFMS	Critical Function Monitoring System
CMF	Common Mode Failure
DNBR	Departure From Nucleate Boiling
DTT	Diverse Turbine Trip
EFS	Emergency Feedwater System
E-M	Electro-Mechanics
EFAS	Emergency Feedwater Actuation System
EFW	Emergengy Feedwater
EFWS	Emergency Feedwater System
DSS	Diverse Scram System
G-E	General Electric
HPI	High Pressure Injection
HPPTS	High Pressurizer Pressure Trip Setpoint
LP&L	Louisiana Power and Light
MFIV	Main Feed Isolation Valve
MFWS	Main Feedwater System
M-G	Motor Generator

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

1.1 PURPOSE

This submittal provides information to support and requests an exemption from a portion of Title 10 of the Code of Federal Regulations (CFR) Section 50.62 (10CFR50.62), "Requirements for Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," as it pertains to Arkansas Nuclear One Unit 2 (ANO 2), San Onofre Nuclear Generating Station Units 2 and 3 (SONGS 2 & 3), and Waterford Steam Electric Station Unit 3 (WSES 3). Specifically, exemption is requested under Title 10 of the Code of Federal Regulations, Section 50.12 (10CFR50.12), from the requirement that these plants have equipment which is diverse and independent from the reactor trip system to automatically initiate the emergency feedwater system under conditions which are indicative of an Anticipated Transient Without Scram (ATWS).

1.2 BACKGROUND

1.2.1 10CFR50.62 Requirements

On June 26, 1984, the Code of Federal Regulations was amended to included Section 10CFR50.62, "Requirements for Reduction of Risk from Anticipated Transient Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants." The requirements of 10CFR50.62, henceforth referred to as the ATWS Rule, as they pertain to ANO 2, SONGS 2 & 3, and WSES 3, are as follows:

> ". . . (c) Requirements. (1) Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative

of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

(2) Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods). . .

(6) Information sufficient to demonstrate to the Commission the adequacy of items in paragraphs (c)(1) through (c)(5) of this section shall be submitted to the Director, Office of Nuclear Reactor Regulation.

(d) Implementation. By 180 days after the issuance of the QA guidance for non-safety related components each licensee shall develop and submit to the Director of the Office of Nuclear Reactor Regulation a proposed schedule for meeting the requirements of paragraphs (c)(1) through (c)(5) of this section. Each shall include an explanation of the schedule along with a justification if the schedule calls for final implementation later than the second refueling outage after July 26, 1984, or the date of issuance of a license authorizing operation above 5 percent of full power. A final schedule shall then be mutually agreed upon by the Commission and licensee."

1.2.2 Underlying Purpose of 10CFR50.62

From its inception, 10CFR50.62 was justified by the NRC Staff on a value/impact (i.e., benefit/cost) basis as a means to reduce the probability of common mode failures affecting the RTS and certain systems that are relied upon to mitigate an ATWS event. A Commission letter, henceforth referred to as SECY-83-293, provides detailed background for the Rule. This letter, Reference 1.1, states on page 5, "The (NRC) staff believes that the final rule . . ., if made effective, would substantially reduce the ATWS risk in a cost effective manner and assure an acceptable level of risk from ATWS events."

The Statement of Considerations for 10CFR50.62 indicates that the purpose of the ATWS rule is to reduce the probability of common mode failures in the system that would prevent or mitigate an ATWS event. Value/impact analyses were an important consideration in the formulation of the Rule. The Statement of Considerations contains a section entitled "Basis for Final Rule as Promulgated by the Commission" (49FR26037, 26038). The requirement for diverse* and independent* emergency feedwater actuation and diverse Turbine Trip is justified by the Staff based on their stated belief that, "It has a highly favorable value/impact for Westinghouse plants and a marginally favorable value/impact for Combustion Engineering and Babcock and Wilcox plants." The following paragraph of this section discusses the requirement for a Diverse Scram System (DSS) in C-E, B&W, and G-E plants. This section states, "It (the DSS) has a favorable value/impact from the Staff's analysis. However, the principal reasons for requiring the feature are to assure emphasis on accident prevention and to obtain the resultant decrease in potential common cause failure paths in the trip system."

---

*Unless otherwise stated, "diverse" means diverse from the reactor trip system. Similarly, "independent" means independent from the reactor trip system.

SECY-83-293 stresses the importance of engineering judgement in the formulation of the Rule. Enclosure D of SECY-83-293 on page 7 states. "It is also realized that doing value/impact calculations is somewhat subjective in arriving at the optimal level of fix, due to uncertainty in probabilistic assessments and in the cost estimates for the modification. Therefore, the Task Force used value-impact calculations only as an aid to evaluate the ATWS rule alternatives." Page 9 of Enclosure D goes on to state, "When value-impact results were borderline, the Task Force relied much more on engineering judgement to determine whether an alternative should or should not be included in the ATWS rule."

Although the NRC Staff has stated that value/impact calculations are not the only basis for its rule making, they have rejected requirements for plant hardware modification that had an unfavorable value/impact ratio (i.e., significantly less than one) and were judged to not contribute significantly to ATWS risk reduction. For example, Enclosure D to SECY-83-293 (pages 2, 31, and 48) indicates that for C-E and B&W plants the NRC staff computed a value/impact ratio of 0.44 for installing extra primary safety valves. The Federal Register, Statement of Considerations accompanying 10CFR50.62 contains a section entitled, "Adding Extra Safety Valves or Burnable Poisons", which indicates that the Staff did not recommend that the Rule require the installation of more safety valves because, ". . .the value/impact is unfavorable for this alternative for existing (C-E and B&W) plants. These plants all have large dry containments and will be most able to mitigate the radiological consequences from an ATWS."

Based on both the Statements of Considerations for the Rule and SECY-83-293, it is concluded that the purpose of the ATWS Rule is to reduce the probability of a severe ATWS* event in a cost-effective manner by reducing the susceptibility of the RTS, EFAS, and TT to common mode failures.

---

*Consistent with the criterion provided in Reference 1.2 and Section 5.5 of Enclosure D to SECY-83-293, a "severe ATWS" event is defined as an ATWS that results in a RCS pressure greater than 3200 psia. The NRC's ATWS Task Force assumes that an ATWS event which results in RCS pressures in excess of ASME Level C pressure, about 3200 psia, will lead to an unacceptable plant condition.

1.2.3 Previous Submittals to the NRC Regarding EFAS Diversity

Since 1984, there has been an ongoing dialog between the Combustion Engineering Owners' Group (CEOG) and the NRC Staff regarding the level of diversity that presently exists between the EFAS and the RTS. In the months following the issuance of the ATWS rule, there were several meetings and telephone conversations between the NRC Staff and the CEOG ATWS Subcommittee. The position of the CEOG ATWS Subcommittee was that the existing level of EFAS diversity satisfies the ATWS Rule and that plant modifications to increase the level of diversity would not be cost beneficial. As a result of these interactions, the CEOG submitted CEN-315 (Reference 1.3) to the NRC. CEN-315 provided information on plant specific designs and diversity features that are generic to the C-E design to support the CEOG's position.

Reference 1.4 provided the Staff's evaluation of CEN-315. Based on the information provided, the Staff's preliminary conclusion was that ANO 2, SONGS 2 & 3, and WSES 3, did not appear to satisfy the ATWS rule requirement for a diverse and independent EFAS. This conclusion was based on the Staff's observation that many of the EFAS components did not appear to have adequate diversity and the EFAS power supplies did not appear to be independent. In Reference 1.4, however, the Staff also stated, that any other diversity considerations would be reviewed on a plant specific basis.

In response to Reference 1.4, CEN-349 (Reference 1.5) was submitted to the Staff. CEN-349 provided detailed information about the diversity between the EFAS and RTS for ANO 2, SONGS 2 & 3, and WSES 3. In evaluating EFAS diversity, CEN-349 considered the three RTS functions (i.e., high pressurizer pressure trip, core protection calculators, and steam generator low level trip) which would have to fail in order for an overpressure ATWS to occur. It demonstrated that all of the EFAS components except for the bistable and matrix relays were diverse from their counterparts in the RTS.

CEN-349 stated, however, that the design of the PPS provides a degree of protection against common mode failures of bistable relays disabling both the EFAS and RTS that is comparable to the protection which would be provided by diverse components. At a minimum, the right combination of 24 out of 48 bistable relays or 24 of of 72 matrix relays in the EFAS and the RTS functions of interest (high pressurizer pressure trip, core protection calculators, and steam generator low level trip) would have to fail in the no trip state to prevent both reactor trip and EFS actuation. Due to the nature of the PPS logic, for some failure combinations, up to 44 out of 48 bistable relays and 62 out of 72 matrix relays, could simultaneously fail in the no trip condition without causing a failure of both the reactor to trip and the EFS to actuate.

CEN-349 stated that, although the EFAS and RTS power supplies are not independent, their design also protects against common mode failures. All PPS power supplies have two circuits, one providing power and the other supplying overvoltage protection, that are diverse and independent of one another. It would require the simultaneous occurrence of two different types of common mode failure, one causing an overvoltage condition on the power circuit and the other causing a failure of the overvoltage protection circuit, in order for a power supply failure to cause both a failure of the RTS to trip the reactor and a failure of the EFAS to actuate EFS.

Reference 1.6 provided the Staff's response to CEN-349. It stated that ANO 2, SONGS 2 & 3, and WSES 3 did not satisfy the ATWS rule requirement for EFAS diversity because the bistable relays and matrix relays in the EFAS are identical to their counterparts in the RTS. In addition, the power supplies in the EFAS and RTS are not independent. Reference 1.5 concluded that either:

(1) diversity and independence must be provided in the areas where they are lacking, or

(2) an exemption from the ATWS rule must be requested in accordance with the provisions of 10CFR50.12

Reference 1.6 also provided guidance regarding the information which should be provided to support an exemption. This is summarized in subsection 1.3.2 of this submittal.

1.3 CRITERIA FOR EXEMPTION

1.3.1 10CFR50.12 Requirements

Title 10 of the Code of Federal Regulations Section 50.12 (10CFR50.12) states:

"(a) The Commission may, upon application by any interested person or upon its own initiative, grant exemptions from the requirements of the regulations of this part which are -

(1) Authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security.

(2) The Commission will not consider granting exemptions unless special circumstances are present."

10CFR50.12 list several categories of special circumstances. The ATWS Rule requirement for a diverse EFAS falls into special circumstances (ii) which is present whenever:

"(ii) Application of the regulation in the particular circumstances would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule."

1.3.2 NRC Staff Guidance

As stated earlier, the NRC provided guidance in Reference 1.6 for requesting exemption from the ATWS rule requirement for a diverse EFAS. This guidance has been interpreted as what the staff views as an adequate exemption request must demonstrate to satisfy special circumstance category (ii) in 10CFR50.12. The Staff's guidance is as follows:

"(1) The main rationale for using identical components in the case of the bistable relays and the matrix relays appears to be the specialized nature of the existing C-E plant protection system design requirements. It is stated that replacement of some of the existing relays with a diverse counterpart is not "reasonable or practicable." Neither CEN-315 nor CEN-349 provide sufficient information to support this claim (neither does CEN-315 nor CEN-349 provide specific information demonstrating that it is not reasonable or practicable to install a totally new, separate, independent, and diverse EFW actuation system that would avoid this "specialized" problem). The justification for not providing diversity and independence in this area must include either the prohibitive costs of adding such a system (for the safety benefit gained), or the competing risks (i.e., the increase in risk due to the addition of the new system), or both.

(2) As noted by the Rule and the ACRS and cited in CEN-315, significant emphasis should be placed on the preventive aspects, e.g., the diverse scram system.

Justification to support an argument for the use of some identical components in both the existing scram system and the emergency feedwater system and its design and operational features, that demonstrates it is an extremely reliable, preventive system and that it is totally diverse and independent from the existing RTS. (Note: This may require installing a diverse scram system which goes significantly beyond the minimum requirements specified for this system in the rule.) Include a discussion of the reliability assurance and maintenance and surveillance programs planned for the diverse scram system to ensure that it remains a highly reliable operable system throughout the life of the plant.

(3) Although the Rule specifically requires that the emergency feedwater actuation be diverse and independent from the existing reactor trip system (emphasis added), there is some potential benefit to having an emergency feedwater actuation system diverse and independent from the new (diverse) scram system. Provide a detailed discussion of the diversity and independence provided between these two functions.

(4) Part 2 of the ATWS mitigating feature is the turbine trip function. Provide a discussion of the turbine trip function and its design and operational features which demonstrate that it is an extremely reliable mitigative feature and that it is diverse and independent from the reactor trip function (either the existing reactor trip system or the diverse scram system or both)."

1.4 OVERVIEW OF THE BASIS FOR EXEMPTION

AP&L, SCE, and LP&L believe that the underlying risk reduction purpose of the ATWS rule can be achieved at their respective C-E designed plants by installing a reliable DSS with an inherently diverse Turbine Trip (TT). Additionally, the existing EFAS need not be modified or supplemented to achieve the intent of 10CFR50.62.

In accordance with the NRC Staff's guidance, this submittal will demonstrate that an exemption from the requirement for an EFAS which is diverse and independent from the existing RTS is justified for the following reasons:

1. It is neither reasonable nor practicable to comply with the ATWS rule requirement for an EFAS that is diverse and independent from the RTS because:

   (a) The cost of replacing the existing EFAS with a totally new, independent, and diverse EFAS is estimated to be approximately $3,200,000 per reactor. This would provide an incremental reduction of the ATWS risk of 9×10^{-7} severe ATWS event per reactor year, with a value of $270,000 per reactor (assuming that the remaining life of the plant is 30 years). The DSS and TT, on the other hand, provide a reduction in risk of about 5.3×10^{-5}. Thus, once the DSS with its inherent diverse TT is installed, the cost of replacing the existing EFAS with a new diverse and independent EFAS would far outweigh the value of the incremental decrease in ATWS risk.

   (b) It is neither reasonable nor practicable to replace the existing EFAS bistable and matrix relays with diverse counterparts and make the existing EFAS power supplies independent of the RTS power supplies. Due to the specialized nature of the PPS in ANO 2, SONGS 2 & 3, and WSES 3, diverse replacement bistable relays and matrix relays would have to be custom designed and custom built to fit within rigid physical and functional constraints and qualified for use in a Class 1E safety system. In order to install independent EFAS power supplies, additional station batteries with the associated equipment would have to be installed or the equipment would need to be powered from an existing source using qualified isolators. In addition to the actual hardware, the cost of maintenance, surveillance, and replacement over the life of the plant must also be considered.

This approach has been evaluated by the NSSS vendor and is not considered a viable solution. Although a precise cost estimate has not been determined, a conservative estimate of one-quarter of the cost of replacing the EFAS has been placed on this approach. This would put the cost at approximately $800,000 per unit. Based on the evaluation performed by the NRC in SECY-83-293, the value/impact ratio of this modification is comparable to other alternatives which were deemed by the NRC as not cost beneficial in achieving the underlying purpose of the ATWS Rule. However, it is probable that the cost will be much higher than the conservative estimate of $800,000 per unit. This is due to the fact that, in addition to the initial effort associated with designing diverse equipment, there are costs associated with the qualification of this equipment. Also, given the physical constraints of the existing equipment, significant hardware and complex wiring modifications would be required to accommodate the new equipment. The initial design effort is a relatively small part of a plant modification of this nature. A large part of the cost is associated with the qualification, installation, testing, and maintenance of the new equipment. The incremental reduction in ATWS risk associated with these changes would be 9.0×10^{-7} severe ATWS event per reactor year, with an estimated value of $270,000 over the remaining life of the plant, which is estimated to be 30 years. Thus, once the DSS with its inherent diverse TT is installed, the cost to install diverse bistable and matrix relays and independent power supplies in the EFAS is comparable to the alternatives previously discounted by the NRC as a non-cost/effective means of decreasing the ATWS risk.

(c) Installation of a new system (in addition to the existing EFAS) to initiate EFW under conditions indicative of an ATWS would also not be a cost beneficial way of reducing the ATWS risk. The EFAS system in ANO 2, SONGS 2 & 3, and WSES 3 includes logic that initiates EFW following a steam generator low level (SGLL) condition. In addition, the logic identifies a steam generator as being ruptured based on the pressures in the steam generators and locks out EFW to a ruptured steam generator. The conditions that are indicative of an ATWS (i.e., high pressurizer pressure, SGLL, and high pressurizer level) can also be indicative of some secondary system pipe breaks. Therefore, the new system would have to include logic to identify and lock out EFW flow to the ruptured steam generator. Also, since the new system would be using its logic to initiate and isolate EFW in parallel with the existing EFAS, measures would have to be taken to assure that the new system and the existing system were not providing contradictory signals (e.g., one system providing a signal to actuate while the other system was providing a signal to isolate. Since the existing EFAS is a four channel Class 1E system, the new system would have to be a Class 1E system with four channels. Thus, the new system would be as expensive as the totally new, independent, and diverse EFAS discussed in item 1(a). As discussed in item 1(b), the cost of such a system far outweighs the benefits.

2. The DSS designs that will be installed at ANO 2, SONGS 2 & 3, and WSES 3 will be extremely reliable, preventive systems. The DSS reliability assurance, maintenance, and surveillance programs will enhance the DSS reliability over the life of the plant.

3. The EFAS diversity and independence from the DSS will provide protection against a common mode failure that prevents the reactor from tripping and the EFW from actuating under

conditions indicative of an ATWS.

4. Due to the nature of the existing turbine trip circuitry, the DSS will provide an inherently diverse TT function. This will be diverse and independent from the RTS and will trip the turbine under conditions indicative of an ATWS.

Section 2 discusses Items 1 through 4 in detail.

1.5 REFERENCES FOR SECTION 1

1.1 SECY-83-293, "Amendments to 10CFR50 Related to Anticipated Transients Without Scram (ATWS) Events", July 19, 1983.

1.2 NUREG 460, "Anticipated Transients Without Scram for Light Water Reactors", March 1980.

1.3 September 16, 1985 letter from R.W. Wells (CEOG) to Fauste Rosa (NRC), "CEN-315 Summary of the Diversity Between the Emergency Feedwater Actuation System for C-E Plants."

1.4 August 4, 1986 letter from D.M. Crutchfield (NRC) to R.W. Wells (CEOG), "NRC Staff Evaluation of CEN-315, Summary of the Diversity Between the Reactor Trip System and the Emergency Feedwater Actuation System."

1.5 December 30, 1986 letter from M.O. Medford (SCE) to G.W. Knighton (NRC), "CEN-349 Response to the NRC's Evaluation for CEN-315 for San Onofre Nuclear Generating Station Units 2 and 3, Arkansas Nuclear One Unit 2, and Waterford Steam Electric Station Unit 3."

1.6 Letter from G.W. Knighton (NRC) to K.P. Baskin (SCE) and J.C. Holcombe (SDG&E), "NRC Evaluation of CEN-315 and CEN-349."

2.0 DETAILED EVALUATION OF THE ATWS RULE REQUIREMENT FOR DIVERSE EFAS

2.1 INTRODUCTION

Potentially, there are three ways to satisfy the ATWS rule requirement for a diverse and independent EFAS. These are:

- Replacing the existing EFAS with a new system that is totally diverse, independent, and separate from the RTS, or
- Replacing the existing EFAS bistable relays and matrix relays with components that are diverse from their counterparts in the RTS and replacing the EFAS power supplies with equipment that is independent from the RTS power supplies, or
- Installing a new system, in addition to the existing EFAS, to initiate auxiliary feedwater under conditions indicative of an ATWS.

An evaluation of each of these options is presented in following sections.

2.2 EVALUATION OF REPLACING THE EXISTING EFAS WITH A TOTALLY NEW, DIVERSE, SEPARATE, AND INDEPENDENT EFAS

2.2.1 Overview and Description of EFAS

The ATWS rule requirement for a diverse and independent EFAS could be satisfied by removing the existing EFAS from the Plant Protection System (PPS) cabinet and replacing it with a new EFAS that is diverse and independent, and located in a separate cabinet.

Before evaluating this approach, it is appropriate to describe the emergency feedwater system (EFWS) and the EFAS logic. The EFWS and EFAS are complex safety related systems configured to meet design requirements that go beyond considerations of the ATWS rule. The EFAS for a C-E designed plant performs the following functions:

- Determines that flow from the Main Feedwater System (MFWS) to the steam generator(s) is insufficient based on low steam generator level,
- Identifies that a steam generator pressure boundary is ruptured and prevents EFW flow to the ruptured generator based on low steam generator pressure or on steam generator differential pressure,
- Starts the EFW pumps,
- Opens the valves necessary to provide a flow path to the intact steam generator(s).

Figures 2-1 through 2-3 depict the EFAS logic used at ANO 2, WSES 3, and SONGS 2 & 3, respectively.

Additionally, the EFAS interacts with the Main Steam Isolation System (MSIS) signal on a component level. To illustrate this interaction, postulate that a large non-isolable secondary pipe break were to occur in steam generator 1 (SG1). A MSIS would be generated when a low pressure condition occurred in either steam generator. Upon MSIS generation, output contacts from the MSIS actuation relays would close the Main Feedwater Isolation Valves (MFIV) and Main Steam Isolation Valves (MSIV) to both steam generators. As the event progresses, an EFAS-2 signal would be generated (note that an EFAS-1 signal would not be generated due to the low pressure condition in SG1). Output contacts from the EFAS relays would block, at the equipment level, the signal from the MSIS actuation relays contacts to close the MFIV associated with steam generator 2 (SG2). This would enable EFW to be delivered to SG2.

Replacing the existing EFAS would involve relocating the EFAS and the MSIS function in a new cabinet that is separate from the existing PPS. This would be required to retain the existing interaction of the EFAS-1, EFAS-2, and MSIS signals on the actuated component level. Figure 2-4 illustrates the integration of the new cabinet with the existing system. This modification would provide an EFAS that is diverse and independent from the RTS. Subsection 2.2.2 examines the impact (cost) of this modification. Subsection 2.2.3 discusses the value (benefit) of this modification. The value is based on an analysis using the same methodology that the NRC staff utilized in SECY-83-293. This calculation considers the effects of uncertainties in the probabilities that are calculation inputs. Subsection 2.2.4 presents a value/impact analysis.

2.2.2 Impact (Cost)

The approximate anticipated cost of installing a new diverse and independent system to replace the existing EFAS is $3,200,000. These costs are summarized in Table 2-1. The costs include the removal of the EFAS and MSIS functions from the existing PPS cabinet. The components that are removed would be replaced with equipment which is diverse from the RTS components and located in a new cabinet that is physically separate and independent from the existing RTS. The EFAS and MSIS actuation devices located in the existing auxiliary relay cabinet would remain unchanged. The costs include the engineering effort and required documentation, the raceway installation, hardware, the installation of the diverse EFAS, and account for construction, cost of capital and escalation to in-service dollars.

2.2.3 Value (Benefit)

The regulatory analysis for the ATWS Rule, which is described in Enclosures C and D of SECY-83-293 (Reference 2.1), used simplified event trees for estimating the severe ATWS frequency (P_{ATWS}) associated with two major types of ATWS events; turbine trip and non-turbine trip events. In order to evaluate the value associated with the plant modifications required by the ATWS Rule, the methodology used in the regulatory analysis to arrive at the final ATWS rule has been examined. The purpose of this evaluation was to establish the benefit of the ATWS Rule modifications as they relate to a cost/benefit analysis for performing the modifications while considering the NRC comments from meetings and telephone conversations concerning the risk reduction basis of the ATWS Rule. Reference 2.2 details this evaluation.

Based on the analysis performed in Reference 2.2 the following conclusions have been made:

o Installation of the DSS and the inherent DTT accounts for over 98% of the achievable risk reduction from a severe ATWS,

o Accounting for the uncertainties does not change the conclusion that installation of the DSS and the inherent DTT accounts for over 98% of the achievable risk reduction from a severe ATWS,

o The installation of a diverse EFAS accounts for less than 2% of the achievable risk reduction, and

o The value of installing a diverse EFAS to mitigate the consequences of a severe ATWS, based on the decrease in risk reduction is $270,000.

These results will be utilized in the following sections to evaluate the value and impact of installing a diverse EFAS.

2.2.4 Value/Impact Analysis

The Value/Impact Ratio (VIR) is defined as:

$$\text{VIR} = \frac{\text{Diverse EFAS Value in Dollars}}{\text{Diverse EFAS Impact in Dollars}} \qquad \text{(Eq. 2-1)}$$

Using the EFAS value computed in Reference 2.2, and the EFAS cost, of $\$3.2 \times 10^6$, Equation 2-1 becomes:

$$\text{VIR} = \frac{\$270{,}000}{\$3.2 \times 10^6} = 0.084 \qquad \text{(Eq. 2-2)}$$

It should be noted that the VIR computed for a diverse EFAS (0.084) is significantly less than the VIR computed by the NRC for extra safety valves (0.44). The NRC staff rejected a requirement for installation of extra safety valves in existing C-E plants because of the unfavorable VIR. Therefore, the incorporation of a diverse EFAS is not cost effective approach if the DSS with its inherently Diverse TT (DTT) is installed. As such,the installation of a new EFAS that is totally diverse, independent, and separate from the RTS would not serve the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

2.3 EVALUATION OF COMPLIANCE BY INSTALLING DIVERSE EFAS BISTABLE AND MATRIX RELAYS AND INDEPENDENT EFAS POWER SUPPLIES

2.3.1 Overview

The existing EFAS would satisfy the ATWS rule if the existing bistable relays and matrix relays were replaced with diverse components and the EFAS power supplies were replaced with independent components. This modification would provide an EFAS that is diverse and independent from the RTS. This section examines the modifications required to provide diversity within the existing Plant Protection System Cabinet.

2.3.2 Impact (Cost)

The first step in achieving diversity within the existing PPS cabinet is to eliminate shared circuitry. It is necessary to provide separate inputs and separate bistables for steam generator level and variable setpoint cards for steam generator pressure. The circuits would then be separate but not diverse. There are two different methods which can be used to provide the diversity. The first method would be to replace the components of the EFAS bistables and matrix relay cards with comparable components from a different vendor. This would achieve only the diversity of manufacturer. This approach has been assessed as inadequate by the NRC Staff to no reduce the risk of common mode failures. The second method would require diverse designs, i.e., operational principle, etc., for the bistable, the variable setpoint card, the bistable relay card and the matrix relay card. This would achieve a higher level of diversity which would acceptable in compliance with the rule. This approach would require a redesign of the existing PPS internal logic cards and involve complex wiring changes with provisions to prevent the interchange of RPS/EFAS components during the surveillance and maintenance of the components.

Due to the specialized nature of the PPS in ANO 2, SONGS 2 & 3, and WSES 3, the replacement of diverse bistable relays and matrix relays would require a custom design and manufacture to fit within rigid physical constraints and meet strict functional requirements. The existing components in the EFAS circuitry were designed and qualified to meet the stringent requirements of IEEE-279 and IEEE-384 at the time of their licensing and their installation in the plants. In order to replace these components a similar qualification program must be performed.

With regard to the independence of power supply within the existing PPS cabinet, each cabinet receives vital AC power from a separate bus. Within the cabinet various power supplies are used to convert the AC power to DC power. Achievement of diversity and independence of power supply within the existing PPS cabinet is constrained by the fact that there is only one source of vital AC power per channel. Modification of the PPS cabinet internal power distribution and physical layout in order to provide separate and independent RTS and EFAS functions would be extremely complex, if at all possible.

In summary, an evaluation and analysis of the potential solution to providing separate and diverse hardware for the RPS/EFAS major safety related electronic components within the PPS cabinet is not considered a viable means to meeting the literal interpretation of the ATWS rule. The bases for this conclusion are as follows:

1) The PPS was designed to meet the requirements of IEEE-279 and IEEE-384. If these requirements are to be met, then modification it may not be possible to satisfy these constraints.

2) The modification of the PPS cabinet to conform to literal compliance with the ATWS Rule is complex. Additionally, based on existing evaluations it may not be possible, and may not be beneficial to the goal of reducing failures in the RPS/EFAS Systems.

3) Although the installation of diverse components on the PPS cabinet may be possible and reduce the probability of Common Mode Failures as intended by the ATWS Rule, it may increase the probability of human error in the maintenance of the diverse equipment.

4) The addition of diverse, qualified components and sources of power supplies is not considered a viable solution to the ATWS rule.

The costs associated with the approach of providing diversity in the PPS cabinet include the following components:

- Design of diverse components,
- Qualification of the diverse components,
- Installation of the diverse components,
- Design of wiring changes to supply independent power supplies,
- Rewiring of existing power supplies to provide independence (if at all possible),
- Training of staff in the maintenance and operation of the new equipment,
- Changes to the maintenance documentation,
- Changes to the Technical Specifications,
- Potential changes to the Surveillance Requirements in the Technical Specifications due to the new equipment.

Since this approach has been evaluated by the NSSS vendor and is not considered a viable solution to compliance with the ATWS Rule, the cost of such a modification has not been precisely determined. However, assume that a conservative cost of the modifications was one-quarter of that of replacing the existing EFAS with a totally diverse and independent EFAS. This would put the estimated cost of providing diversity within the PPS at approximately $800,000.

2.3.3 Value (Benefit)

Using the NRC Staff's methodology, the effect on P_{ATWS} of replacing the existing EFAS bistable relays and matrix relays with diverse components and installing independent EFAS power supplies would be the same as replacing the existing EFAS with a new EFAS that is, totally diverse, independent, and separate from the RTS. Thus, the incremental ATWS risk reduction would be 9.0×10^{-7} severe ATWS events per reactor year, the same as calculated in Appendix A. The value, therefore, would be $270,000.

2.3.4 Value/Impact

The VIR would be (equation 2-1):

$$\text{VIR} = \frac{\text{Diverse EFAS Value in Dollars}}{\text{Diverse EFAS Impact in Dollars}}$$

Using one-quarter of the EFAS value computed in Reference 2.2, and the estimated conservative cost of providing diversity in the PPS cabinet, of $800,000, Equation 2-1 becomes:

$$\text{VIR} = \frac{\$270,000}{\$800,000} = 0.42 \qquad \text{(Eq. 2-3)}$$

It should be noted that this VIR (0.42) is virtually equivalent to the VIR computed by the NRC for extra safety valves (0.44). As was noted previously, the NRC staff rejected a requirement for installation of extra safety valves in existing [illegible] plants because of the unfavorable VIR. Therefore, using the same rationale as was used in the formulation of the ATWS Rule, replacement of the existing EFAS bistable relays and matrix relays with diverse replacements and installing independent power supplies is not considered a cost effective means of risk reduction from an ATWS if the DSS with its inherently diverse TT is installed. As such, the installation of diverse bistable and matrix relays and independent power supplies in the EFAS would not serve the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

2.4 EVALUATION OF COMPLIANCE BY INSTALLING A REDUNDANT EFAS THAT IS DIVERSE AND INDEPENDENT FROM THE RTS

Another potential approach for complying with the ATWS rule is the installation of a new system (in addition to the existing EFAS) to initiate EFW under conditions indicative of an ATWS. This section will examine two options for implementing this approach:

- Installing a redundant control grade EFAS
- Installing a redundant safety grade EFAS

The first option creates competing risks, while the second option has a highly unfavorable VIR and also imposed competing risks.

2.4.1 Installing a Redundant Control Grade EFAS

In previous discussions with the NRC , some Staff members suggested that it may be possible to install a relatively inexpensive system (e.g., a one or two channel control grade system) that uses simple logic to initiate EFW under conditions indicative of an ATWS. This would, however, impose competing risks.

As was discussed earlier, the EFW System and EFAS are complex safety related systems configured to meet design requirements that go beyond considerations of the ATWS rule. The EFAS monitors steam generator levels to determine if flow from the MFWS to the steam generators is sufficient to maintain adequate steam generator inventory. Steam generator inventory may, however, be insufficient as a result of a secondary side pipe break. The EFAS, therefore, monitors steam generator pressure and steam generator differential pressure to identify a rupture steam generator. If a low pressure (i.e., a pressure less than a fixed value) condition is detected in a steam generator, that steam generator is identified as ruptured. Similarly, if high differential steam generator pressure is detected, the steam generator with low pressure is identifies as ruptured.

EFW flow to a ruptured steam generator would impose two potential risks. First, during an excess heat removal by the secondary system event such as a main steam line break (MSLB), it could potentially increase the rate of heat removal and exacerbate the rapid cooldown of RCS. Second, it could potentially cause EFW to be diverted away from the intact steam generator where it might be needed to remove energy from the primary system. The EFAS logic, therefore, locks out EFW to a ruptured steam generator.

The conditions that are indicative of an ATWS (i.e., high pressurizer pressure, SGLL, and high pressurizer level) can also be indicative of some secondary system pipe breaks. During a large, non-isolable secondary pipe break, which is part of the plant design basis, both steam generators would blow down through the break and depressurize until a main steam isolation signal was generated on low steam generator pressure. In addition, the plant would be expected to trip on a valid signal, which, depending on the specifics of the transient, might be high pressurizer pressure, low steam generator level, low Departure form Nucleate Boiling (DNBR), or low pressurizer pressure. The main steam isolation valves would close, causing the intact steam generator to repressurize. The ruptured steam generator would continue to blow down through the break, and hence depressurize. In addition, a low level condition would certainly occur in the ruptured steam generator, and probably in the intact steam generator as well. As such, the Class 1E EFAS would be expected to generate a valid signal to block EFW flow to the ruptured steam generator, while the simple control grade EFAS would be expected to generate a contradictory signal to feed the ruptured steam generator. Therefore, the new system would also have to include logic to identify and lock out EFW flow to a ruptured steam generator.

Installation of a more complex control grade system, which incorporated logic to identify and lock out EFW flow to a ruptured steam generator, would also pose problems. Signals from the two EFASs (the existing safety grade system and the backfit of the control grade system) would have to be integrated at the component (e.g., pumps and valves) level. There are four options for integrating the signals from the two systems, (1) giving the signals from the two systems equal weight, (2) giving the signal from the control grade system preference, (3) giving the signal from the safety grade system preference, or (4) installing additional hardware with logic to differentiate between valid and faulty signals.

Some background information is useful for understanding the implications of each of these options. Even if the control grade EFAS were to incorporate logic to identify and block EFW flow to a ruptured steam generator, there are credible scenarios which could result the control grade system producing signal which contradict the safety grade EFAS signals. These scenarios would include (1) spurious failures of the control grade system, (2) failures of the control grade system due to a harsh containment environment during an inside containment high energy line break, or (3) different signal errors in the two systems.

The first option, giving equal weight to the signals from the safety grade and the control grade system, would be unacceptable. Whenever a low level condition occurs in a steam generator, the valves in the piping that provide a flow path for the EFW must be either open (if the steam generator associated with the valves is intact) or shut (if the steam generator associated with the valves is rupture). If these valves received signals to open from one EFAS and at the same time received contradictory signals to shut from the other EFAS, in the absence of logic to give one set of signals preference over the other, there would be no assurance of the valves assuming the correct position. This would be detrimental to plant safety.

Options (2) and (3) involve giving the signals from one EFAS preference over the signals from the other EFAS. If the control grade EFAS signals were preferred, however, this would be equivalent to replacing the safety grade EFAS with a control grade system. Giving the signals from the safety grade EFAS preference would defeat the purpose of installing the control grade EFAS. Thus, neither of these options in acceptable.

The fourth option involves implementing logic to differentiate between valid and faulty EFAS signals. If this logic were in a control grade system, it would allow the action of a control grade system to override the safety grade EFAS, which would not be acceptable. A safety grade system that would validate signals from the existing and supplemental EFASs would have to monitor steam generator level to identify when steam generator inventory was insufficient, and use steam generator differential pressure to differentiate between a ruptured and intact steam generator. This signal validation system would have to be as reliable as the existing the EFAS, because it would be capable of overriding the existing system. Hence, it would have to consist of at least three, and preferably four channels. Thus the signal validation system would have to be a complex safety grade system that duplicates most of the capabilities of the existing EFAS. As such, it would be as costly as the new, independent, and diverse EFAS which is discussed in Subsection 2.2. Subsection 2.2.4 demonstrates that the VIR of such a system is much less than one, indicating that its installation would not serve the underling purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner. In addition, a plant with two systems (one safety grade and one control grade) that serve identical functions, and a third system designed to validate the signals from the other two systems, might be susceptible to systems interactions that are difficult to analyzed and potentially detrimental to plant safety. Thus, the installation of a control grade EFAS to supplement the existing EFAS would impose competing risks and as such is not justified.

2.4.2 Installing a Redundant Safety Grade EFAS

To prevent a signal from the existing four channel Class 1E EFAS being overridden by a signal from a less reliable system, any EFAS that supplements the existing EFAS would have to be a class 1E system with four or more channels. Thus, the new system would be as expensive as the totally new, independent, and diverse EFAS discussed above in item Subsection 2.2. As was discussed in Subsection 2.2.4, the VIR of such a system is much less than 1, indicating that its installation would not serve the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

In addition, installation of a second safety grade EFAS would impose competing risks. If a second Class 1E EFAS were installed, it would be controlling the same hardware (i.e., pumps and valves) as the existing EFAS. This gives rise to the question, "How should the signals from the two systems be integrated on the hardware level?"

An underlying assumption of the ATWS Rule is that a common mode failure disabling a redundant safety grade system is a credible event. Suppose one of the EFAS correctly identified a steam generator as being intact and in need of EFW as indicated by a low level condition. It would send signals to a set of valves to open and thereby provide a EFW flow path to the steam generator. Due to a common mode failure, however, the other EFAS identified the same steam generator as ruptured and therefore sent contradictory signals to the same valves to close and block EFW flow to that steam generator. If the signals from both systems received equal preference, there would be no assurance of the valves actually opening as they should. If the signal from the existing EFAS were given preference, this would defeat the purpose of installing the second EFAS. If signals from the new EFAS were given preference, then there would be no point in retaining the existing system.

Thus, base on considerations of competing risks and VIR, installation of a new, redundant EFAS that is diverse and independent of the existing EFAS is not justified.

2.5 REFERENCES FOR SECTION 2

2.1 SECY-83-293, "Amendments to 10CFR50 Related to Anticipated Transients Without Scram (ATWS) Events", July 19, 1983.

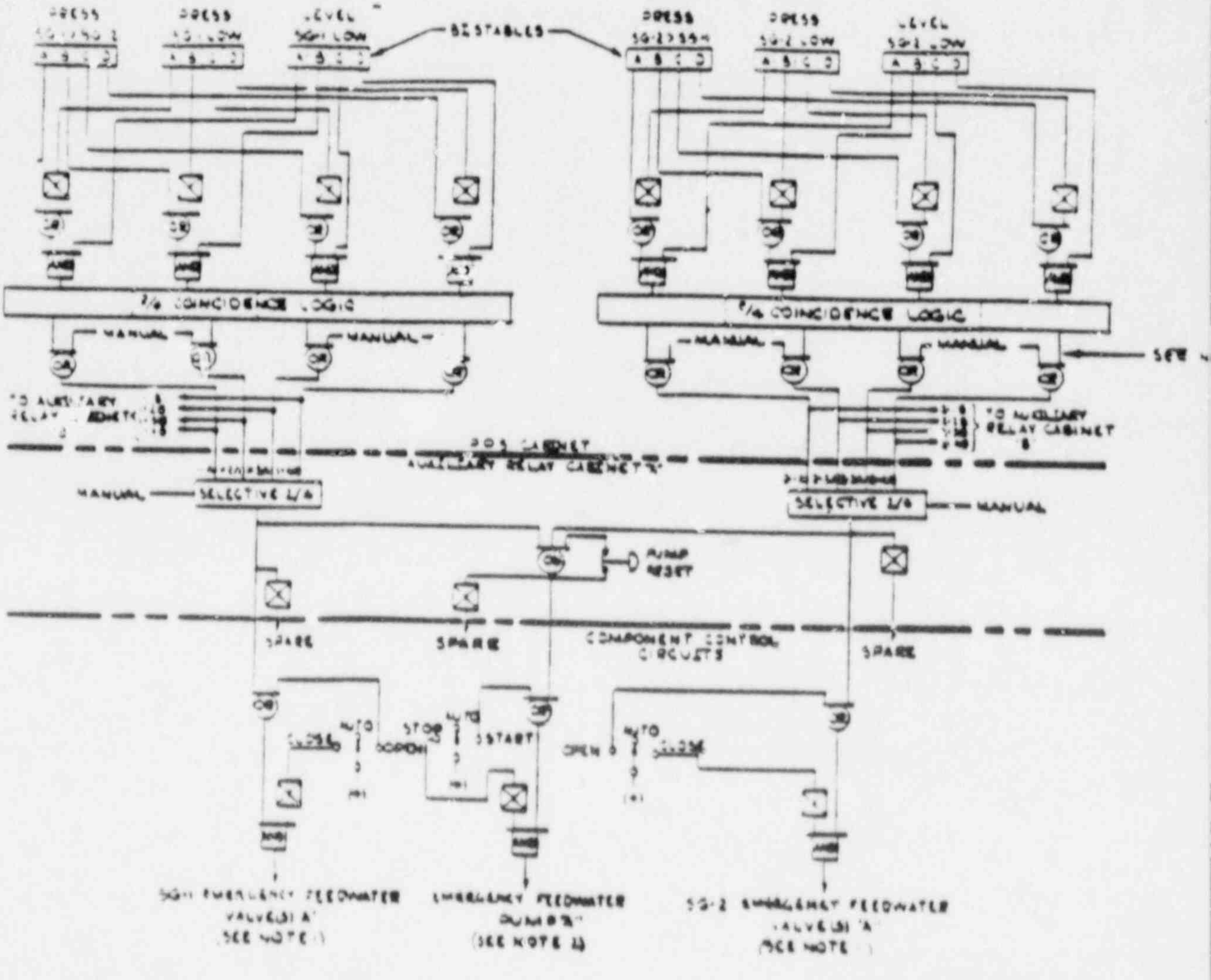
2.2 CEN-380, Supplement 1, "Evaluation of ATWS Risk Reduction to Support a Request for Exemption from 10CFR60.62 for Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3, and Waterford Steam Electric Station Unit 3," September, 1988.

TABLE 2-1
IMPACT (COST) TO IMPLEMENT NEW SAFETY GRADE DIVERSE EFAS

	COST
RACEWAY (CONDUIT AND CABLE) INSTALLATION	$ 200,000
HARDWARE AND INSTALLATION	2,125,000
ENGINEERING AND HOME OFFICE	325,000
CONSTRUCTION AND COST OF CAPITAL	325,000
ESCALATION TO IN-SERVICE DOLLARS	225,000
TOTAL CAPITAL COST (IN SERVICE DOLLARS)	$3,200,000

Figure 2-1

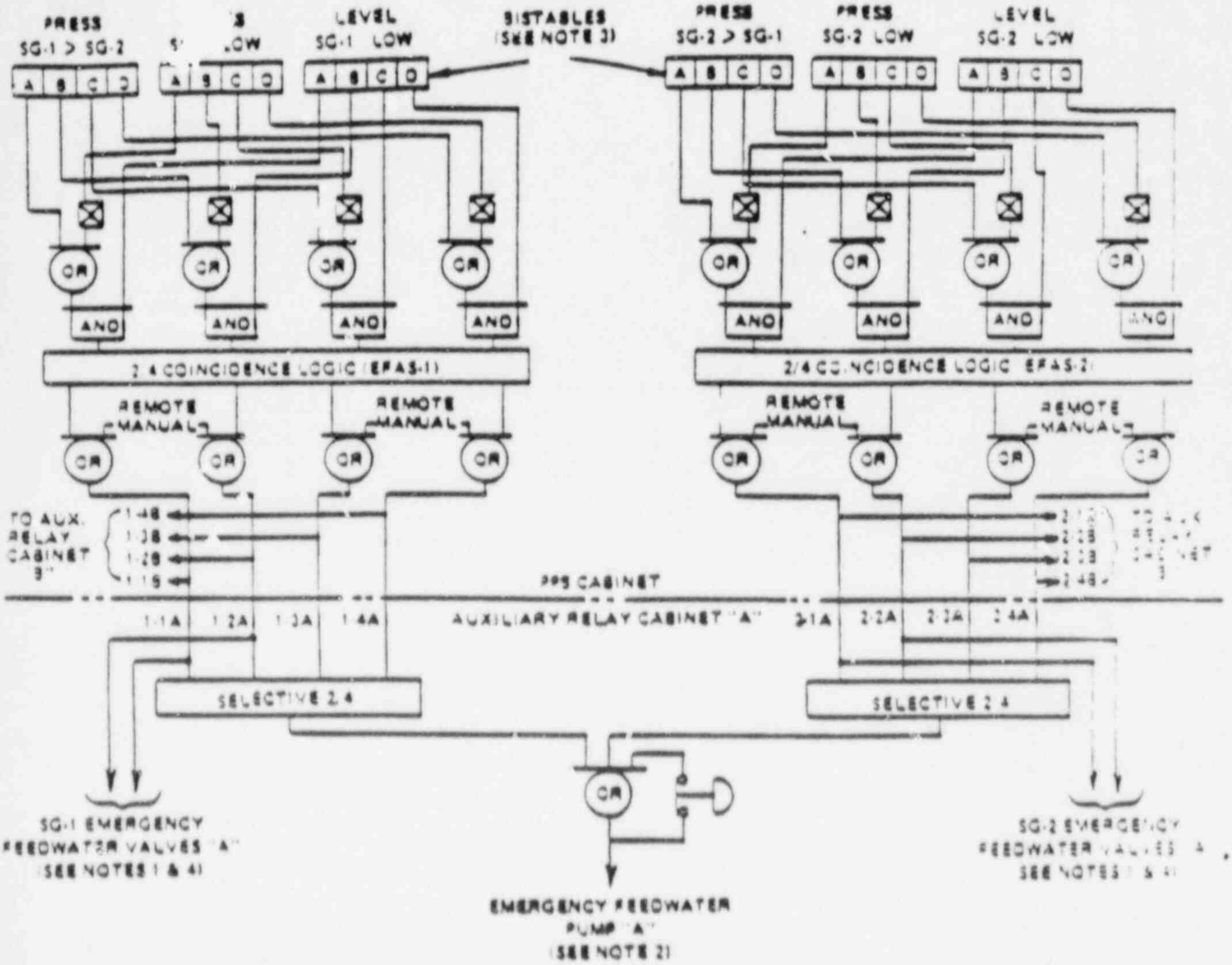
ANO 2 EFAS Logic Diagram



1 THESE MANUAL ACTUATIONS
ARE IN A REMOTE LOCATION,
E.G. CONTROL ROOM.
2 STARTS IF OUTPUT HIGH (H)
STOPS IF OUTPUT LOW (H)
3 OPEN IF OUTPUT HIGH (H)
CLOSES IF OUTPUT LOW (H)

Figure 2-2

SONGS 2 & 3 EFAS Logic Diagram



4. EMERGENCY FEEDWATER VALVES IN AUXILIARY RELAY CABINET "B" ARE ACTUATED BY OUTPUTS 1-3 & 4 AND 2-3 & 4

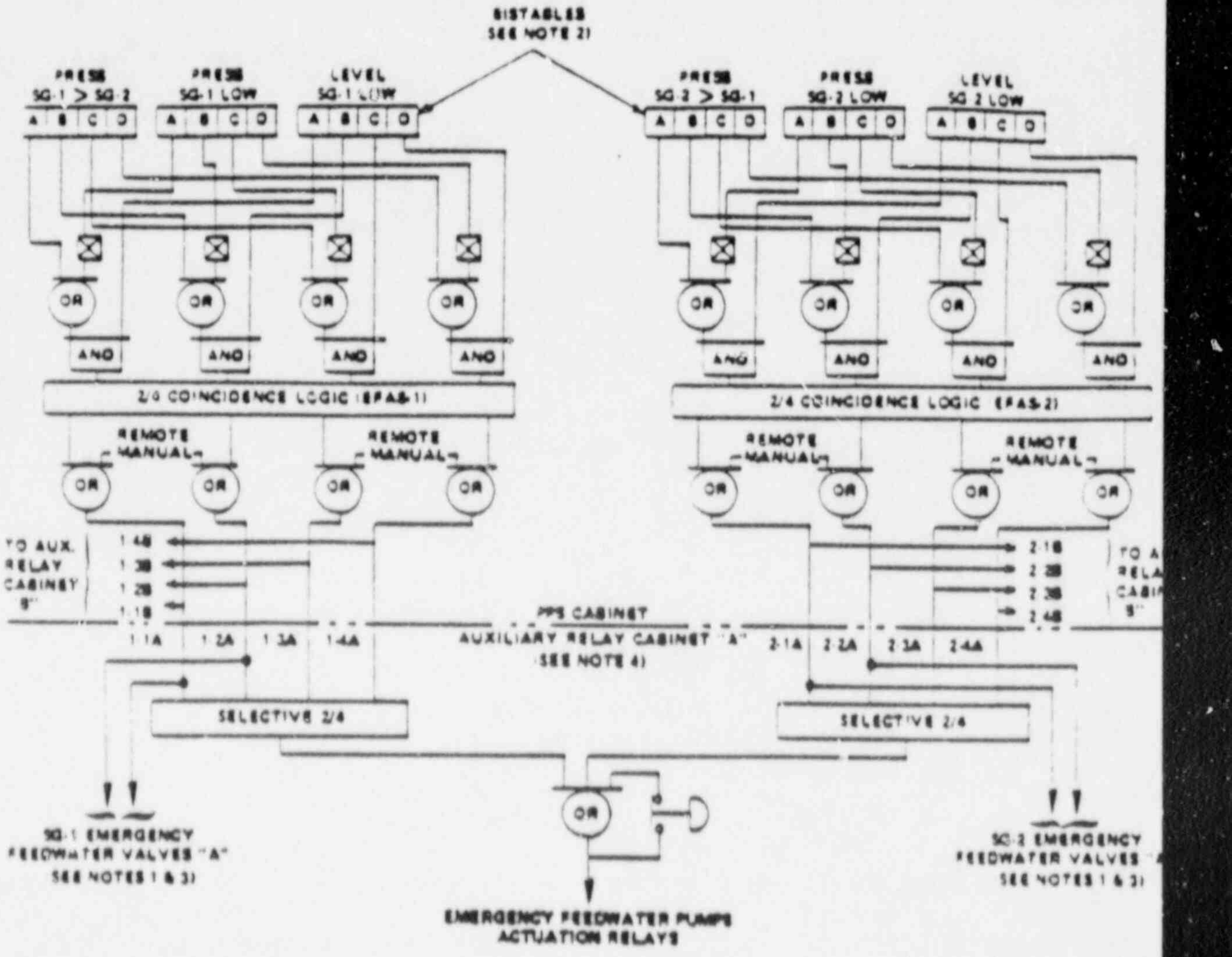
3. LOGIC OUTPUT IS 1 WHEN BISTABLE TRIPPED

2. STARTS IF OUTPUT HIGH (+)
STOPS IF OUTPUT LOW (-)

1. OPEN IF OUTPUT HIGH (+)
CLOSES IF OUTPUT LOW (-)

Figure 2-3

WSES 3 EFAS Logic Diagram

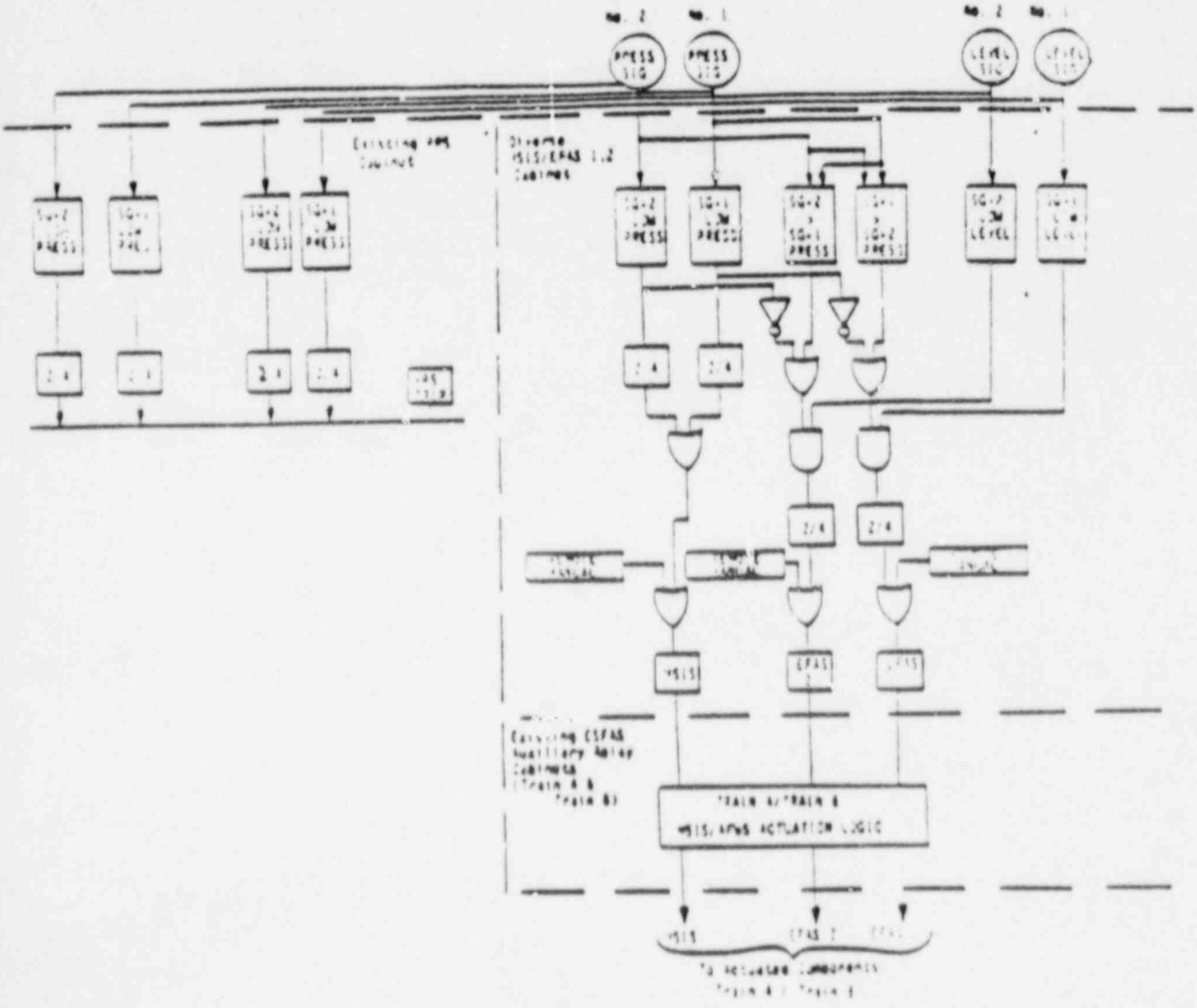


NOTES.

1. OPEN IF OUTPUT HIGH (+)
   CLOSES IF OUTPUT LOW (-)
2. LOGIC OUTPUT IS 1 WHEN BISTABLE TRIPPED
3. EMERGENCY FEEDWATER VALVES "B" IN AUXILIARY RELAY CABINET "B" ARE ACTUATED BY SSRS 3 & 4
4. AUXILIARY RELAY CABINET "B" IS IDENTICAL TO CABINET "A" EXCEPT AS STATED ABOVE

Figure 2-4

Integration of a New, Separate, Diverse, and Independent EFAS and MSIS with the existing PPS



3.0 DIVERSE SCRAM SYSTEM

3.1 OVERVIEW

The NRC analysis of the ATWS risk reduction due to the plant modifications associated with the installation of a DSS assumed a decrease in the RPS Electrical component of the risk from 2.0 x 10^{-5} to 2.0 x 10-6. This analysis assumed a DSS availability of 90%. The DSS designs which are proposed for WSES 3, SONGS 2 & 3, and ANO 2 are expected to exceed this availability goal. Therefore, the DSS designs which will be implemented will result in a greater decrease in ATWS risk than that which was considered by the NRC.

This Section will discuss the design detail of the Diverse Scram Systems which are under consideration by LP&L, SCE and AP&L. The discussion will concentrate on the aspects of the proposed DSS designs which conform to or exceed the requirements of the ATWS Rule and the NRC guidance of complying with the ATWS Rule.

3.2 WATERFORD STEAM ELECTRIC STATION UNIT 3 DSS DESIGN

3.2.1 General Description

The DSS for WSES 3 is designed to initiate a reactor trip for conditions indicative of an ATWS by monitoring pressurizer pressure.

Pressurizer pressure increases because of the imbalance between the energy added to the primary system by the core and the energy removed by the secondary system. The DSS will generate a signal when the pressure setpoint is reached. This signal interrupts the power supply that maintains the control rod position. Once the power field is arrested, the control rods drop into the core halting the reaction.

The WSES 3 DSS employs two parallel paths of circuitry, each consisting of a pressure sensor, a bistable, a bistable relay, and a trip relay. The pressure sensor is a Barton diaphragm-type sensor. The sensor monitors the system parameter (i.e. pressurizer pressure) and generates a signal. If the setpoint has been exceeded, the bistable switches indicating a trip. This trip signal is sent through the bistable relay to the trip relay. The bistable relay provides for the voltage change between the bistable and the trip relay. When the trip relay receives the signal, the electric field of the motor-generator (M-G) set is interrupted. This removes the power supply for the CEDMCS without requiring actuation of the reactor trip breakers. Once the power to the CEDMCS has been removed, a reactor scram occurs.

The operating status of the DSS will be provided to the control room operators through an ATWS display which will be incorporated into the Qualified Safety Parameter Display System (QSPDS). The QSPDS is "human factor" engineered to provide operators with clear, concise data from the inadequate core cooling instrumentation. As part of the QSPDS, the ATWS display will be quality controlled. The QSPDS will provide continuous monitoring via alarms to inform the operators when a high pressure state occurs. The ATWS display will be available to operators during both normal and abnormal conditions. Consequently its use as part of the QSPDS will be integrated into operator training. Additionally, the main control room annunciators will provide indication of a DSS trip or system bypass/trouble state. Locally (at the M-G sets), read and green lights will provide DSS trip indication and amber lights will indicate system bypass.

In summary, the DSS to be installed at WSES 3 will be diverse from the existing RTS and EFAS functions. As such the DSS will ensure the diversity between the EFAS and the new RTS (i.e., the current RTS and the DSS). This diversity will further reduce the chance that a CMF would prevent both a reactor trip and the actuation of emergency feedwater.

3.2.2 Conformance to NRC Guidance

Supplementary information (49FR26043, 26044) was provided with the Federal Register notification of the ATWS rule. This supplementary information includes guidance concerning the degree of diversity from the RTS which is required of the DSS and mitigating systems. The guidance states that equipment diversity to minimize the potential for CMF is required from the sensor output to and including the components used to interrupt control rod power for the DSS. Therefore, all DSS instrument channel components (excluding sensors and signal conditioning equipment upstream of the bistables) and logic channel components, and all DSS actuation devices must be diverse from the RTS in accordance with the published guidance. This includes establishing electrical independence from the existing RTS. The areas of guidance are as follows:

1) Safety Related (IEEE-279)
2) Redundancy
3) Diversity from the RTS
4) Electrical Independence from the existing RTS
5) Physical Separation from the existing RTS
6) Environmental Qualification
7) Seismic Qualification
8) Quality Assurance for Test, Maintenance, and Surveillance
9) Safety Related (1E) Power Supply
10) Testability at Power
11) Inadvertent Actuation

In these areas the NRC establishes the criteria for such things as diversity, testability, etc. for a DSS design that the NRC feels will comply with 10CFR50.62. These guidelines have been integrated into the design for the WSES 3 DSS as discussed below.

3.2.2.1 Safety Related

Staff Position - Not required but the implementation must be such that the existing protection system continues to meet all applicable safety related criteria.

Although not required to satisfy IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," the DSS designed for WSES 3 will use components which demonstrate high quality assurance. All of the components except for the power supply for the final actuation device and the final actuation device itself, will be safety class 1E. The final actuation device will be powered by a non-1E DC vital bus that is available during a loss of offsite power event.

In order to avoid jeopardizing the existing level of safety for the RTS, the design for the DSS is such that there is no interaction with the RTS. This is done by locating the equipment in separate cabinets on a different elevation. Additionally the DSS is electrically isolated from the RTS using qualified components. Physical and electrical isolation of the DSS from the RTS maintains the integrity of the RTS and, consequently does not invalidate the safety classification of the system.

3.2.2.2 Redundancy

Staff Position - Not Required

Redundancy alone does not preclude CMF occurrences. Consequently, no requirements are made on redundancy of the DSS. The design, however, is to be reliable, and should minimize the possibility for spurious action. As such, the WSES 3 DSS design employs two parallel paths based on a two out of two logic. This design feature will provide increased reliability and accuracy over that provided by a single channel system.

3.2.2.3 Diversity From the Existing Reactor Trip System

Staff Position - Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failures is required from the sensors to and including the components used to interrupt control rod power. Circuit breakers from different manufacturers alone is not sufficient to provide the required diversity for the interruption of control rod power. The sensors need not be of a diverse design or manufacturer. Existing protection system instrument-sensing lines may be used. Sensors and instrument - sensing lines should be selected such that adverse interactions with existing control systems.

In the guidance the NRC provides details how component diversity can be achieved. It states that diversity can be achieved by incorporating as many of the following methods as possible. Among these methods are:

- Use of components from different manufacturers
- Use of electro-mechanical devices versus electronic devices
- Use of energize versus de-energize-to-actuate trip status
- Use of AC versus DC power sources

The following subsections provide a discussion of the diversity between the existing RTS and the DSS on a component by component basis.

3.2.2.3.1 Sensors

The first component in the trip path for these systems are the sensors. The WSES 3 RTS and DSS share a common process card and power supply for the sensors. These are considered as part of the sensor and as such do not violate the overall diversity requirements. However, a certain level of diversity does exist between these sensors. The RTS sensor element uses a Rosemount capacitance capsule type sensor where the DSS employs a Barton diaphragm type sensor. This not only provides diversity of manufacturers but also of operational principle. The Rosemount sensor is a capacitor, two plates on either side of a di-electric, where a change in pressure results in a change in the capacitance of the system. The Barton sensor operates on a bellows principle where the deflection of the bellows caused by a change in pressure results in a change of tension across a strain gauge. The change in strain gauge resistance indicates the pressure change. The Barton sensors had no previous RTS control system function, and since diversity exists between the other elements of the DSS and RTS, interactions at the sensor level are minimized.

3.2.3.3.2 Bistables

The second component in the DSS is the NAL Bistable card. The bistable in the DSS is diverse from the RTS bistables in manufacturer (Westinghouse for the DSS versus Electro- Mechanics for the RTS and Gould for the CPCs). and power supply. The CPCs provide an auxiliary trip in the RTS on high pressurizer pressure using digital processing. The power supply for the DSS bistable card is a Westinghouse power supply which provides 26 VDC with a 24 VDC source as backup should the 26 VDC source fail. The RTS power supply is a Power Mate supply which provides 12 VDC. The CPC power supply is 16 VDC Lambda supply. Thus, the DSS NAL bistable card has nearly ideal diversity from the RTS and CPC auxiliary trip bistables.

3.2.3.3.3 Bistable Relay

The third component in the DSS circuitry is the NAI bistable relay card. Similar diversity exists between the bistable relays as did between the bistables. That is, they are diverse in manufacturer, design principle, and power supply. The DSS NAI bistable relay is designed by Westinghouse, is analog in design principle, and has a Westinghouse 26 VDC power supply with a 24 VDC backup source. The RTS bistable card is designed by Electro-Mechanics, is digital in design principle, and has a Power Mate 12 VDC power supply. The the DSS NAI bistable relay card has nearly ideal diversity from the RTS bistable relay.

3.2.3.3.4 Actuation Device

The final component of the DSS is a Potter Brumfield power relay which is powered by the non-1E vital bus. The parallel device for the RTS is not a relay and is powered by an 1E vital bus. Therefore, diversity is well established between these components.

However, there are other relays in the RTS circuitry. With the exception of one, all of the RTS relays are diverse from the DSS Potter Brumfield power relay in manufacturer. The exception is a Potter Brumfield rotary relay. The DSS and the RTS Potter Brumfield relays, however, have different design specifications and operate on different principles. The coil for the DSS Potter Brumfield relay is oriented such that when energized and de-energized, the relay toggles. The coils for the Potter Brumfield rotary relay in the RTS are shaped in two semicircles. When energized and de-energized, these coils spin the relay rather than toggle it. No other relay in the RTS operates on this exact same toggle mechanism. Therefore, diversity in operational principle exists.

Diversity in power supply for these relays also exists. The DSS relay receives power from a 125 VDC vital bus. The RTS relays, including the Potter Brumfield rotary relay, receive power either from a 120 VAC vital bus or a 12 VDC Power Mate power supply.

Although there is a common manufacturer for one of the RTS relays and the DSS relay, no other similarities exist. Therefore, sufficient diversity is established for the actuation device in the DSS to meet requirements.

3.2.2.4 Electrical Independence From the Existing Reactor Trip System

Staff Position - Required from sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits.

As stated above, the power supplies for the non-safety related circuits of the DSS are to be electrically isolated from the safety related circuits of the RTS. This will be accomplished by a series of circuit breakers and fuses , all of which are qualified as 1E. This pre [illegible] the possibility of a failure of the power supply to affect the [illegible]ion of the other power supplies. Electrical independence is therefore established.

The RTS and the DSS are designed such that a CMF producing an overvoltage or an undervoltage condition will not compromise both the RTS and ATWS prevention/mitigation functions. During an undervoltage occurrence, an alarm is generated if the voltage on the AC vital bus drops to between 115 and 116 volts. Since the Westinghouse power supplies are operable down to 112 volts, the operation of the NAL card and NAI card are assured during a time of undervoltage conditions of which the operator has no knowledge. Likewise, the Potter Brumfield will remain operable down to 75% of its rated input voltage. This is long after an undervoltage alarm would have occurred. Therefore, the ATWS circuitry will provide continuous protection during an undetected undervoltage occurrence.

During an overvoltage occurrence, a regulator on the output of the RTS power supplies maintains a steady supply to the components. Should an overvoltage state continue to worsen, the operator is notified by an alarm when the input voltage to the power supplies reaches a setpoint between 129 and 130 volts. Likewise if the output voltage of the Power Mate supplies increases to 14 volts (note that the RTS components are still operable at this voltage), the power supply overvoltage protection device automatically drops the output voltage to zero. When any of the two auctioneered power supplies in a channel drop to zero, a reactor trip will be generated. Therefore, the ATWS circuitry will provide continuous protection during an overvoltage occurrence.

3.2.2.5 Physical Separation From the Existing Reactor Trip System

Staff Position - Not required, unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated.

Although not required, physical separation from the existing RTS is provided for the DSS. Separate cabinets will house the electronics associated with the DSS. This equipment will be located on the +21 MSL elevation. Similar equipment for the RTS is located on the +46 MSL elevation. This separation is considered sufficient to preclude the possibility of common cause failures.

3.2.2.6 Environmental Qualification

Staff Position - For anticipated operational occurrences only, not for accidents.

In Title 10 of the Code of Federal Regulations, Section 50.49(c), a mild environment as defined as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." All materials that operate as part of the DSS will, at a minimum, meet the qualification for a mild environment.

3.2.2.7 Seismic Qualification

Staff Position - Not required.

Although the NRC's equipment qualification guidance states that the DSS does not require seismic qualification, the DSS must not jeopardize the qualification of the existing RTS. The components of the DSS from the sensor output to the final actuation device will be removed from the RTS in separate cabinets. Therefore, the DSS will not violate the seismic qualification of the existing RTS.

3.2.2.8 Quality Assurance for Test, Maintenance, and Surveillance

Staff Position - The Commission has released a generic letter (85-06, April 16, 1986) in which is provided the explicit Quality Assurance (QA) guidance required by 10CFR50.[illegible]. While Appendix B is viewed as a useful reference in which to frame the staff's guidance for non-safety related ATWS equipment, it does not meet the intent of the ATWS QA program. The equipment encompassed by 10CFR50.62 is not required to be safety related; therefore, less stringent QA guidance is acceptable. This letter incorporates a lesser degree of stringency by eliminating requirements for involving parties outside the normal line organization and requirements for a formalized program and detailed record keeping for all quality practices.

LP&L has included in its Nuclear Operations Management Manual, a chapter that defines the quality program for non-safety related ATWS equipment. This non-Appendix B program addresses 10CFR50.62 and incorporates the guidance provided by Generic Letter 85-06.

Testing will be performed prior to installation and operation when appropriate to demonstrate the the non-safety ATWS equipment conforms to its design specifications. Additionally, the ATWS equipment will be periodically tested to ensure that the tested requirements are satisfied. The measuring and test equipment which will be used to determine the acceptability of work or process status will be controlled and calibrated or adjusted at specific intervals in accordance with reviewed and approved procedures.

Although the above program program is sufficient to support the reliability of the DSS, consideration was given to the inclusion of a DSS test requirement on the WSES 3 Technical Specifications. On February 6, 1987, the NRC published in the Federal Register (Volume 52, Number 25, Page 3788), an interim statement on the proposed Policy Statement on Technical Specification Improvements for Nuclear Power Reactors. In this statement, the NRC states that the Technical Specifications are to address only the structures, systems and components required to function or actuate during an accident or transient as described in Chapter 15 of the Final Safety Analysis Repo is not credited in the accident analysis and therefore can not be considered as part of the primary success path. As such, the incorporation of a DSS testing requirement into the WSES 3 Technical Specifications would be in direct contradiction to the NRC's Technical Specification Improvement Program and, therefore, will not occur.

3.2.2.9 Safety Related Power Supply

Staff Position - Not required, but must be capable of performing safety functions with loss of offsite power. Logic power must be from an instrument power supply independent from the power supplies for the existing reactor trip system. Existing RTS sensor and instrument channel power supplies may be used provided the possibility of common mode failure is prevented.

The RTS is composed of four channels A,B,C, and D. Each channel possess circuitry identical to the RTS circuitry. Channels A and C are powered from the "A" battery, and Channels B and D are powered from the "B" battery. The DSS will be composed of only two channels A and B. The 26 VDC power supplies will receive power from the "A" battery for Channel A of the DSS and from the "B" battery for Channel B of the DSS. These 26 VDC power supplies will all be 1E safety-related supplies. The 125 VDC vital bus in each channel will receive power from the "AB" battery. This will be a non-1E vital bus. However, all power supplies for the DSS including the 125 VDC vital buses, will be independent from the existing (as stated above), and will be functional during a loss of offsite power.

3.2.2.11 Testability at Power

Staff Position - Required

LP&L has made provisions in the design of the DSS to permit periodic testing of process equipment, bistable, and logic when the reactor is operating at power. The level of testing is comparable to present reactor protection system requirements. That is, a combination of simultaneous and overlapping tests of components and subsystems is performed to insure full system functional capability. Because the existing RTS is redundant and independent of the diverse scram system, the existing system will provide the trip functions during the periodic testing of the diverse system.

To test the DSS circuitry at power, the Potter Brumfield power relay is bypassed by an identical Potter Brumfield power relay placed in parallel. This bypassed state is indicated in the control room by an audible alarm and a bypass indication light on the local panel display. Once the power relay is bypassed, a test signal consistent with an ATWS occurrence is sent to the NAL card. A successful test will trip the power relay, switching a red light to a green light on the QSPDS. This designates actuation of the DSS circuitry and a main control room annunciator.

3.2.2.11 Inadvertent Actuation

Staff Position - The design should be such that the frequency of inadvertent reactor trip and challenges to other safety systems is minimized.

LP&L will employ a DSS that includes the use of two channels operating on a two out of two logic, reliable power supplies, and testing to support a satisfactory level of quality assurance features. These design features are considered by LP&L to be sufficient to minimize the frequency of inadvertent actuation and challenges to other safety systems.

3.2.3 Reliability Assurance, Maintenance, and Surveillance

3.2.3.1 Reliability Assurance Program

LP&L has included in its Nuclear Operations Management Manual, a chapter that defines the quality program for non-safety related ATWS equipment. This non-Appendix B program addresses 10CFR50.62 and incorporates the guidance provided by Generic Letter 85-06.

3.2.3.2 Maintenance Program

Testing will be performed prior to installation and operation when appropriate to demonstrate the the non-safety ATWS equipment conforms to its design specifications. Additionally, the ATWS equipment will be periodically tested to ensure that the tested requirements are satisfied. The measuring and test equipment which will be used to determine the acceptability of work or process status will be controlled and calibrated or adjusted at specific intervals in accordance with reviewed and approved procedures.

3.2.3.3 Surveillance Program

The ATWS equipment will be periodically tested to ensure that the tested requirements are satisfied.

3.2.4 Conclusion

The WSES 3 proposed DSS design is highly reliable. It has a very high level of diversity and is completely separate from and independent of the the RTS. Using the NRC's methodology and accounting for the effects of uncertainties, it has been demonstrated that the DSS with its diverse TT accounts for 98% of the ATWS risk reduction that could be obtained by installing all three systems required by the ATWS rule. Therefore, the installation of the DSS alone satisfies the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

3.3 SAN ONOFRE NUCLEAR GENERATING STATION UNITS 2 AND 3

3.3.1 General Description

SCE intends to implement the SONGS 2 & 3 DSS as a control grade system by utilizing four new pressurizer pressure transmitters to provide signals to the DSS in a two-out-of-four trip logic. The transmitters will be isolated from the rest of the DSS which will be powered from a non-1E uninterruptable power supply (UPS). The components for the DSS actuation logic and means of interrupting power to the CEDMCS will be diverse from the existing RPS.

While a two channel system is adequate to meet the requirements of 10CFR50.62, SCE has elected to install a four channel system in order to:

- Enhance the reliability of overall plant operation,
- Reduce the potential for spurious trips,
- Reduce the potential for errors during operational testing.

The DSS design will use high pressurizer pressure as the parameter indicative of an ATWS. The trip setpoint will be greater than the RPS High Pressurizer Pressure Trip Setpoint (HPPTS) and less than the Primary Safety Valve (PSV) set pressure which is given in the Technical Specifications. The DSS HPPTS is greater than the existing RCS HPPTS permitted by the Technical Specifications in order to avoid unnecessary reactor scrams. The DSS HPPTS is less than the minimum PSV set pressure permitted by the Technical Specifications in order to prevent a delay in the generation of a trip signal caused by the opening of the PSVs.

The ATWS/DSS Main Signal Path consists of four measurement channels, four two-out-of-four logics and two trip paths. Each measurement channel consists of a pressure transmitter sensor, a signal conditioner, and an alarm block and a timer block which are part of the configured function block of a Foxboro Spec. 200 Micro control module.

Each of the four two-out-of-four logics, which is also a configured function block of the Foxboro Spec. 200 Micro Module, activates one of the two trip paths to open an M-G set output contactor. This occurs when any of the two of the four inputs from the four measurement channels reach the high-high pressurizer pressure setpoint simultaneously. Activation of channel 1 and/or 3 of the two-out-of-four logic energizes the trip path #1 relay which opens the M-G Set #1 output contactor, while activation of channel 2 and/or 4 of the two-out-of-four logic energizes the trip path #2 relay to open the M-G Set #2 output contactor.

Opening of the M-G Set #1 and #2 output contactors interrupts the three phase power to the CEDMCS and trips the reactor. Activation of both trip paths is required to initiate a reactor trip. Once the trip is actuated, it is sealed until manually reset at the DSS panel.

In summary, the DSS for SONGS 2 & 3 was designed to be a highly reliable system which meets or exceeds the requirements of 10CFR50.62. It provides the ATWS prevention features in terms of providing an alternate trip function on conditions which are indicative of an ATWS and minimizes the potential for common cause failure of the trip function by satisfying the diversity and independence requirements prescribed by the ATWS rule.

3.3.2 Conformance to NRC Guidance

Supplementary information (49FR26043, 26044) was provided with the Federal Register notification of the ATWS rule. This supplementary information includes guidance concerning the degree of diversity from the RTS which is required of the DSS and mitigating systems. The guidance states that equipment diversity to minimize the potential for CMF is required from the sensor output to and including the components used to interrupt control rod power for the DSS. Therefore, all DSS instrument channel components (excluding sensors and signal conditioning equipment upstream of the bistables) and logic channel components, and all DSS actuation devices must be diverse from the RTS in accordance with the published guidance. This includes establishing electrical independence from the existing RTS. The areas of guidance are as follows:

1) Safety Related (IEEE-279)
2) Redundancy
3) Diversity from the RTS
4) Electrical Independence from the existing RTS
5) Physical Separation from the existing RTS
6) Environmental Qualification
7) Seismic Qualification
8) Quality Assurance for Test, Maintenance, and Surveillance
9) Safety Related (1E) Power Supply
10) Testability at Power
11) Inadvertent Actuation

In these areas the NRC establishes the criteria for such things as diversity, testability, etc. for a DSS design that the feel will comply with 10CFR50.62. These guidelines are integrated into the design for the SONGS 2 & 3 DSS as discussed below.

3.3.2.1 Safety Related

Staff Position - Not required but the implementation must be such that the existing protection system continues to meet all applicable safety related criteria.

The DSS is a control grade system which utilizes safety related isolation. All existing Final Safety Analysis Report (FSAR) design criteria for associated circuits will be maintained as well as the reliability level for a two-out-of-four (with channel bypass) trip logic.

3.3.2.2 Redundancy

Staff Position - Not Required

Redundancy alone does not preclude CMF occurrences. Consequently, no requirements are made on redundancy of the DSS. The design, however, is to be reliable, and should minimize the possibility for spurious action. SCE has elected to install a four channel system to enhance the reliability of the overall plant operation by reducing the potential for spurious trips and reducing the potential for errors during operational testing. The potential of spurious trips is further reduced in the SONGS 2 & 3 DSS design by:

- The introduction of a timer circuit in the trip logic to filter out short duration transients,

- The use of energize to trip circuits to exclude the activation of a trip by component failures.

3.3.2.3 Diversity From the Existing Reactor Trip System

Staff Position - Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failures is required from the sensors to and including the components used to interrupt control rod power. Circuit breakers from different manufacturers alone is not sufficient to provide the required diversity for the interruption of control rod power. The sensors need not be of a diverse design or manufacturer. Existing protection system instrument-sensing lines may be used. Sensors and instrument - sensing lines should be selected such that adverse interactions with existing control systems.

In the guidance the NRC provides details how component diversity can be achieved. It states that diversity can be achieved by incorporating as many of the following methods as possible. Among these methods are:

- Use of components from different manufacturers
- Use of electro-mechanical devices versus electronic devices
- Use of energize versus deenergize-to-actuate trip status
- Use of AC versus DC power sources

The following subsections provide a discussion of the diversity between the existing RTS and the DSS on a component by component basis.

3.3.2.3.1 Sensors

Although not required by the ATWS rule, SCE will employ four capacitance detection pressure transmitters to provide signals to the four DSS channel inputs. These transmitters will be installed at approximately the 33 foot level around the outside wall of the biological shield. The sensing lines of these transmitters are connected to the existing pressurizer pressure sensing lines through instrument valves and share instrument lines with the existing RPS pressurizer pressure transmitter. The DSS transmitters are diverse from the existing RPS pressure transmitters in that the DSS transmitters are manufactured by Rosemount and the RPS transmitters are manufactured by Foxboro. Additionally the DSS transmitters are qualified for Class IE application and are Quality Class II and Seismic Category I in design.

The sensor design which is to be utilized in the SONGS 2 & 3 DSS is diverse from the existing RPS sensors and therefore, exceeds the requirements of 10CFR50.62.

3.3.3.3.2 Bistables and Bistable Relays

The SONGS 2 & 3 DSS does not specifically utilize bistable or bistable relay components in its design. The DSS trip path, following the sensor output, is a Foxboro Spec 200 Micro Control Module. The Foxboro Spec 200 Micro Control Module is a computer based control device which is configured to perform the following functions.

- Alarm Block - Compares the input signal with the setpoint to generate a local state 1 output to activate the timer.

- Timer Block - Receives input from the alarm block and generates a local state 1 output if the logic state 1 status persists for a period of 200 msec,

- Bistable Block - Provides channel trip status to indicating lights and to the Critical Function Monitoring System (CFMS) through the multiplexer when the timer block output changes to logic state 1,

- 2-out-of-4 Logic - Receives input from the timer output of each channel and generates a logic state 1 output when any two out of the four inputs are state 1.

The ATWS DSS receives power from two separate SCE non-IE UPS power panels. The logic power is supplied by four Foxboro power supplies each of which is modified for parallel operation with diodes for reverse voltage protection. The supplies are also modified to allow voltage monitoring prior to the diodes. The logic power supplies for channels 1 and 2 operate in parallel and the logic power supplies for channels 3 and 4 operate in parallel. Dual power supplies supply power to the multiplexer. This power supply is manufactured by Computer Products, Inc. Both of these power supplies have internally installed diodes and redundancy such the the output is parallel and diode shared. In addition, these power supplies have provisions for voltage monitoring prior to the diodes. A second dual ± 15 VDC power supply provides contact sense power to the CPI contact input cards. The RPS and CPCs utilize Power Mate 12 VDC power supplies which take power from the AC Vital Bus.

Given this configuration of the DSS Control Module, it is concluded that total diversity exists between the existing RPS bistable and

and bistable relay components, and the DSS. Diversity exists in design principle, manufacturer and power supply.

3.3.3.3.3 Actuation Device

The final components of the DSS are four Foxboro Model N-2AO-L2C-R trip contactor output relay modules and M-G Set trip Relays 14CR which are powered by the non-IE UPS power panels. The parallel device for the RTS is not a relay but rather a mechanical circuit breaker powered by an 1E vital bus. Therefore, diversity is well established between these components.

3.3.2.4 Electrical Independence From the Existing Reactor Trip System

Staff Position - Required from sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits.

The safety related sensors in the existing RTS will be isolated from the DSS using qualified isolators. All other DSS logic, actuation devices, etc. will be powered from a non-1E UPS from the Class 1E PPS power.

3.3.2.5 Physical Separation From the Existing Reactor Trip System

Staff Position - Not required, unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated.

Although not required, physical separation from the existing RTS is provided for the DSS. Separate cabinets will house the electronics associated with the DSS. This equipment will be located in the CEDMCS equipment room. This area was selected because it was outside the control room, it has air conditioning, it was close to the M-G sets and close to the penetration area, and it is a separate security zone that would reduce the possibility for tampering.

3.3.2.6 Environmental Qualification

Staff Position - For anticipated operational occurrences only, not for accidents.

In Title 10 of the Code of Federal Regulations, Section 50.49(c), a mild environment as defined as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." All materials that operate as part of the DSS will, at a minimum, meet the qualification for a mild environment.

3.3.2.7 Seismic Qualification

Staff Position - Not required.

Although the NRC's equipment qualification guidance states that the DSS does not require seismic qualification, the DSS is Seismic Category II. However the pressure transmitters are Seismic Category I design.

3.3.2.8 Quality Assurance for Test, Maintenance, and Surveillance

Staff Position - The Commission has released a generic letter

(85-06, April 16, 1986) in which is provided the explicit Quality Assurance (QA) guidance required by 10CFR50.62. While Appendix B is viewed as a useful reference in which to frame the staff's guidance for non-safety related ATWS equipment, it does not meet the intent of the ATWS QA program. The equipment encompassed by 10CFR50.62 is not required to be safety related; therefore, less stringent QA guidance is acceptable. This letter incorporates a lesser degree of stringency by eliminating requirements for involving parties outside the normal line organization and requirements for a formalized program and detailed record keeping for all quality practices.

SCE will incorporate into the SONGS 2 & 3 Updated FSAR a Quality Class III/ATWS. This Quality Class is defined as:

"Those structure, components and systems which are used to reduce the risk from an Anticipated Transient without Scram (ATWS), not in Quality Class I,II,III, or IV, whose failure could inconvenience normal plant operations shall be identified as Quality Class III/ATWS and shall be controlled in accordance with NRC Generic Letter 85-06. ... Those items designated as Quality Classes I, II, III,IV and III/ATWS make up the Project Q-List used in development, review, approval, and control of the design of major plant structures, components, and systems."

Testing will be performed prior to installation and operation when appropriate to demonstrate the the non-safety ATWS equipment conforms to its design specifications. Additionally, the ATWS equipment will be periodically tested to ensure that the tested requirements are satisfied. The measuring and test equipment which will be used to determine the acceptability of work or process status will be controlled and calibrated or adjusted at specific intervals in accordance with reviewed and approved procedures.

Although the above program program is sufficient to support the reliability of the DSS, consideration was given to the inclusion of a DSS test requirement on the SONGS 2 & 3 Technical Specifications. On February 6, 1987, the NRC published in the Federal Register (Volume 52, Number 25, Page 3788), an interim statement on the proposed Policy Statement on Technical Specification Improvements for Nuclear Power Reactors. In this statement, the NRC states that the Technical Specifications are to address only the structures, systems and components required to function or actuate during an accident or transient as described in Chapter 15 of the FSAR. The DSS clearly is not credited in the accident analysis and therefore can not be considered as part of the primary success path. As such, the incorporation of a DSS testing requirement into the SONGS 2 & 3 Technical Specifications would be in direct contradiction to the NRC's Technical Specification Improvement Program and, therefore, will not occur.

Therefore, the DSS will meet the guidance prescribed by the NRC for quality assurance for test, maintenance, and surveillance.

3.3.2.9 Safety Related Power Supply

Staff Position - Not required, but must be capable of performing safety functions with loss of offsite power. Logic power must be from an instrument power supply independent from the power supplies for the existing reactor trip system. Existing RTS sensor and instrument channel power supplies may be used provided the possibility of common mode failure is prevented.

Power to the DSS is from five different sources, namely, two Uninterruptable Power Supply (UPS) panels, the M-G sets control powers and the tie breaker control power. Separation between the class 1E tie breaker control circuitry and the non-Class 1E tie breaker status indicator circuitry is accomplished by Class 1E fuses. Therefore, the SCE DSS design interface satisfies the NRC guidance with regard to safety related power supplies.

3.3.2.11 Testability at Power

Staff Position - Required

SCE has made provisions in the design of the DSS to permit periodic testing of DSS equipment. On-line testing will be provided to allow functional testing of one selected channel at a time. Testing of the 2/4 logic matrix and final trip actuation will be done during plant shutdown or prior to startup.

3.3.2.11 Inadvertent Actuation

Staff Position - The design should be such that the frequency of inadvertent reactor trip and challenges to other safety systems is minimized.

SCE will employ a DSS that includes the use of four channels operating on a two- out- of-four logic, reliable power supplies, and testing to support a satisfactory level of quality assurance features. In addition to the logic design, the DSS also incorporates a timer block which will further reduce the possibility of inadvertent actuation.

These design features are considered by SCE to be sufficient to minimize the frequency of inadvertent actuation and challenges to other safety systems.

3.3.3 Reliability Assurance, Maintenance, and Surveillance

3.3.3.1 Reliability Assurance Program

The SONGS 2 & 3 DSS has been designed to be a reliable system. The combination of the Maintenance and Surveillance Programs outlined in the following sections ensure that the system will be reliable and perform the preventative function for which is was designed.

3.3.3.2 Maintenance Program

The DSS has been designed so that it can be tested on-line. The on-line tests which will be performed include periodic calibration and functional testing. This maintenance program will become part of the Station's surveillance program.

3.3.3.3 Surveillance Program

The DSS equipment will be periodically tested to ensure the equipment operability.

Although a formal surveillance program has not yet been established, it is anticipated that the following test program will be installed.

- Daily Channel Check
- Monthly Functional Test
- Calibration at Refueling Intervals

3.3.4 Conclusion

The SONGS 2 & 3 DSS design is highly reliable. It has a very high level of diversity and is completely separate from and independent of the the RTS. Additionally, although not required by 10CFR50.62, the SONGS 2 & 3 DSS design exceeds the ATWS rule requirements and guidance in that it incorporates four new diverse pressure transmitters to further increase the level of diversity of the DSS and further reduce the potential for common mode failure.

Using the NRC's methodology and accounting for the effects of uncertainties, it has been demonstrated that the DSS with its diverse TT accounts for 98% of the ATWS risk reduction that could be obtained by installing all three systems required by the ATWS rule. Therefore, the installation of the DSS alone satisfies the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

3.4 ARKANSAS NUCLEAR ONE UNIT 2

3.4.1 General Description

AP&L intends to implement the ANO 2 as a control grade system by utilizing new pressurizer pressure transmitters to provide signals to the DSS in a two-out-of-four trip logic. The safety related sensors will be isolated from the rest of the DSS which will be powered from a non-1E uninterruptable power supply (UPS). The components for the DSS actuation logic and means of interrupting power to the CEDMCS will be diverse from the existing RPS.

While a two channel system is adequate to meet the requirements of 10CFR50.62, AP&L has elected to install a four channel system in order to:

- Enhance the reliability of overall plant operation,
- Reduce the potential for spurious trips,
- Reduce the potential for errors during operational testing.

The DSS design will use high pressurizer pressure as the parameter indicative of an ATWS. The trip setpoint will be greater than the RPS High Pressurizer Pressure Trip Setpoint (HPPTS) and less than the Primary Safety Valve (PSV) set pressure which is given in the Technical Specifications. The DSS HPPTS is greater than the existing RCS HPPTS permitted by the Technical Specifications in order to avoid unnecessary reactor scrams. The DSS HPPTS is less than the minimum PSV set pressure permitted by the Technical Specifications in order to prevent a delay in the generation of a trip signal caused by the opening of the PSVs.

The ATWS/DSS Main Signal Path consists of four measurement channels, four two-out-of-four logics and two trip paths. Each measurement channel consists of a pressure transmitter sensor, a signal conditioner, and an alarm block and a timer block which are part of the configured function block of a Foxboro Spec. 200 Micro control module.

Each of the four two-out-of-four logics, which is also a configured function block of the Foxboro Spec. 200 Micro Module, activates one of the two trip paths to open an M-G set output contactor. this occurs when any of the two of the four inputs from the four measurement channels reach the high-high pressurizer pressure setpoint simultaneously. Activation of channel 1 and/or 3 of the two-out-of-four logic energizes the trip path #1 relay which opens the M-G Set #1 output contactor, while activation of channel 2 and/or 4 of the two-out-of-four logic energizes the trip path #2 relay to open the M-G Set #2 output contactor.

Opening of the M-G Set #1 and #2 output contactors interrupts the three phase power to the CEDMCS and trips the reactor. Activation of both trip paths is required to initiate a reactor trip. Once the trip is actuated, it is sealed until manually reset at the DSS panel.

In summary, the DSS for ANO 2 was designed to be a highly reliable system which meets or exceeds the requirements of 10CFR50.62. It provides the ATWS prevention features in terms of providing an alternate trip function on conditions which are indicative of an ATWS and minimizes the potential for common cause failure of the trip function by satisfying the diversity and independence requirements prescribed by the ATWS rule.

3.4.2 Conformance to NRC Guidance

Supplementary information (49FR26043, 26044) is provided with the Federal Register notification of the ATWS rule. This supplementary information includes guidance concerning the degree of diversity from the RTS which is required of the DSS and mitigating systems. The guidance states that equipment diversity to minimize the potential for CMF is required from the sensor output to and including the components used to interrupt control rod power for the DSS. Therefore, all DSS instrument channel components (excluding sensors and signal conditioning equipment upstream of the bistables) and logic channel components, and all DSS actuation devices must be diverse from the RTS in accordance with the published guidance. This includes establishing electrical independence from the existing RTS. The areas of guidance are as follows:

1) Safety Related (IEEE-279)
2) Redundancy
3) Diversity from the RTS
4) Electrical Independence from the existing RTS
5) Physical Separation from the existing RTS
6) Environmental Qualification
7) Seismic Qualification
8) Quality Assurance for Test, Maintenance, and Surveillance
9) Safety Related (1E) Power Supply
10) Testability at Power
11) Inadvertent Actuation

In these areas the NRC establishes the criteria for such things as diversity, testability, etc. for a DSS design that the feel will comply with 10CFR50.62. Though not formally required, these guidelines are integrated into the design for the ANO 2 DSS as discussed below.

3.4.2.1 Safety Rela .

Staff Position - Not required but the implementation must be such that the existing protection system continues to meet all applicable safety related criteria.

The DSS is a control grade system which utilizes safety related isolation. All existing FSAR design criteria for associated circuits will be maintained as well as the reliability level for a two-out-of-four (with channel bypass) trip logic.

3.4.2.2 Redundancy

Staff Position - Not Required

Redundancy alone does not preclude CMF occurrences. Consequently, no requirements are made on redundancy of the DSS. The design, however, is to be reliable, and should minimize the possibility for spurious action. AP&L has elected to install a four channel system to enhance the reliability of the overall plant operation by reducing the potential for spurious trips and reducing the potential for errors during operational testing. The potential of spurious trips is further reduced in the ANO 2 DSS design by:

- The introduction of a timer circuit in the trip logic to filter out short duration transients,
- The use of energize to trip circuits to exclude the activation of a trip by component failures.

3.4.2.3 Diversity From the Existing Reactor Trip System

Staff Position - Equipment diversity to the extent reasonable and

> practicable to minimize the potential for common cause failures is required from the sensors to and including the components used to interrupt control rod power. Circuit breakers from different manufacturers alone is not sufficient to provide the required diversity for the interruption of control rod power. The sensors need not be of a diverse design or manufacturer. Existing protection system instrument-sensing lines may be used. Sensors and instrument - sensing lines should be selected such that adverse interactions with existing control systems.

In the guidance the NRC provides details how component diversity can be achieved. It states that diversity can be achieved by incorporating as many of the following methods as possible. Among these methods are:

- Use of components from different manufacturers
- Use of electro-mechanical devices versus electronic devices
- Use of energize versus deenergize-to-actuate trip status
- Use of AC versus DC power sources

The following subsections provide a discussion of the diversity between the existing RTS and the DSS on a component by component basis.

3.4.2.3.1 Sensors

Although not required by the ATWS rule, the DSS for ANO 2 will employ four capacitance detection pressure transmitters to provide signals to the four DSS channel inputs. The sensing lines of these transmitters are connected to the existing pressurizer pressure sensing lines through instrument valves and share instrument lines with the existing RPS pressurizer pressure transmitter. The DSS transmitters are diverse from the existing RPS pressure transmitters in that the DSS transmitters are manufactured by Rosemount and the RPS transmitters are manufactured by Foxboro. Additionally the DSS transmitters are qualified for Class 1E application and are Quality Class II and Seismic Category I in design.

The sensor design which is to be utilized in the ANO 2 DSS is diverse from the existing RPS sensors and therefore, exceeds the requirements of 10CFR50.62.

3.4.3.3.2 Bistables and Bistable Relays

The ANO 2 DSS does not specifically utilize bistable or bistable relay components in its design. The DSS trip path, following the sensor output, is a Foxboro Spec 200 Micro Control Module. The Foxboro Spec 200 Micro Control Module is a computer based control device which is configured to perform the following functions.

- Alarm Block - Compares the input signal with the setpoint to generate a local state 1 output to activate the timer,

- Timer Block - Receives input from the alarm block and generates a local state 1 output if the logic state 1 status persists for a period of 200 msec,

- Bistable Block - Provides channel trip status to indicating lights and to the Critical Function Monitoring System (CFMS) through the multiplexer when the timer block output changes to logic state 1.

- 2-out-of-4 Logic - Receives input from the timer output of each channel and generates a logic state 1 output when any two out of the four inputs are state 1.

The ATWS DSS receives power from two separate ANO 2 non-IE UPS power panels. The logic power is supplied by four Foxboro power supplies each of which is modified for parallel operation with diodes for reverse voltage protection. The supplies are also modified to allow voltage monitoring prior to the diodes. The logic power supplies for channels 1 and 2 operate in parallel and the logic power supplies for channels 3 and 4 operate in parallel. Dual power supplies supply power to the multiplexer. This power supply is manufactured by Computer Products, Inc. Both of these power supplies have internally installed diodes and redundancy such the the output is parallel and diode shared. In addition, these power supplies have provisions for voltage monitoring prior to the diodes. A second dual ± 15 VDC power supply provides contact sense power to the CPI contact input cards. The RPS and CPCs utilize Power Mate 12 VDC power supplies which take power from the AC Vital Bus.

Given this configuration of the DSS Control Module, it is concluded that total diversity exists between the existing RPS bistable and and bistable relay components, and the DSS. Diversity exists in design principle, manufacturer and power supply.

3.4.3.3.3 Actuation Device

The final components of the DSS are four Foxboro Model N-2AO-L2C-R trip contactor output relay modules and M-G Set trip Relays 14CR which are powered by the non-IE UPS power panels. The parallel device for the RTS is not a relay but rather a mechanical circuit breaker powered by an 1E vital bus. Therefore, diversity is well established between these components.

3.4.2.4 Electrical Independence From the Existing Reactor Trip System

Staff Position - Required from sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits.

The safety related sensors in the existing RTS will be isolated from the DSS using qualified isolators. All other DSS logic, actuation devices, etc. will be powered from a non-1E UPS from the Class 1E PPS power.

3.4.2.5 Physical Separation From the Existing Reactor Trip System

Staff Position - Not required, unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated.

Although not required, physical separation from the existing RTS is provided for the DSS. Separate cabinets will house the electronics associated with the DSS. This equipment will be located in the CEDMCS equipment room. This area was selected because it was outside the control room, it has air conditioning, it was close to the M-G sets and close to the penetration area, and it is a separate security zone that would reduce the possibility for tampering.

3.4.2.6 Environmental Qualification

Staff Position - For anticipated operational occurrences only, not for accidents.

In Title 10 of the Code of Federal Regulations, Section 50.49(c), a mild environment as defined as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." All materials that operate as part of the DSS will, at a minimum, meet the qualification for a mild environment.

3.4.2.7 Seismic Qualification

Staff Position - Not required.

Although the NRC's equipment qualification guidance states that the DSS does not require seismic qualification, the DSS is Seismic Category II. However the pressure transmitters are Seismic Category I design.

3.4.2.8 Quality Assurance for Test, Maintenance, and Surveillance

Staff Position - The Commission has released a generic letter (85-05, April 16, 1986) in which is provided the explicit Quality Assurance (QA) guidance required by 10CFR50.62. While Appendix B is viewed as a useful reference in which to frame the staff's guidance for non-safety related ATWS equipment, it does not meet the intent of the ATWS QA program. The equipment encompassed by 10CFR50.62 is not required to be safety related; therefore, less stringent QA guidance is acceptable. This letter incorporates a lesser degree of stringency by eliminating requirements for involving parties outside the normal line organization and requirements for a formalized program and detailed record keeping for all quality practices.

Testing of the DSS will be performed prior to installation and operation when appropriate to demonstrate that the non-safety ATWS equipment conforms to its design specifications. Additionally, the ATWS equipment will be periodically tested to ensure that the tested requirements are satisfied. The measuring and test equipment which will be used to determine the acceptability of work or process status will be controlled and calibrated or adjusted at specific intervals in accordance with reviewed and approved procedures.

Although the above program is sufficient to support the reliability of the DSS, consideration was given to inclusion of the DSS test requirement in the ANO 2 Technical Specifications. On February 6, 1987, the NRC published in the Federal Register (Volume 52, Number 25, Page 3788), an interim statement on the proposed Policy Statement on Technical Specification Improvements for Nuclear Power Reactors. In this statement, the NRC states that the Technical Specifications are to address only the structures, systems, and components required to function or actuate during an accident or transient as described in Chapter 15 of the FSAR. The DSS clearly is not credited in the accident analysis and therefore, can not be considered as part of the primary success path. As such, the incorporation of a DSS testing requirement into the ANO 2 Technical Specifications would be in direct contradiction to the NRC's Technical Specification Improvement Program, and, therefore, will not occur.

3.4.2.9 Safety Related Power Supply

Staff Position - Not required, but must be capable of performing safety functions with loss of offsite power. Logic power must be from an instrument power supply independent from the power supplies for the existing reactor trip system. Existing RTS sensor and instrument channel power supplies may be used provided the possibility of common mode failure is prevented.

Power to the DSS is from five different sources, namely, two UPS panels, the M-G sets control powers and the tie breaker control power. Separation between the class 1E tie breaker control circuitry and the non-Class 1E tie breaker status indicator circuitry is accomplished by Class 1E fuses. Therefore, the ANO 2 DSS design interface satisfies the NRC guidance with regard to safety related power supplies.

3.4.2.11 Testability at Power

Staff Position - Required

AP&L has made provisions in the design of the DSS to permit periodic testing of DSS equipment. On-line testing will be provided to allow functional testing of one selected channel at a time. Testing of the 2/4 logic matrix and final trip actuation will be done during plant shutdown or prior to startup.

3.4.2.11 Inadvertent Actuation

Staff Position - The design should be such that the frequency of inadvertent reactor trip and challenges to other safety systems is minimized.

AP&L will employ a DSS that includes the use of four channels operating on a two-out-of-four logic, reliable power supplies, and testing to support a satisfactory level of quality assurance features. In addition to the logic design, the DSS also incorporates a timer block which will further reduce the possibility of inadvertent actuation.

These design features are considered by AP&L to be sufficient to minimize the frequency of inadvertent actuation and challenges to other safety systems.

3.4.3 Reliability Assurance, Maintenance, and Surveillance

3.4.3.1 Reliability Assurance Program

The ANO 2 DSS has been designed to be a reliable system. The combination of the Maintenance and Surveillance Programs outlined in the following sections ensure that the system will be reliable and perform the preventative function for which is was designed.

3.4.3.2 Maintenance Program

The DSS has been designed so that it can be tested on-line. The on-line tests which will be performed include periodic calibration and functional testing. This maintenance program will become part of the Station's surveillance program.

3.4.3.3 Surveillance Program

The DSS is not covered by the Technical Specifications. However, a surveillance program will be established by the Station to test the DSS ensure its operability. Although a formal surveillance program has not yet been established, it is anticipated that the following test program will be installed.

- Daily Channel Check
- Monthly Functional Test
- Calibration at Refueling Intervals

3.4.4 Conclusion

The ANO 2 DSS design is highly reliable. It has a very high level of diversity and is completely separate from and independent of the the RTS. Additionally, although not required by 10CFR50.62, the ANO 2 DSS exceeds the ATWS rule requirements and guidance in that it incorporates four new diverse pressure transmitters to further increase the level of diversity of the DSS and further reduce the potential for common mode failure.

Using the NRC's methodology and accounting for the effects of uncertainties, it has been demonstrated that the DSS with its diverse TT accounts for 98% of the ATWS risk reduction that could be obtained by installing all three systems required by the ATWS rule. Therefore, the installation of the DSS alone satisfies the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

4.0 DIVERSITY OF THE EXISTING EFAS FROM THE DSS

4.1 OVERVIEW

This section will provide a component by component comparison of the existing EFAS and the DSS for each plant design. References will be made to the details of the DSS component design which were presented in Section 3 of this report.

4.2 WATERFORD STEAM ELECTRIC STATION UNIT 3

As was previously described in Section 3.2 of this report, LP&L intends to utilize a control grade DSS for WSES 3. The DSS will utilize a two out of two logic and diverse type of sensor design. This section will describe the diversity between the DSS and the existing EFAS components.

4.2.1 Sensors

The first components in the EFAS circuitry are the sensors. The steam generator level sensors used by the EFAS are diverse from the DSS sensors in manufacturer and design principle. The DSS sensors are a Barton diaphragm type sensor. The EFAS sensors are capacitance proportional to level devices manufactured by Rosemount. Thus, the EFAS steam generator level sensors have nearly ideal diversity from the RTDs used by the RTS. The details of these sensor designs are provided in Section 3.2 of this report.

4.2.2 Bistables

The second components in the EFAS circuitry are the bistables. The EFAS bistables are diverse from the DSS bistables in manufacturer and power supply. The bistables used by the EFAS are analog devices manufactured by Electro-Mechanics (E-M). The DSS bistables are also analog devices. However, they are manufactured by Westinghouse and utilize a Westinghouse 26 VDC power supply with a 24 VDC backup source. The EFAS power supply is a Power Mate supply which provides 12 VDC. Thus, the EFAS steam generator level bistables have nearly ideal diversity from the DSS bistables.

4.2.3 Bistable Relays

The third components are the bistable relays. The bistable relays used by the EFAS are electro-mechanical devices manufactured by E-M. The DSS utilizes analog devices which are manufactured by Westinghouse. Like the bistables, the bistable relays are powered by a Westinghouse 26 VDC supply with a 24 VDC backup while the EFAS relays are powered from a Power Mate 12 VDC power supply. Therefore, given the differences in design principle, manufacturer and power supply, the bistable relays for the DSS and the EFAS have nearly ideal diversity.

4.2.4 Actuation Devices

That the final components are the actuation devices. The actuation devices used by the EFAS are electro-mechanical rotary relays with multiple contacts manufactured by Potter-Brumfield. The EFAS actuation devices are deenergize to trip status devices. The EFAS relays are powered by an IE vital buss. The DSS utilizes a Potter Brumfield power relay which differs in design principle, specification and power source from the EFAS actuation device. Although the EFAS and the DSS relays are manufactured by Potter Brumfield, they differ in power supply, voltage, current, DC resistance, and coil power. Also, the windings in the EFAS rotary relays have special coil lead routing and deck/contact arrangements. Consequently, substantial diversity exists between the DSS power relay and the EFAS relays.

4.2.5 Conclusions

The existing EFAS is totally diverse and separate from and independent of the DSS. This provides a very high degree of protection against a common mode failure that causes a failure of the reactor to scram and the auxiliary feedwater to actuate following an anticipated transient. As such, installation the DSS with its diverse TT meets or exceeds the underlying purpose and requirements of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

4.3 SAN ONOFRE NUCLEAR GENERATING STATION UNIT 2 AND 3

As was previously described in Section 3.3 of this report, SCE intends to implement a control grade DSS for SONGS 2 & 3. The DSS will utilize four new pressurizer pressure transmitters to provide signals to the DSS in a two out of four trip logic. This section will describe the diversity between the DSS and the existing EFAS components.

4.3.1 Sensors

The first components in the EFAS circuitry are the sensors. The steam generator level sensors which are used by the EFAS are forced balanced transducers manufactured by Foxboro, while the DSS employs four capacitance detection transmitters which are manufactured by Rosemount. The sensors design which is to be utilized in the SONGS 2 & 3 DSS is, therefore, diverse from the EFAS sensors. Since 10CFR50.62 does not require diversity in the sensors, the proposed DSS design exceeds the requirements of 10CFR50.62 with regard to diversity between the DSS and the EFAS.

4.3.2 Bistables and Bistable Relays

The next components are the bistables and bistable relays. The bistables used by the EFAS are analog devices manufactured by E-M. The DSS does not specifically use bistable or bistable relay components in its design. As was described in detail in Section 3.3.3.3.2, the DSS trip path following the sensor output is a Foxboro Spec 200 Micro Control Module. The Foxboro Spec 200 Micro Control Module is a computer based control device which is configured to alarm, pressure switch, timing, bistable switching functions, and logic functions.

Given this configuration of the DSS Control Module, it is concluded that total diversity exists between the existing EFAS bistable and bistable relay components and the DSS.

4.3.3 Actuation Devices

The final components are the actuation devices. The actuation devices used by the EFAS are electro-mechanical rotary relays with multiple contacts manufactured by Potter-Brumfield. The EFAS actuation devices are deenergize to trip status devices. The DSS utilizes four Foxboro Model N-2AO-L2C-R trip contactor output relay modules and Model 14CR M-G Set trip relays. Additionally there are differences in power supply, the DSS actuation devices are powered from the non-IE UPS power panels while the EFAS is powered by an IE vital bus.

4.3.4 Conclusions

The existing EFAS is totally diverse and separate from and independent of the DSS. This provides a very high degree of protection against a common mode failure that causes a failure of the reactor to scram and the auxiliary feedwater to actuate following an anticipated transient. As such, installation the DSS with its diverse TT achieves the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

4.4 ARKANSAS NUCLEAR ONE, UNIT 2

As was previously described in Section 3.4 of this report, AP&L intends to implement a control grade DSS for ANO 2. The DSS will employ four capacitance detection pressure transmitters to provide signals to the DSS in a two out of four trip logic. This section will describe the diversity between the DSS and the existing EFAS components.

4.4.1 Sensors

The first components in the EFAS circuitry are the sensors. The steam generator level sensors which are used by the EFAS are forced balanced transducers manufactured by Foxboro. while the DSS employs four capacitance detection transmitters which are manufactured by Rosemount. The sensors design which is to be utilized in the ANO 2 DSS is, therefore, diverse from the EFAS sensors. Since 10CFR50.62 does not require diversity in the sensors, the proposed DSS design exceeds the requirements of 10CFR50.62 with regard to diversity between the DSS and the EFAS.

4.4.2 Bistables and Bistable Relays

The next components in the circuitry are the bistables and bistable relays. The bistables used by the EFAS are analog devices manufactured by E-M. The DSS does not specifically use bistable or bistable relay components in its design. As was described in detail in Section 3.3.3.3.2, the DSS trip path following the sensor output is a Foxboro Spec 200 Micro Control Module. The Foxboro Spec 200 Micro Control Module is a computer based control device which is configured to alarm, pressure switch, timing, bistable switching functions, and logic functions.

Given this configuration of the DSS Control Module, it is concluded that total diversity exists between the existing EFAS bistable and bistable relay components and the DSS.

4.4.3 Actuation Devices

The final components are the actuation devices. The actuation devices used by the EFAS are electro-mechanical rotary relays with multiple contacts manufactured by Potter-Brumfield. The EFAS actuation devices are deenergize to trip status devices. The DSS utilizes four Foxboro Model N-2AO-L2C-R trip contactor output relay modules and Model 14CR M-G Set trip relays. Additionally there are differences in power supply, the DSS actuation devices are powered from the non-IE UPS power panels while the EFAS is powered by an IE vital bus.

4.4.4 Conclusions

The existing EFAS is totally diverse and separate from and independent of the DSS. This provides a very high degree of protection against a common mode failure that causes a failure of the reactor to scram and the auxiliary feedwater to actuate following an anticipated transient. As such, installation the DSS with its diverse TT achieves the underlying purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner.

5.0 DIVERSE TURBINE TRIP

The implementation of a DSS provides a diverse Turbine Trip (TT). The DSS will trip the reactor under conditions indicative of an ATWS. When the DSS causes a reactor scram, it also causes the turbine to trip because the DSS interrupts power to the Control Element Assembly (CEA) coils upstream of the rod power bus undervoltage relays in the Control Element Drive Mechanism Control System (CEDMCS). These relays actuate the turbine trip circuitry. If a DSS is implemented, the existing TT becomes a diverse TT due to the diversity between the DSS and the existing RTS. The dependence of the diverse TT upon DSS actuation means that the operating status of the DSS will reflect the operating status of the DTT, as well. Therefore the control room annunciators and other ATWS displays will similarly relay the information of the diverse TT status.

Thus, installation of the DSS will satisfy the 10CFR50.62 requirement that the plants will have equipment diverse from the RTS to automatically trip the turbine under conditions indicative of an ATWS. This is accomplished because the circuitry required to satisfy the component diversity requirements for a diverse reactor scram is essentially the same as for the DTT. Therefore, given the installation of a DSS, adequate diversity exists between the DTT and the RTS for compliance with 10CFR50.62.

6.0 SUMMARY AND CONCLUSIONS

6.1 SUMMARY

6.1.1 Purpose of 10CFR50.62

10CFR50.62 requires that ANO 2, SONGS 2 & 3, and WSES 3 have the following systems to supplement the existing RTS:

- Diverse Scram System independent from the existing RTS.
- Emergency Feedwater Actuation System diverse from the RTS.
- Turbine Trip diverse from the RTS.

Based on the Statement of Considerations for the Rule and statements of the NRC Staff in SECY-83-293, the underlying purpose of 10CFR50.62 is to reduce the probability of a severe ATWS event in a cost effective manner by reducing the probability of common mode failures in the reactor trip system, turbine trip system, and emergency feedwater actuation system.

6.1.2 NRC Staff's Interpretation of the ATWS Rule

Reports previously submitted to the NRC Staff have demonstrated that all of the components in the existing EFAS at ANO 2, SONGS 2 & 3, and WSES 3 except for the bistable relays and matrix relays are diverse from their components in the RTS. The design of the EFAS and RTS, however, provides considerable protection against common failures of the bistable relays or matrix relays disabling both systems.

Similarly, although the EFAS power supplies are not independent, their design is such that it would require the simultaneous occurrence of two different types of common mode failures (an overvoltage condition and failure of the overvoltage protection) affecting large number of these power supplies to prevent and reactor trip and the delivery of AFW to the steam generators.

The NRC Staff has completed their review of the submittals. The Staff has stated that ANO 2, SONGS 2 & 3, and WSES 3 do not presently satisfy the ATWS rule requirement for EFAS diversity because the bistable relays and matrix relays in the EFAS are identical to their counterparts in the RTS. In addition, the power supplies in the EFAS and RTS are not independent.

Based on this, the owners of the plants covered in this report conclude the Staff interprets the ATWS rule to require complete diversity of all EFAS components from their counterparts in the EFAS and complete independence of EFAS power supplies.

6.1.3 Why it is not Reasonable or Practicable to Comply with the NRC Staff's Interpretation of the ATWS Rule

It is not reasonable or practicable to comply with the NRC Staff's interpretation of the ATWS rule requirement for a system diverse and independent from the RTS to actuate emergency feedwater under conditions indicative of an ATWS. There are potentially three ways to comply with the Staff's interpretation.

o Replacing the existing EFAS with a totally new, independent, and diverse EFAS would cost $3,200,000 per reactor. This would not be cost beneficial, as it would provide an incremental reduction of the ATWS risk of 9×10^{-7} severe ATWS event per reactor year, with a value of $270,000 per reactor

- Replacing the existing EFAS bistable and matrix relays with diverse counterparts and make the existing EFAS power supplies independent of the RTS power supplies has been reviewed by the NSSS vendor and has been deemed not to be a viable alternative for compliance with the ATWS rule. This is due to complexity of the wiring changes required and the potential for human error in the maintenance of the new equipment. For each reactor, the cost to install diverse replacement bistable and matrix relays and independent EFAS power supplies has been conservatively estimated at one-quarter of the cost for installing a new EFAS system. This includes the costs of the qualification and installation, and maintenance of the replacement components. The incremental reduction in ATWS risk associated with these changes would be 9×10^{-7} severe ATWS event per reactor year, with an estimated value of $270,000 over the remaining life of the plant. Based on this conservative estimate of the cost of providing diversity within the PPS cabinet, and considering the criteria used by the NRC in their discounting of other hardware modifications to reduce the risk of ATWS, obtaining the required diversity within the PPS cabinet is not considered cost beneficial in reducing the incremental risk of an ATWS.

- Installing a new system (in addition to the existing EFAS) to initiate EFW under conditions indicative of an ATWS would also not be a cost beneficial way of reducing the ATWS risk. The EFAS is a four channel class 1E system includes logic which initiates EFW following a steam generator low level condition, identifies a steam generator as being ruptured based on the pressures in the steam generators and locks out EFW to a ruptured steam generator. The conditions that are indicative of an ATWS (i.e., high pressurizer pressure, SGLL, and high pressurizer level) can also be indicative of some secondary system pipe breaks. To assure that a signal from the existing

Class 1E EFAS was not over ridden by a contradictory signal from a control grade system, the supplemental EFAS would also have to be a four channel Class 1E system. Thus, the supplemental system would cost $3,200,000 per reactor, the same as the totally new, independent, and diverse EFAS. Again, this would not be cost beneficial.

Thus, none of the potential ways to comply with the NRC Staff's interpretation of the ATWS rule would not serve the underling purpose of 10CFR50.62 to reduce the ATWS risk in a cost effective manner. Virtually all of the ATWS risk reduction that could be obtained by compliance is obtained by installing the DSS with an inherently diverse TT. This has been demonstrated using the methodology and assumptions of the NRC's own regulatory analysis. Additionally, the effect of uncertainties were factored into the analysis.

6.1.4 Diverse Scram System

The DSS designs that will be installed at ANO 2, SONGS 2 & 3, and WSES 3 will be extremely reliable preventive systems. The DSS reliability assurance, maintenance, and surveillance programs will enhance the DSS reliability over the life of the plant.

6.1.5 Diversity of the Existing EFAS from the DSS

The EFAS diversity and independence from the DSS will provide protection against a common mode failure that prevents the reactor from tripping and the EFW from actuating under conditions indicative of an ATWS.

6.1.6 Diverse Turbine Trip

Due to the nature of the existing turbine trip circuitry, the DSS will provide an inherently diverse TT function. This will be diverse and independent from the RTS and will trip the turbine under conditions indicative of an ATWS.

6.2 EXEMPTION REQUEST

AP&L, SCE, and LP&L propose to implement a DSS with its inherently diverse turbine trip function at there respective reactors, ANO 2, SONGS 2 & 3, and WSES 3. The DSS will be independent from the existing RTS. Additionally, the EFAS is diverse from and independent of the DSS. The proposed course of action presents no risk to the public health and safety since the plant modifications proposed to satisfy the NRC Staff's interpretation of 10CFR50.62 all have a value/impact ratio substantially less than 1.0 and further plant hardware modifications provide an insignificant reduction in the ATWS risk.

As provided for by 10CFR50.12, AP&L, SCE, and LP&L hereby requests that the NRC grant an exemption for ANO 2, SONGS 2 & 3, and WSES 3 from the requirements of 10CFR50.62 for equipment diverse from the RTS to initiate the emergency feedwater system under conditions indicative of an ATWS.

CEOG COMBUSTION ENGINEERING OWNERS GROUP

CEN-380 SUPPLEMENT 1

EVALUATION OF
ATWS RULE 10 CFR 50.62
RISK REDUCTION
TO SUPPORT
REQUEST FOR EXEMPTION

FOR

ARKANSAS NUCLEAR ONE UNIT 2
SAN ONOFRE NUCLEAR GENERATING
STATION UNITS 2 AND 3
AND
WATERFORD STEAM ELECTRIC STATION
UNIT 3

PREPARED FOR THE

C-E OWNERS GROUP

SEPTEMBER, 1988

COMBUSTION ENGINEERING, INC.

CEN-380
Supplement 1

EVALUATION OF RISK REDUCTION
TO SUPPORT
A REQUEST FOR EXEMPTION
FROM ATWS RULE 10CFR50.62
FOR
ARKANSAS NUCLEAR ONE UNIT 2
SAN ONOFRE NUCLEAR GENERATING STATION UNITS 2 AND 3
AND
WATERFORD STEAM ELECTRIC STATION UNIT 3

SEPTEMBER, 1988

PREPARED BY

C-E POWER SYSTEMS
COMBUSTION ENGINEERING, INC.
WINDSOR, CT

ABSTRACT

This supplement to CEN-380 provides the analysis of the risk reduction associated with the installation of the hardware as required by the ATWS Rule, 10CFR50.62. The analysis was performed in support of an exemption request from a portion of 10CFR50.62 by the Arkansas Power and Light Company, the Southern California Edison Company, and Louisiana Power and Light for Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3, and Waterford Steam Electric System Unit 3, respectively. The analysis presented in this report reviews the basis of the risk reduction analysis performed by the NRC in the formulation of the 10CFR50.62 and provides the benefit which is derived from the equipment required by the 10CFR50.62.

LIST OF ABBREVIATIONS

AT	Anticipated Transient
ATWS	Anticipated Transient Without Scram
CD	Core Damage
C-E	Combustion Engineering, Inc.
DSS	Diverse Scram System
EFAS	Emergency Feedwater Actuation System
EFW	Emergency Feedwater
HPI	High Pressure Injection
MTC	Moderator Temperature Coefficient
NRC	Nuclear Regulatory Commission
P ATWS	Probabilty of a Severe Anticipated Transient Without Scram
RCS	Reactor Coolant System
RPS	Reactor Protection System
RTS	Reactor Trip System
TT	Turbine Trip

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

This supplement to CEN-380, Reference 1-1, will provide an evaluation of the risk reduction and value associated with the installation of the hardware modifications required by the ATWS rule, 10CFR50.62. The evaluation will examine the same probability estimates and event trees which were used in the NRC analysis on which the ATWS Rule was based.

1.1 REFERENCES FOR SECTION 1.0

1.1 CEN-380, "ATWS Rule 10CFR50.62, Request for Exemption for Arkansas Nuclear One Unit 2, San Onofre Nuclear Generating Station Units 2 and 3, and Waterford Steam Electric Station Unit 3," September, 1988.

2.0 EVALUATION OF RISK REDUCTION

The regulatory analysis for the ATWS Rule, as described in Enclosures C and D of SECY-83-293 (Reference 2.1), used simplified event trees for estimating the severe ATWS frequency (P_{ATWS}). Two major types of ATWS events were considered in this regulatory analysis; turbine trip and non-turbine trip events. Figures 2-1 and 2-2 present the event trees for the base cases for these transients. These base cases assumed that only existing plant systems were available during the ATWS event. In the event trees, P_{ATWS} is the sum of the frequencies associated with each branch of an event tree which leads to "unacceptable consequences" (which were labeled as "CD" for "Core Damage"). As can be seen in Figures 2-1 and 2-2, "unacceptable consequences" result from an Anticipated Transient ("AT") combined with a failure of the Reactor Protection System (RPS) to complete a scram from either a "RPS Elect[ric]" or "RPS Mech[anical]" failure, and either:

- o an unfavorable Moderator Temperature Coefficient ("MTC Overpressure"),
- o a failure to initiate Emergency Feedwater Flow ("EFW System Reliability"), or
- o a failure to initiate High Pressure Injection ("HPI") of borated water into the Reactor Coolant System (RCS).

At each branch point on an event tree, the upper branch indicates success (or favorable condition), while the lower branch indicates failure (or unfavorable condition). For example, under "MTC Overpressure" the upper branches following the branch points, indicate the probability of a favorable MTC, i.e., one which precludes overpressurization of the reactor coolant system. Note that Figures 2-1 and 2-2 are taken directly from the SECY-83-293 (Enclosure D, pages 65 and 66) except that Figure 2-2 includes "$P_{ATWS} = 8.0 \times 10^{-5}$" (the total of Figures 2-1 and 2-2).

The basis for the frequency or probability assigned to each branch as stated in SECY-83-293 is the following:

(a) Frequency of Anticipated Transients ("AT"), 2.8 and 1.2 per reactor year for turbine trip and non-turbine trip events, respectively, is based on plant operating experience as provided in References 2.2 and 2.3.

(b) Probability of a Reactor Protection System electrical ("RPS Elect") or mechanical failure ("RPS Mech"), 2.0×10^{-5} and 1.0×10^{-5}, respectively, is based on plant operating experience as provided in Appendix A of SECY-83-293.

(c) Probabilities of an unfavorable moderator temperature coefficient ("MTC Overpressure"), 0.5 and 1.0, are based on previous NRC review (Reference 2.4) of the analysis of C-E plant responses to ATWS events (References 2.5 and 2.6). Inherent in the non-turbine trip probability for an unfavorable MTC, 1.0, is the NRC assumption that an RPS electrical failure causes a failure to initiate a turbine trip following a reactor trip signal or any other signal. It is also important to note that these values correspond to the probability of the MTC being insufficiently negative such that the reactor coolant system pressure exceeds 3200 psia. For the purposes of the estimates of P_{ATWS}, the SECY-83-293 assumes that exceeding 3200 psia will lead to unacceptable consequences.

(d) The probabilities of failing to initiate emergency feedwater, 0.04 if automatic initiation is required, and 0.16 if manual initiation is required, are based on References 2.7 and Enclosure D of SECY-83-293, respectively. Note that the NRC analysis assumes that a RPS electrical failure also causes a failure to automatically initiate emergency feedwater.

(e) The probability of failing to initiate high pressure boron injection is based on an estimate of human error provided in Enclosure D of SECY-83-293.

Figure 2-3 is the simplified event tree used in SECY-83-293 to estimate P_{ATWS} for C-E manufactured plants which are modified in accordance to the ATWS Rule. This Figure is taken directly from page 67 of Enclosure D to SECY-83-293 except that the frequencies for the bottom three branches are added into the total.

These plant modifications are reflected in Figure 2-3 in the following ways:

- The addition of a turbine trip actuation which is diverse from the reactor trip system. This will assure that all anticipated transients of concern will result in a turbine trip, even in the presence of a RPS electrical failure. Therefore, the frequency of the significant anticipated transients is the sum of the turbine trip and non-turbine trip event frequencies (i.e., 4.0 per reactor year).
- The addition of a DSS which reduces the RPS electrical failure probability from 2.0×10^{-5} to 2.0×10^{-6}.
- The addition of a new EFAS that is totally diverse, independent, and separate from the RTS. This assures automatic emergency feedwater initiation even in the presence of a RPS electrical failure, and eliminates the reliance on manual initiation. Consequently, the failure probability decrease from 0.16 to 0.04.

The evaluation of the impact of various ATWS related plant modifications presented in SECY-83-293 used the probabilities given above as point estimates to calculate the severe ATWS frequencies. Enclosure D of SECY-83-293 (page 31) states that the net effect of adding a DSS, a diverse TT, and a diverse EFAS is a reduction of P_{ATWS} from 8.0×10^{-5} per reactor year to 2.2×10^{-5} per reactor year. Note that the "Total" frequency on Figure 2-3 is actually 2.62×10^{-5} per reactor year when the frequencies for the bottom three branches are added into the total. Using this corrected value, the addition of the DSS, diverse TT, and diverse EFAS results in a net reduction of the severe ATWS frequency of 5.38×10^{-5} per reactor year.

Figure 2-4 uses the same methodology as was used in SECY-83-293 to show the effect on the severe ATWS frequency of adding only the DSS with its inherently diverse TT. The effect is to reduce P_{ATWS} from 8.0×10^{-5} per reactor year to 2.66×10^{-5} per reactor year, a net reduction of 5.34×10^{-5} per reactor year. Thus, the use of this methodology indicates that the addition of a new diverse EFAS to a plant with a DSS and a diverse TT is an incremental reduction in P_{ATWS} of only 0.04×10^{-5} per reactor year, or 0.7% of that which would obtainable from the addition of all three systems. It should be emphasized that this analysis did not address the impact of uncertainties in the estimates of the failure probabilities.

To evaluate the impact of the modifications with uncertainties considered, the sequences on Figures 2-1 through 2-4 were translated into equations and solved using the CESAM code (Reference 2.8). Table 2-1 summarizes the failure probability distribution parameters used for this analysis. The following paragraphs summarize how these parameters were derived assuming that anticipated transient frequency and MTC overpressure were treated as constants.

NUREG-0460 states that the total unavailability of the RPS is in the range of 10^{-5} to 10^{-4} and that the value 3.0×10^{-5} was selected for the analysis. This suggests that the total RPS unavailability is log-normally distributed with a median of 3.0×10^{-5} and an error factor of 3. On pages 65 and 66 of Enclosure D to SECY-83-293, the NRC divided the total RPS unavailability into RPS mechanical and RPS electrical with values of 1.0×10^{-5} and 2.0×10^{-5} respectively. These values were assumed to be medians and an error factor of 3 was assigned to each.

Both "failure to manually initiate EFW" and "failure to initiate high pressure injection" are human errors. The failure probabilities (0.16 and 0.05 respectively) were assumed to be median values and an error factor of 5 was used based on Table 20.26 of NUREG/CR-1278 (Reference 2.9).

For automatic initiation of EFW, the failure probability of 0.04 was assumed to be the median value. Analyses of engineered safety features actuation systems have yielded error factors in the range of 4 to 5. Therefore, an error factor of 5 was used for failure to automatically initiate EFW.

A DSS failure probability of 0.1 can be derived from a reduction in "RPS Elect" from 2.0×10^{-5} in Figure 2-1 to 2.0×10^{-6} in Figure 2-3. The value of 0.1 was assumed to be a median value and an error factor of 3 was selected based on the error factor used for the RPS.

The severe ATWS frequencies were calculated for three cases. The first is the base case as represented by Figures 2-1 and 2-2. The second is based on modifying the plant to include a DSS, diverse TT and diverse EFAS as represented by Figure 2-3. The third case is based on modifying the plant to include a DSS and diverse TT. The results of these calculations are presented in Table 2-2.

Using the mean values, the net effect of modifying the plant to include a DSS, a diverse TT and a diverse EFAS is to reduce PATWS from 8.98 x 10^{-5}/year to 3.6 x 10^{-5}/year, a net reduction of 5.38 x 10^{-5}/year. If only the DSS and diverse TT are included, PATWS is reduced from 8.98 x 10^{-5}/year to 3.69 x 10^{-5}/year, a net reduction of 5.29 x 10^{-5}/year.

The results of the evaluation of the impacts of ATWS related modifications, both with and without uncertainties considered is summarized in Table 2-2. As shown on Table 2-2, the DSS and diverse Turbine Trip account for over 98% of the risk reduction achievable by installing a DSS, a diverse Turbine Trip and diverse EFAS. The diverse EFAS accounts for less than 2% of the achievable risk reduction.

The incremental ATWS risk reduction (decrease in P_{ATWS}) associated with the installation of a diverse EFAS is calculated from the ATWS probabilities listed in Table 2-2. The calculated incremental risk reduction afforded by diverse EFAS installation is 9.0 x 10^{-7} per reactor year. This is based on C-E analysis with uncertainties propagated, which, of the three analyses summarized in Table 2-2, yields the largest incremental value for diverse EFAS.

In the regulatory analysis in Enclosures C and D of SECY-83-293, the value of a plant modification is calculated as:

$$\text{Value} = (\text{Cost of Unmitigated ATWS}) \times (\text{Decrease in } P_{ATWS}) \times (\text{30 Years of Remaining Plant Lifetime}) \qquad \text{(Eq. 2-1)}$$

In Enclosure D to SECY-83-293 (page 31) the NRC assumes the cost of an unmitigated ATWS to be $10 billion. Using this value, Equation 2-1 reduces to:

$$\text{Value} = (\$3.0 \times 10^{11}) \times (\text{Decrease in } P_{ATWS}) \qquad \text{(Eq. 2-2)}$$

Using the decrease P_{ATWS} for diverse EFAS from Table 2-2, Equation 2-2 becomes:

$$\text{Value} = (\$3.0 \times 10^{11}) \times (9.0 \times 10^{-7}) = \underline{\$270{,}000} \qquad \text{(Eq. 2-3)}$$

2.1 REFERENCES FOR SECTION 2.0

2.1 SECY-83-293, "Amendments to 10CFR50 Related to Anticipated Transients Without Scram (ATWS) Events", July 19, 1983.

2.2 EPRI NP-2230, "ATWS: A Reappraisal: Part 3: Frequency of Anticipated Transients", January, 1982.

2.3 EPRI NP-801, "ATWS: A Reappraisal: Part III: Frequency of Anticipated Transients", July, 1978.

2.4 NUREG 460, "Anticipated Transients Without Scram for Light Water Reactors", March 1980.

2.5 CENPD-158, Revision 1, ATWS Analyses, "Analysis of ATWS in Combustion Engineering NSSS's", May, 1976.

2.6 CENPD-263, "ATWS Early Verification, Response to NRC Letter of February 15, 1979, for Combustion Engineering NSSS's", November, 1979.

2.7 SAI-011-82-SJ, "Technical Support for the Utility Group on ATWS", Science Applications, Inc., December 31, 1981.

2.8 "A Users' Manual for CESAM, Combustion Engineering Monte Carlo Sampling Code", CE-CES-49, April, 1985.

2.9 A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with an Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, October, 1980.

TABLE 2-1
FAILURE PROBABILITIES FOR ATWS ANALYSIS

ITEM	POINT ESTIMATES	MEDIAN	ERROR FACTOR
ANTICIPATED TRANSIENT	4.0		
TURBINE TRIP	2.8		
NON-TURBINE TRIP	1.2		
RPS ELECTRICAL		2×10^{-5}	3
RPS MECHANICAL		1×10^{-5}	3
DIVERSE SCRAM SYSTEM		1×10^{-1}	3
MTC OVER PRESSURE	0.5		
AUTOMATIC EFW ACTUATION		4×10^{-2}	5
MANUAL EFW ACTUATION		0.16	5
HIGH PRESSURE INJECTION ACTUATION (MANUAL)		5×10^{-2}	5

TABLE 2-2

EFFECTS OF PLANT MODIFICATIONS ON P_{ATWS}

		P_{ATWS}		
Treatment of Uncertainties	Base Case	All Three Modifications Included	DSS and Diverse TT Included	Benefit Attributable To DSS + TT
NRC Staff Analysis (Uncertainties Not Considered)	8.0×10^{-5}	2.62×10^{-5}	2.66×10^{-5}	99.3%
C-E Analysis (Uncertainties Propagated, Mean Values)	8.98×10^{-5}	3.60×10^{-5}	3.69×10^{-5}	98.3%
C-E Analysis (Uncertainties Propagated, Median Value)	7.83×10^{-5}	2.99×10^{-5}	3.04×10^{-5}	99.0%

TABLE 2-3

ATWS CORE MELT FREQUENCY REDUCTIONS AND ASSOCIATED VALUES (BENEFITS)*

MODIFICATION	CORE MELT FREQUENCY REDUCTION	PERCENT OF TOTAL FREQUENCY REDUCTION	VALUE
INCLUDE:			
DSS, DIVERSE TURBINE TRIP AND DIVERSE EFAS	5.38×10^{-5}	100%	$16,140,000
INCLUDE:			
DSS AND DIVERSE TURBINE TRIP ONLY	5.29×10^{-5}	98.3%	$15,870,000
INCLUDE:			
DIVERSE EFAS	9×10^{-7}	1.7%	$270,000

---

* Based on C-E analysis with uncertainties propagated, mean values

Figure 2-1

C-E/B&W Base Cases Turbine Trip Transients

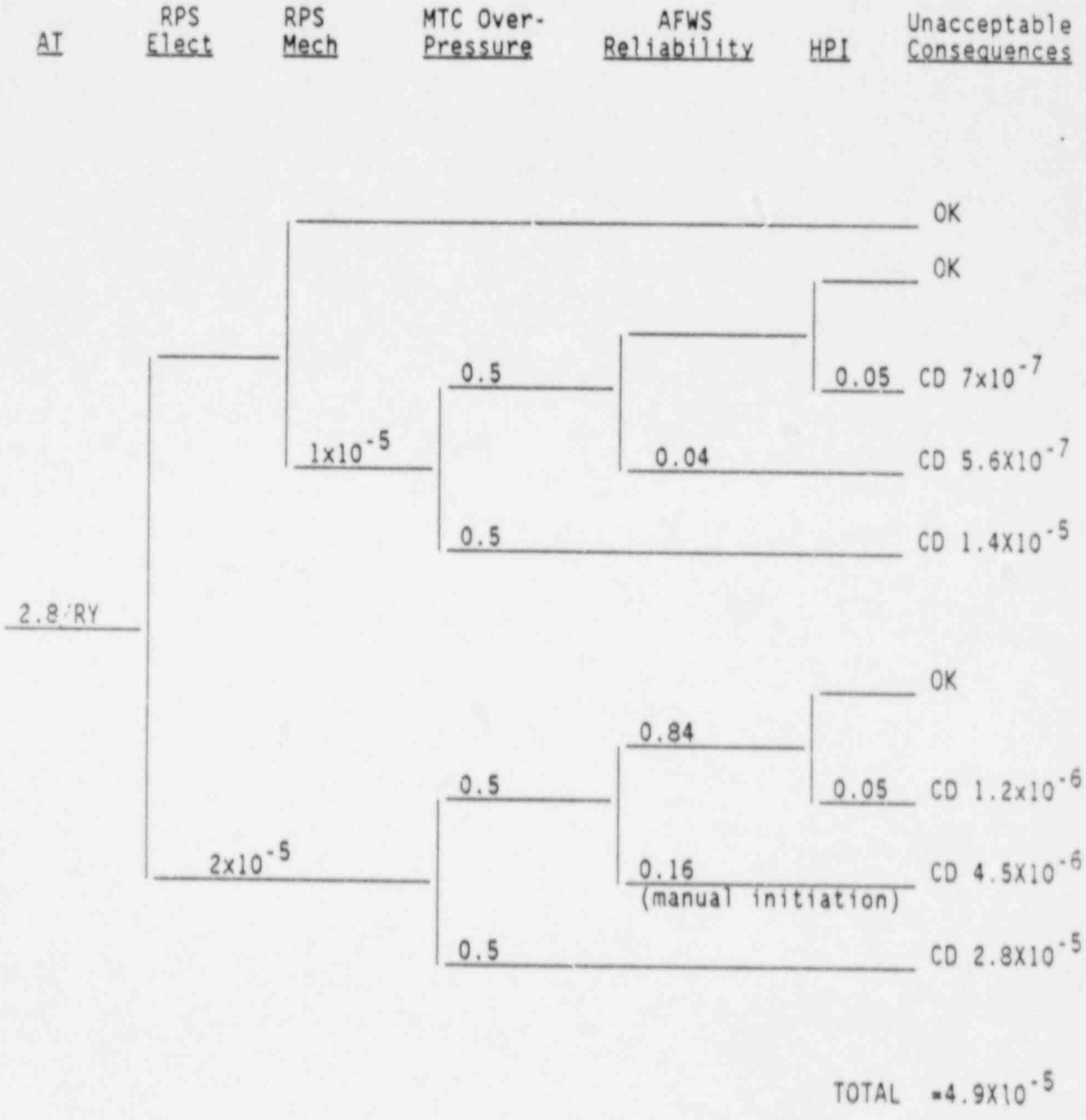
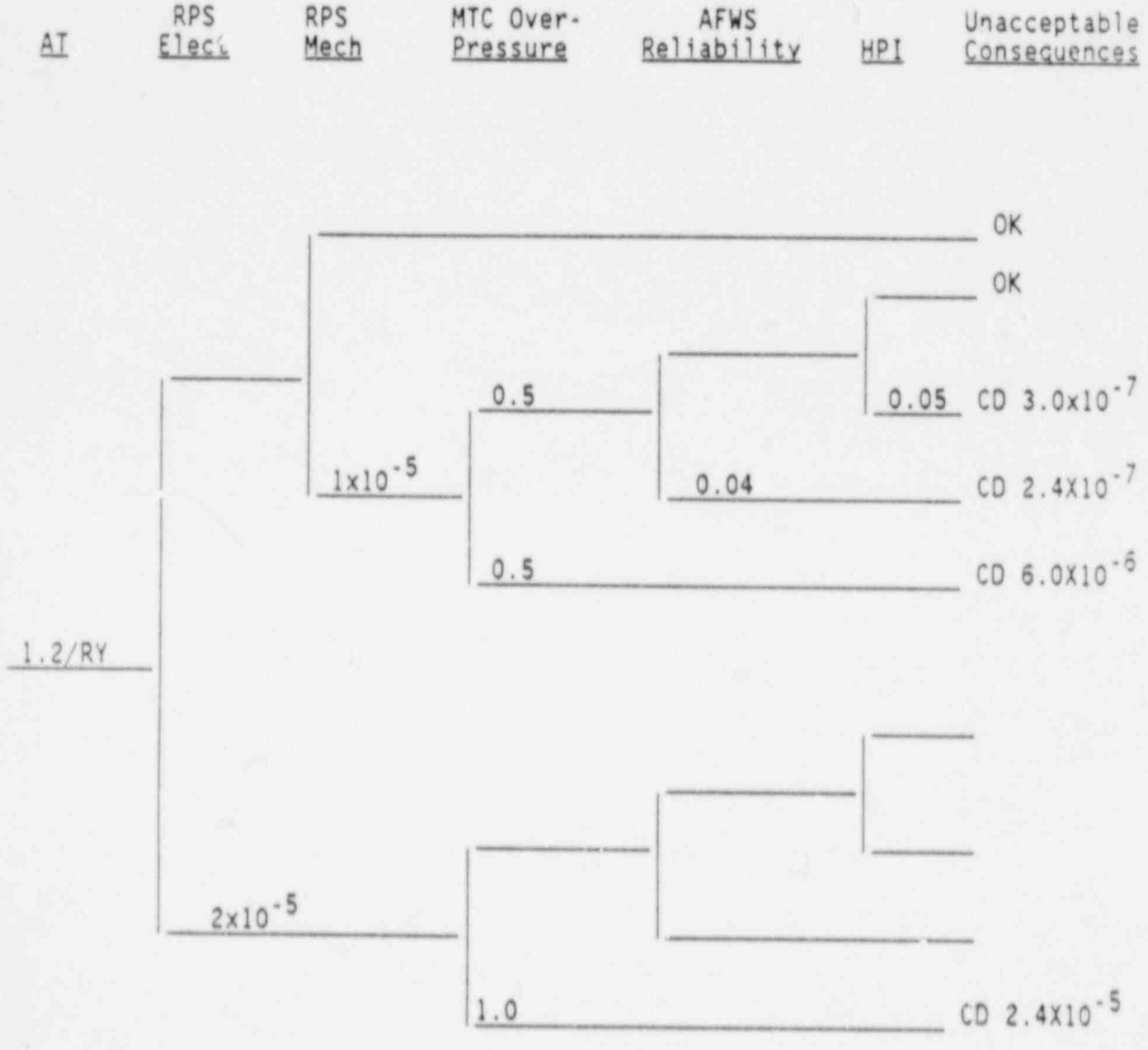


Figure 2-2

C-E/B&W Base Cases Non-Turbine Trip Transients



TOTAL = $3.1\text{X}10^{-5}$

P_{ATWS} = $8.0\text{X}10^{-5}$

Figure 2-3

Diverse Scram System Installed
Diverse AFW and Turbine Trip Installed

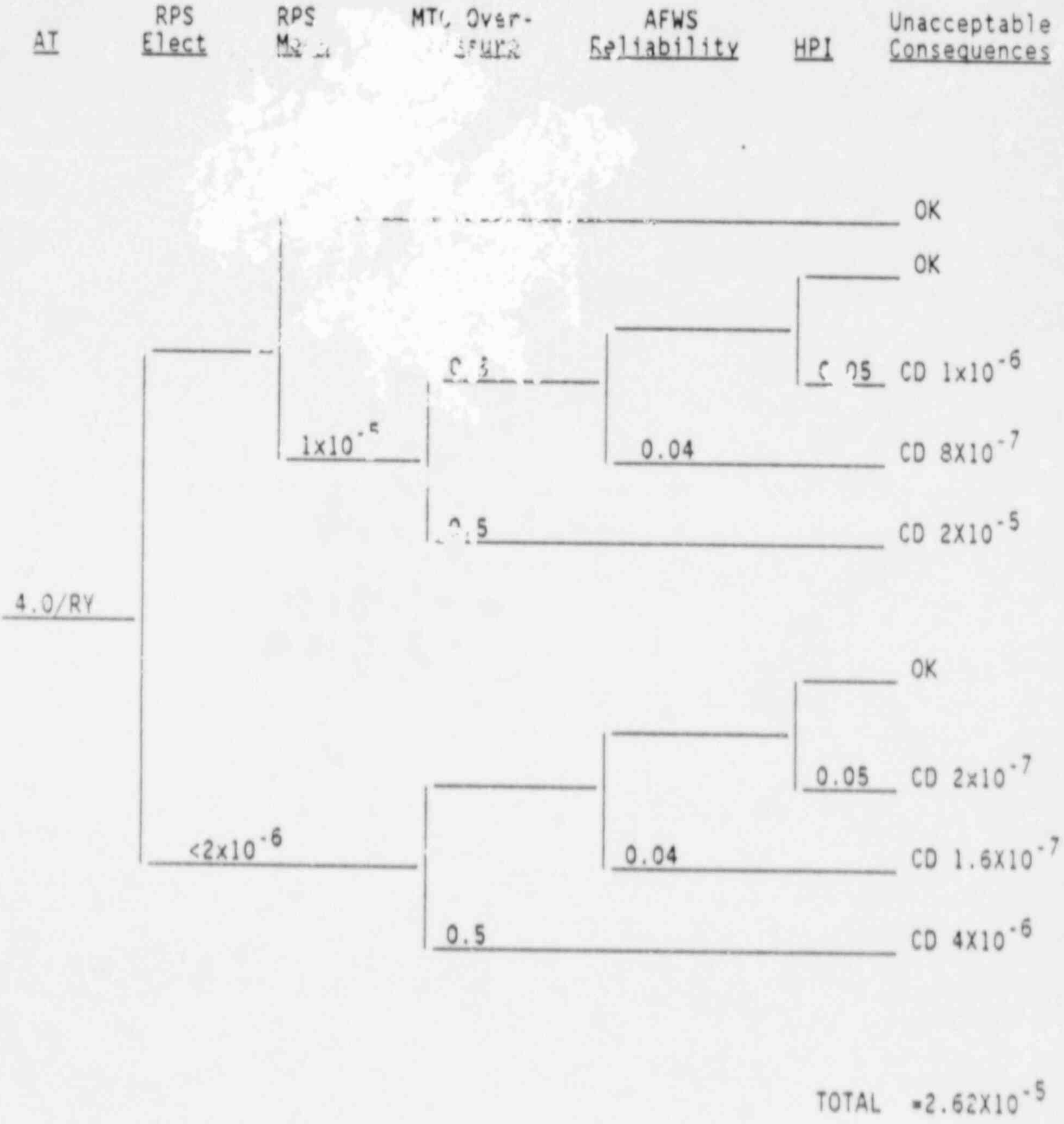
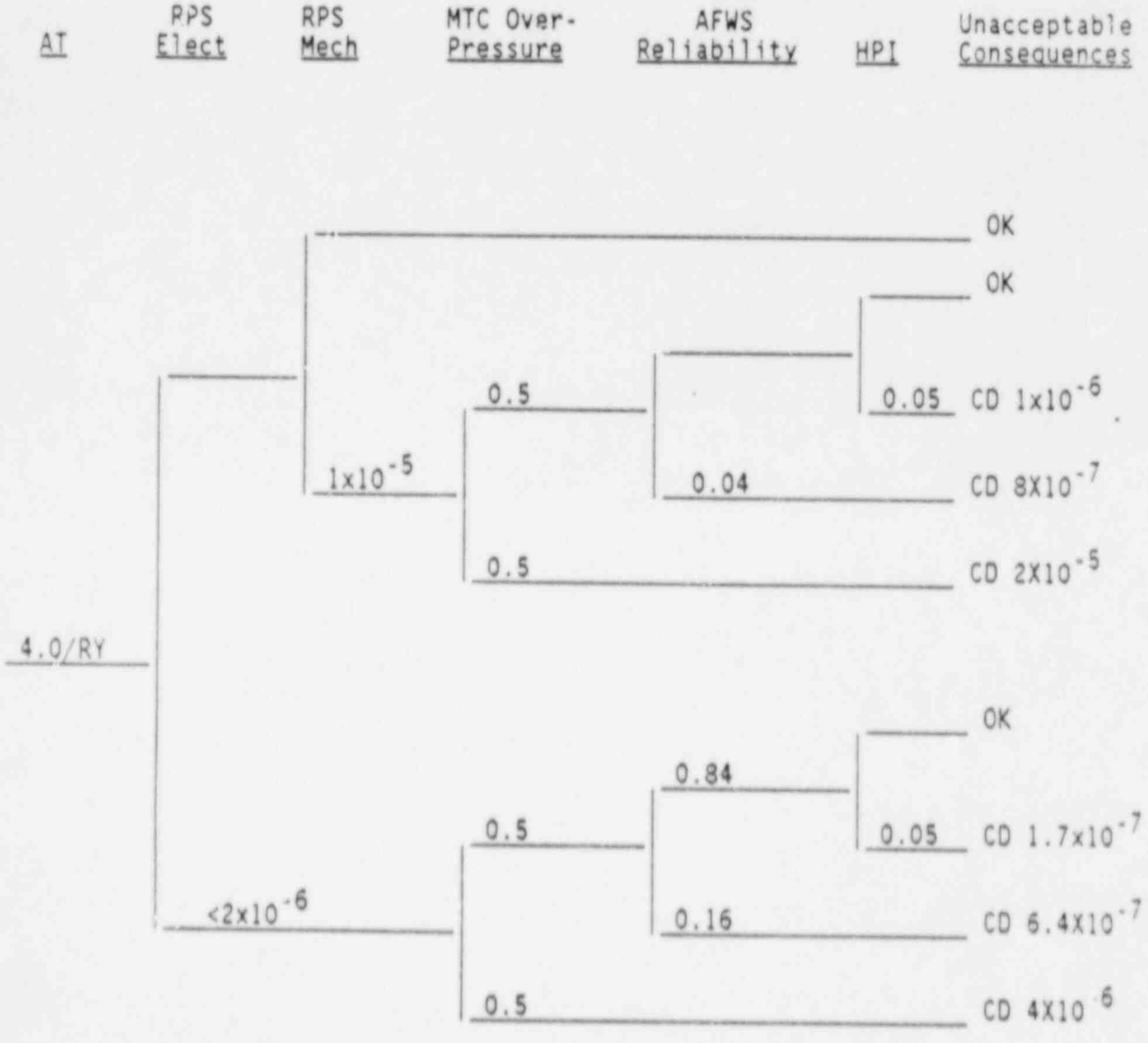


Figure 2-4

Diverse Scram System and Turbine Trip Installed



TOTAL =2.66X10^{-5}

3.0 CONCLUSIONS

Based on this evaluation, it has been shown that the value of the plant modifications associated with compliance with the ATWS rule is $270,000. The evaluation was performed using the same methodology as was used in SECY-83-293 and has considered the effects of the uncertainties of the probabalistic analysis. The results of this evaluation will be factored into the Value/Impact analysis presented in CEN-380.