

Westinghouse Non-Proprietary Class 3

**WCAP-15830-NP
Revision 0**

March 2003

Staggered Integrated ESF Testing



LEGAL NOTICE

This report was prepared as an account of work sponsored by the CE Owners Group and Westinghouse Electric Company LLC. Neither Westinghouse nor the CEOG, nor any person acting on their behalf:

- A. Makes any warranty or representation, express or implied including the warranties of fitness for a particular purpose or merchantability, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or
- B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method, or process disclosed in this report.

Westinghouse Electric Company LLC
2000 Day Hill Road P.O. Box 500
Windsor, Connecticut 06095-0500

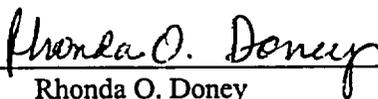
WCAP-15830-NP, Rev. 0

Staggered Integrated ESF Testing

March 2003

Author: 
Joseph R. Congdon
Plant Systems Engineering

Author: 
David Finnicum
Reliability Risk Assessment

Approved: 
Rhonda O. Doney
Plant Systems Engineering

COPYRIGHT NOTICE

This report has been prepared by Westinghouse Electric Company LLC, for the members of the CE Owners Group participating in this Group Task. Information in this report is the property of and contains copyright information owned by Westinghouse Electric Company LLC and /or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document and the information contained therein in strict accordance with the terms and conditions of the agreement under which it was provided to you.

As a participating member of this CE Owners Group task, you are permitted to make the number of copies of the information contained in this report which are necessary for your internal use in connection with your implementation of the report results for your plant(s) in your normal conduct of business. Should implementation of this report involve a third party, you are permitted to make the number of copies of the information contained in this report which are necessary for the third party's use in supporting your implementation at your plant(s) in your normal conduct of business if you have received the prior, written consent of Westinghouse Electric Company LLC to transmit this information to a third party or parties. All copies made by you must include the copyright notice in all instances.

The NRC is permitted to make the number of copies beyond those necessary for its internal use that are necessary in order to have one copy available for public viewing in the appropriate docket files in the NRC public document room in Washington, DC if the number of copies submitted is insufficient for this purpose. Copies made by the NRC must include the copyright notice in all instances.

TABLE OF CONTENTS

1.0	INTRODUCTION	1-1
1.1	Purpose	1-1
1.2	Approach and Methodology.....	1-1
2.0	SCOPE.....	2-1
2.1	Statement of Need and Benefits.....	2-1
2.2	Applicable Technical Specification Surveillance Requirements	2-4
2.3	Integrated ESF Testing Bases and Related Industry Initiatives	2-6
2.3.1	Technical Specification Bases.....	2-6
2.3.2	Regulatory Guidelines.....	2-8
2.3.3	Industry Standards and Guides.....	2-9
2.3.4	Related ESFAS CEOG Reports	2-10
3.0	BACKGROUND	3-1
3.1	Engineered Safety Features Actuation System (ESFAS) System Description.....	3-1
3.1.1	Non-CE ESFAS Design.....	3-1
3.1.2	CE ESFAS Design	3-3
4.0	APPROACH AND METHODOLOGY.....	4-1
4.1	Overview.....	4-1
4.2	Procedure Review Process.....	4-1
4.2.1	Functions Tested by the Integrated ESF Test.....	4-1
4.2.2	Diesel Generator Testing Included in the Integrated ESF Test.....	4-2
4.2.3	Review and Overlap with Other ESF Surveillance Tests.....	4-2
4.2.4	Procedure Review Results	4-5
4.3	Component Screening and Preliminary Categorization Process	4-12
4.3.1	Category Definitions	4-12
4.3.2	Classification Results	4-16
4.4	Guidelines for Plant Specific PSA Model Adjustments and Requantification of Risk.....	4-18
4.4.1	Category A-1.....	4-18
4.4.2	Category A-2.....	4-19
4.4.3	Category A-3.....	4-20
4.4.4	Category A-4.....	4-21
4.4.5	Category B	4-22
4.5	Common Cause Adjustment When Introducing Staggered Testing.....	4-23
4.5.1	Introduction	4-24
4.5.2	CCF for standby equipment	4-25
4.5.3	Conclusions.....	4-26
4.6	Load shed and Breaker modeling issues and considerations	4-30
4.6.1	Breaker Modeling Issues.....	4-30
5.0	TECHNICAL JUSTIFICATION.....	5-1
5.1	Assessment of Deterministic Factors	5-1
5.1.1	Impact On Defense-In-Depth.....	5-1
5.1.2	Impact On Deterministic Safety Margins.....	5-2
5.2	Assessment of Risk Factors	5-2
5.2.1	Process Summary.....	5-2
5.2.2	Evaluation of Results	5-4
5.3	Operating Review and Analsis.....	5-9
5.3.1	Analyses of All Failures and Issues Discovered during Intergrated ESF Testing.....	5-9
5.3.2	Analyses of Equipment Failures Discovered during Intergrated ESF Testing.....	5-10
6.0	RESULTS AND CONCLUSIONS.....	6-1
6.1	Risk Evaluation.....	6-1
7.0	REFERENCES	7-1

App. A	Application of WCAP-15830 to Calvert Cliffs Units 1 and 2	A-1
App. B	Application of WCAP-15830 to Fort Calhoun Station	B-1
App. C	Application of WCAP-15830 to Palisades Nuclear Power Plant.....	C-1
App. D	Application of WCAP-15830 to Waterford Steam Electric Station Unit 3	D-1

LIST OF TABLES

4.2-1	Functions Addressed by Integrated ESF Testing.....	4-3
4.2-2	Emergency Diesel Generator Testing Included In The Integrated Safeguards Tests	4-4
4-3-1	Summary of Classification Results by Unit	4-17
5.2-1	Results from Sequential to Staggered Integrated ESF Testing.....	5-2
5.3-1	Integrated ESF Test Performance Summary	5-10
5.3-2	Verifications vs Failures.....	5-10

LIST OF FIGURES

4.2-1	SIAS Actuation Testing at Calvert Cliffs Units 1 and 2.....	4-6
4.2-2	CIS Actuation Testing at Calvert Cliffs Units 1 and 2	4-7
4.2-3	CSAS Actuation Testing at Calvert Cliffs Units 1 and 2	4-8
4.2-4	RAS Actuation Testing at Calvert Cliffs Units 1 and 2.....	4-9
4.2-5	Undervoltage Sensing Testing at Calvert Cliffs Units 1 and 2.....	4-10
4.2-6	EDG Sequencer Testing at Calvert Cliffs Units 1 and 2	4-11
4.3-1	Component Categorization Process Flow Chart.....	4-14

ACRONYMS

AFAS	Auxiliary Feedwater Actuation Signal
ALARA	As Low As Reasonably Achievable
ANO2	Arkansas Nuclear One Unit 2
ASME	American Society of Mechanical Engineers
CC	Calvert Cliffs
CCF	Common Cause Failure
CCW	Component Cooling Water
CDF	Core Damage Frequency
CE	Combustion Engineering
CEOG	CE Owners Group
CIAS	Containment Isolation Actuation Signal
CS	Containment Spray
CSAS	Containment Spray Actuation Signal
DBA	Design Basis Accident
DG-1, DG-2	Emergency Diesel Generator for Train A and Train B respectively
EA	Engineering Analysis
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EFAS	Emergency Feedwater Actuation Signal
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FCS	Fort Calhoun Station
FTS	Failure to Start
HPSI	High Pressure Safety Injection
IST	In-service Testing
LCO	Limiting Condition for Operation
LERF	Large Early Release Fraction (some fraction of CDF)
LOP	Loss of Power
LPSI	Low Pressure Safety Injection
LTOP	Low Temperature Over Pressurization
MCC	Motor Control Center
MP2	Millstone Point Unit 2
MSIS	Main Steam Isolation Signal
NRC	Nuclear Regulatory Commission
OOS	Out of Service
OPPD	Omaha Public Power District
PAL	Palisades
PSA	Probabilistic Safety Analysis
PVNGS	Palo Verde Nuclear Generation Station
PWR	Pressurized Water Reactor
RAS	Recirculation Actuation Signal
RCS	Reactor Coolant System
RPS	Reactor Protection System
RWST	Refueling Water Storage Tank
SDC	Shutdown Cooling

ACRONYMS (continued)

SIAS	Safety Injection Actuation Signal
SL	St. Lucie
STI	Surveillance Test Interval
TS	Technical Specification
UV	Under Voltage
VCT	Volume Control Tank
VIAS	Ventilation Isolation Actuation Signal
WSES	Waterford Steam Electric Station

ABSTRACT

This report documents the results of Combustion Engineering Owners Group (CEOG) Task 2016, "Staggered Integrated ESF Testing". CEOG Task 2016 used a risk-Informed approach to demonstrate that changing the integrated Engineered Safety Features (ESF) test from once per cycle on a sequential basis to once every other cycle on a staggered basis results in a negligible change in risk. Currently, integrated ESF testing is performed on both ESF trains each refueling cycle. Using a staggered approach, one ESF train would be tested each refueling outage with each ESF train being tested once every other cycle. The basic premise of the project was the belief that the integrated ESF test is not the primary/sole operability test for the majority of the components tested. Other surveillance procedures are performed on many of these components and functions on a more frequent basis. Therefore, there is considerable overlap between other tests and the integrated ESF test.

The calculated change in core damage frequencies (i.e. Δ CDFs) at the plants varied from { } to { }. The change in large early release frequencies (i.e. Δ LERFs) at the plants varied from { }. ANO-2 had no components for which the integrated ESF test was the sole test of operability, therefore that plant had no change in CDF or LERF associated with the proposed change to the integrated ESF test scheme. The acceptance guidelines for the proposed change as provided in Section 2.2.5 of Regulatory Guide 1.174 consider CDF changes and LERF changes of $1.0E-06/\text{yr}$ and $1.0E-07/\text{yr}$, respectively, to be very small regardless of base CDF and LERF. The guidelines also consider plant changes resulting in very small changes in CDF and LERF to be acceptable from a risk perspective.

The conclusion is that changing the integrated ESF test from once per cycle with sequential testing to once every other cycle with staggered testing results in very small risk changes. Therefore the proposed changes are acceptable from a risk perspective.

1.0 INTRODUCTION

1.1 PURPOSE

The objective of this report is to demonstrate on a risk-informed basis that extending the surveillance test interval for surveillance requirements typically addressed by "Integrated ESF testing" results in a negligible change in plant risk. All of the identified surveillance requirements apply to both ESF trains and are performed when the plant is shutdown each refueling outage. This report supports changing the integrated ESF test interval from once per refueling cycle on a sequential basis (i.e. both trains tested each refueling cycle) to once every other cycle on a staggered basis (i.e. each train tested once every two refueling cycles with one train being tested each refueling cycle on an alternating basis).

Seven CEQG utilities representing a total of twelve units participated in this task. The participants included:

1. Arizona Public Service, Palo Verde Units 1, 2 and 3
2. Entergy Nuclear South, Arkansas Nuclear One, Unit 2 and Waterford Steam Electric Station, Unit 3
3. Constellation Entergy Group, Calvert Cliffs Nuclear Power Plant, Units 1 and 2
4. Nuclear Management Company, Palisades
5. Florida Power and Light, St. Lucie Units 1 and 2
6. Dominion Nuclear Connecticut, Millstone Unit 2
7. Omaha Public Power District, Ft. Calhoun Station

The proposed change will benefit the utilities in the following ways:

1. Critical path and operations and maintenance cost savings
2. Reduce Human Performance challenges
3. Dose reduction (ALARA)
4. Reduce RCS mass addition challenges
5. Reduce wear and tear on safety equipment
6. Reduce challenges to safety related equipment
7. Negligible impact on plant risk

1.2 APPROACH AND METHODOLOGY

This effort used a risk-informed approach to demonstrate that any change in risk will be negligible if a staggered test frequency were adopted for integrated ESF testing. Currently, integrated ESF testing is performed on both ESF trains every refueling cycle. Using a staggered approach, only one train would be tested each refueling outage. The integrated ESF test is typically not the primary or sole operability test for the majority of the components and functions tested. Other, more frequently performed surveillance tests also verify the operability of many of the components and functions tested by the integrated ESF test. Therefore, there exists a certain amount of overlap in ESF testing.

For the components and functions that are tested only by the integrated ESF test, the risk model was adjusted, the risk associated with the change in test frequency was recalculated and the overall change in risk requantified. In some cases, a deterministic basis was developed to show that the component failure mode addressed by the integrated ESF test is not risk-significant. These components were exempted from further PSA review and analysis.

2.0 SCOPE

2.1 STATEMENT OF NEED AND BENEFITS

Reduction in potential for transients

The potential for unexpected transients is increased during the period when the plant is being lined-up for the integrated ESF test, through test performance, and restoration following the test. This potential results from the need to establish special test conditions to perform the test while maintaining safe shutdown conditions. Examples of the special conditions include: abnormal valve alignments, installing jumpers, lifting leads, placing breakers in "TEST" position and placing relays in the "CONTACT" position.

Transients and near misses that have occurred concurrent with integrated ESF testing include: inadvertently transferring water to the containment sump, inadvertent transfers from the Boric Acid Storage Tanks resulting in violating the minimum requirements, overflowing the RWST, and exceeding the maximum overpressure in the VCT. Reducing the amount of testing, (one train versus both trains) will reduce the potential for these and similar transients during a refueling outage.

Reduction in human performance challenges

Integrated ESF testing is the most complex test run during an outage. Testing on each channel takes approximately 24 hours to complete: eight (8) hours to establish the equipment lineup, 8 hours to run the transients, and 8 hours to restore. During the 8 hours when the transients are run, essentially all other work on site stops. The transients result in short term loss of normal lighting in all areas of the plant, and also loss of power to the cranes in containment, spent fuel storage area and the turbine building.

The integrated ESF test usually does not identify many equipment failures but does lead to other "human performance" issues due to its complexity and duration. The same test engineers and operator crews run the test on both trains. Therefore they are fatigued by the time testing concludes.

During a typical refueling outage at a plant, there are extra personnel in the plant performing a variety of tasks. Many of these people may be contractors or technicians from other plants. Many systems/components are tagged Out-of-Service (OOS) to support outage maintenance activities. It is challenging for Outage Management and Operations to coordinate and safely execute all the required work activities, surveillance testing, and post maintenance. Events have occurred as a result of breakdowns in communications and administrative controls, which challenged the plant staff to maintain configuration control of the plant. For example, there have been conflicts when performing pre-test system alignment and clearing tags to return a component to service. Reducing the amount of required testing and sometimes complex system alignments to support the testing will help reduce the human performance pressures on plant personnel as they strive to do the work and at the same time maintain the plant safely shutdown. Staggered integrated ESF testing will improve scheduling and the coordination of outage activities centered on safety related equipment maintenance, thus minimizing impacts on shutdown safety. It will also reduce the number of potential challenges to containment closure.

Reducing the amount of integrated ESF testing during the outage will reduce stress on plant operators and wear and tear on safety related equipment. The integrated ESF test demands very close timing and coordination among those involved in supporting the test. Frequently, a portion of the test will have to be repeated because of inadvertently starting a stop watch or data recorder at the required time. Unplanned repetitive testing due to things like missing a data point creates extra stress on the test crew and results in unnecessary wear and tear on safety related equipment.

Reduction in radiation dose to personnel (ALARA)

Radiation exposure related to this test may be significant at some utilities. Setting up for and restoration from integrated ESF testing requires a number of off-normal conditions to be established by operators and technicians. Valve alignments may require accessing potential high radiation fields or contaminated areas in the auxiliary building and the containment. During the test, operators may also have to be stationed in these remote locations to observe equipment response and collect data. Many of these actions also require independent verifications. The proposed change to reduce the amount of testing may result in savings in avoidable exposure. This would help the plant realize the lowest achievable radiation exposure for the outage.

Reduction in RCS mass additions challenges

Integrated ESF testing involves testing the response of an entire ESF train to various actuation signals, either with or without offsite power available. This includes starting the High Pressure Safety Injection (HPSI), Low Pressure Safety Injection (LPSI) and Containment Spray (CS) pumps on minimum-flow recirculation. System pre-test alignments are designed to avoid moving water into the primary system. However, these pumps are more than capable of injecting water into the RCS when an isolation valve is misaligned or check valve leaks-by during refueling. RCS conditions during the test are cold and depressurized. Therefore, the danger exists for low-temperature overpressure conditions if the RCS is inadvertently pressurized by one of these pumps. Such overpressurization is unlikely, since the pressurizer will be vented and Low Temperature Overpressure Protection (LTOP) will be in effect. Nevertheless, it is important to always strive to minimize the opportunities for inadvertent mass additions to the primary system while shutdown. Staggered integrated ESF testing supports this objective.

Reduction in challenges to safety equipment and plant security

As mentioned previously, by reducing the amount of integrated ESF testing the number of times components will be cycled for testing will be reduced. One complete train of safeguards equipment will be available throughout the outage since it will no longer be necessary to switch protected trains to support testing of the entire system. Having the same protected train for the entire outage will enhance safety by making it easier for plant personnel to keep track of the protected train, thus reducing the likelihood of certain human-performance errors. There have been a few events in which the vulnerability of a plant to single active failures has unknowingly increased because of inadequate procedural controls when establishing the required configuration and alignment for the test. The electrical transients sometimes result in failures of non-vital components having sensitive electronics.

Reducing the amount of integrated ESF testing will also reduce the number of events related to site security systems and procedures. There have been occasions when security systems/equipment have been inadvertently removed from service during testing because of failures in electrical power supplies or transfer devices. Back up procedures exist to deal with these situations, but the mere occurrence generates additional documentation. The situations will be less likely with the reduced test frequency.

In addition to the work stoppage that occurs when this test is run, there are additional costs associated with security. The security doors lose power; consequently extra guards must be assigned to watch the doors.

Reduction in safety related equipment wear and tear

By necessity, ESF system equipment must be exercised by testing, since the primary purpose of periodic testing is to prove operability. However, for the reasons mentioned above, sometimes it is necessary to repeat a complete test or part of the test for reasons that are relatively minor or insignificant, or could be accomplished by other means. It is this additional wear-and-tear on equipment that could be limited by reducing the amount of integrated ESF testing performed during an outage.

Also, by necessity during the integrated ESF test, the HPSI, LPSI and CS pumps must be operated for a time with only minimum recirculation flow. The pumps are designed to operate in this condition, but it is desirable to limit the duration of operation at low flow rate to the extent possible. On the other hand some large pumps such as Component Cooling Water (CCW) and Service Water (SW) may be operated at high flow and low discharge pressure during the test, because they are aligned to support both Shutdown Cooling (SDC) and ECCS loads. This operating condition also contributes to wear and tear on the pumps and system components.

Reduction in potential for personnel injury

Setting up for and restoration from integrated ESF testing requires a number of off-normal conditions to be established by plant operators and technicians. For example, breakers may need to be moved in and out of TEST position, fuses pulled, leads lifted and jumpers installed. Test connections and recorders must be installed to support data collection. Valve alignments, requiring access to remote locations within the auxiliary building and the containment, must be executed. During the test, operators must be stationed in remote locations to observe equipment response and collect data. Many of these activities place the operator or technician in a potential injury prone situation, e.g. electrical shock, burns, injury to the eyes or injury from a fall. By reducing the amount of testing, the amount of exposure to personnel injury will also be reduced.

Reduction in Operation and Maintenance costs

Integrated ESF testing is the most expensive test performed during an outage in terms of critical path activity. Some utilities estimate that eliminating the test on one channel per outage would result in a critical path savings of 16-24 hours. It is an expensive test because it takes a large amount of time and resources to execute safely. Because the test is considered an infrequent test, a separate dedicated team is typically used. The team is assembled several days prior to the test for training. The training is very detailed and includes operations, maintenance, engineering, quality assurance and health physics. Many activities must be coordinated. The team is used to perform the pre-test activities, execute the test and restore the system to normal after the test. By reducing integrated ESF testing in the outage by one half, thousands of dollars in labor costs alone can be saved each outage.

Cost is associated with:

- Being a critical path activity
- Having to hire contractors to cover tasks otherwise done by the plant staff
- Bring extra security personnel on shift
- Extra reporting and documentation associated with problems created by running an integrated ESF test

2.2 APPLICABLE TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENTS

Integrated ESF testing is performed each refueling outage to satisfy various TS surveillance requirements. Both engineered safeguard trains are tested, one train at a time. The test procedure explicitly lists all surveillance requirements addressed by the test procedure. There is considerable variation in integrated ESF test procedures from one plant to the next within the CEOG. All tests do however have certain objectives in common. The following is a summary of the surveillance requirements (per NUREG 1432, Reference 3) that are typically addressed by integrated ESF testing at most plants. These surveillance requirements are therefore the primary scope of this report

SR 3.3.5.2 - Perform a Channel Functional Test on each ESFAS Manual Trip channel.

SR 3.8.1.11 - Verify that on an actual or simulated loss of offsite power signal:

- a. De-energization of emergency buses
- b. Load shedding from emergency buses
- c. EDG auto-start from standby condition
 1. Energizes permanently connected loads in $< [10]^1$ seconds
 2. Maintains steady state voltage $\geq [3740]$ V and $\leq [4580]$ V
 3. Maintains steady state frequency $\geq [58.8]$ Hz and $< [61.2]$ Hz, and
 4. Supplies permanently connected [and auto-connected] shutdown loads for $\geq [5]$ minutes.

SR 3.8.1.12 - Verify on an actual or simulated Engineered Safety Features (ESF) actuation signal each EDG auto-starts from standby condition and:

- a. In $\leq [10]$ seconds after auto-start and during tests, achieves voltage $\geq [3740]$ V and frequency of $\geq [58.8]$ Hz
- b. Achieves steady state voltage $\geq [3740]$ V and $\leq [4580]$ V and frequency $\geq [58.8]$ Hz and $< [61.2]$ Hz
- c. Operates for $\geq [5]$ minutes
- d. Permanently connected loads remain energized from the offsite power system, and
- e. Emergency loads are energized [or auto-connected through the automatic load sequencer] from the offsite power system.

SR 3.8.1.16 - Verify each EDG:

- a. Synchronizes with offsite power source while loaded with emergency loads upon a simulated restoration of offsite power
- b. Transfers loads to offsite power source, and
- c. Returns to ready-to-load operation.

SR 3.8.1.18 - Verify interval between each sequenced load block is within $\pm [10\%$ of design interval] for each emergency [and shutdown] load sequencer.

¹ Note that the bracketed information obtained from NUREG 1432 and provided herein is intended to be treated as utility controlled information and should not be treated as proprietary information.

SR 3.8.1.19 - Verify on an actual or simulated loss of offsite power signal in conjunction with an actual or simulated ESF actuation signal:

- a. De-energization of emergency buses
- b. Load shedding from emergency buses
- c. EDG auto-starts from standby condition and
 1. Energizes permanently connected loads in $< [10]$ seconds
 2. Energizes auto-connected emergency loads through [load sequencer]
 3. Achieves steady state voltage $\geq [3740]$ V and $\leq [4580]$ V
 4. Achieves steady state frequency $\geq [58.8]$ Hz and $< [61.2]$ Hz, and
 5. Supplies permanently connected [and auto-connected] shutdown loads for $\geq [5]$ minutes.

Plants frequently coordinate other EDG surveillance testing with the integrated ESF test when it makes sense to do so. The type and nature of these tests varies greatly from plant to plant within the CEOG. These additional EDG surveillances are not explicitly within the scope of this report. The following is a list of surveillances falling into this category:

- SR 3.8.1.9 - Verify each EDG rejects a load greater than or equal to its associated single largest post-accident load.
- SR 3.8.1.10 - Verify each EDG does not trip, and voltage is maintained within limits during and following a full load rejection.
- SR 3.8.1.13 - Verify each EDG automatic trip is bypassed on [actual or simulated loss of voltage signal on the emergency bus concurrent with] an actual or simulated ESF actuation signal (except those trips listed in TSs).
- SR 3.8.1.14 - Verify each EDG operates for ≥ 24 hours at the specified loads and times.
- SR 3.8.1.15 - Verify each EDG starts within $\leq [10]$ seconds and achieves rated voltage and frequency when stated within 5 minutes of shutting down following $\geq [2]$ hours of operation.
- SR 3.8.1.17 - Verify, with a EDG operating in test mode and connected to its bus, an actual or simulated ESF actuation signal overrides the test mode by returning EDG to ready-to-load operation and automatically energizing the emergency load from offsite power

The utility may also use the integrated ESF test to partially satisfy additional technical specification surveillance requirements or testing required by the Technical Requirement Manual. This report does not specifically address these additional test requirements. Each utility must evaluate the impact of adopting staggered ESF testing on situations involving a partial compliance and modify the test accordingly. The following surveillance requirements provide examples that are typically partially addressed by the integrated ESF test.

LCO 3.3.6 - Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip

- SR 3.3.6.2 - Subgroup relay testing
- SR 3.3.6.3 - Channel Functional test on ESFAS Trip channels

LCO 3.3.5 - ESFAS Instrumentation

- SR 3.3.5.4 - ESF Response Time verifications

LCO 3.5.2 - ECCS – Operating

- SR 3.5.2.5 - Charging pump flow verification
- SR 3.5.2.6 - ESF actuation verification of ECCS automatic valves
- SR 3.5.2.7 - ESF actuation verification of ECCS pumps

LCO 3.6.6 - Containment Spray and Cooling Systems

- SR 3.6.6.6 - ESF actuation verification of CS automatic valves
- SR 3.6.6.7 - ESF actuation verification of CS pumps
- SR 3.5.6.8 - ESF actuation verification of Containment Cooling Trains

LCO 3.6.3 - Containment Isolation Valves

- SR 3.6.3.7 - ESF actuation verification of automatic Containment Isolation valves

LCO 3.7.7 - Component Cooling Water

- SR 3.7.7.2 - ESF actuation verification of automatic CCW valves
- SR 3.7.7.3 - ESF actuation verification of CCW pumps

2.3 INTEGRATED ESF TESTING BASES AND RELATED INDUSTRY INITIATIVES

2.3.1 Technical Specification Bases

The regulatory bases for integrated ESF testing is rooted in the bases for the individual TS surveillance requirements. The following surveillance requirements (per NUREG 1432) are typically addressed by the integrated ESF test:

- SR 3.3.5.2 - Channel Functional Test on ESFAS Manual Trip Channel
- SR 3.8.1.11 - EDG start verification on Loss of Offsite Power
- SR 3.8.1.12 - EDG start verification on ESF actuation
- SR 3.8.1.16 - Restoration of offsite power following Loss of Offsite power verification
- SR 3.8.1.18 - EDG Load sequencer interval verifications
- SR 3.8.1.19 - EDG start verification on Loss of Off-site Power with ESF actuation

SR 3.3.5.2 - Perform a Channel Functional Test on each ESFAS Manual Trip channel.

This Surveillance verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the Function.

SR 3.8.1.11 - EDG start verification on Loss of Offsite Power

This surveillance demonstrates the "as designed operation" of the standby power sources during loss of the offsite source. The test verifies all actions encountered from the loss of offsite power, including shedding of the nonessential loads and energizing the emergency buses and respective loads from the EDG. It further demonstrates the capability of the EDG to automatically achieve the required voltage and frequency within the specified time.

The EDG auto-start time of [10] seconds is derived from requirements of the accident analysis to respond to a design basis large break LOCA. The Surveillance should be continued for a minimum of 5 minutes in order to demonstrate that all starting transients have decayed and stability is achieved. The requirement to verify the connection and power supply of permanent and auto-connected loads shows the relationship of these loads to the EDG loading logic. In certain circumstances, many of these loads cannot actually be connected or loaded without undue hardship or potential for undesired operation. For instance, Emergency Core Cooling Systems (ECCS) injection valves are not desired to be stroked open, high pressure injection systems are not capable of being operated at full flow, and Shutdown Cooling (SDC) systems performing a decay heat removal function are not desired to be realigned to the ECCS mode of operation. In lieu of actually connecting and loading of loads, tests that adequately show the capability of the EDG system to perform these functions are acceptable. This testing may include any series of sequential or overlapping steps so that the entire connection and loading sequence is verified. The surveillance is performed when the plant is shutdown on a normal refueling interval.

SR 3.8.1.12 - EDG start verification on ESF actuation

This surveillance demonstrates that the EDG automatically starts and achieves the required voltage and frequency within the specified time ([10] seconds) from the design basis actuation signal (LOCA signal) and operates for [5] minutes. This period provides sufficient time to demonstrate stability. SR 3.8.1.12.d and SR 3.8.1.12.e ensure that permanently connected loads and emergency loads are energized from the offsite electrical power system on an ESF signal without loss of offsite power. The requirement to verify the connection of permanent and auto-connected loads is intended to verify the EDG loading logic. In certain circumstances, many of these loads cannot actually be connected or loaded without undue hardship or potential for undesired operation. For instance, ECCS injection valves are not desired to be stroked open, high pressure injection systems are not capable of being operated at full flow, or SDC systems performing a decay heat removal function are not desired to be realigned to the ECCS mode of operation. In lieu of actual demonstration of connection and loading of loads, testing that adequately shows the capability of the EDG system to perform these functions is acceptable. This testing may include any series of sequential, overlapping, or total steps so that the entire connection and loading sequence is verified.

SR 3.8.1.16 - Restoration of offsite power following Loss of Offsite power verification

This surveillance ensures that the manual synchronization and automatic load transfer from the EDG to the offsite source can be made and that the EDG can be returned to ready to load status when offsite power is restored. It also ensures that the auto-start logic is reset to allow the EDG to reload if a subsequent loss of offsite power were to occur. The EDG is considered to be in ready to load status when the EDG is at rated speed and voltage, the output breaker is open and can receive an auto-close signal on bus undervoltage, and the load sequence timers are reset.

SR 3.8.1.18 - EDG Load sequencer interval verifications

Under accident [and loss of offsite power] conditions loads are sequentially connected to the bus by the [automatic load sequencer]. The sequencing logic controls the permissive and starting signals to motor breakers to prevent overloading of the EDGs due to high motor starting currents. The [10]% load sequence time interval tolerance ensures that sufficient time exists for the EDG to restore frequency and voltage prior to applying the next load and that safety analysis assumptions regarding ESF equipment time delays are not violated.

SR 3.8.1.19 - EDG start verification on Loss of Off-site Power with ESF actuation

In the event of a DBA coincident with a loss of offsite power, the EDGs are required to supply the necessary power to ESF systems so that the fuel, RCS, and containment design limits are not exceeded.

This surveillance demonstrates the EDG operation, as discussed in the Bases for SR 3.8.1.11, during a loss of offsite power actuation test signal in conjunction with an ESF actuation signal. In lieu of actually connecting and loading of loads, testing that adequately shows the capability of the EDG system to perform these functions is acceptable. This testing may include any series of sequential or overlapping, steps so that the entire connection and loading sequence is verified.

2.3.2 Regulatory Guidelines

Regulatory Guide 1.174, July 1998, An approach for using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific changes to the Licensing Basis. (Reference 1)

This regulatory guide describes an acceptable approach for assessing the nature and impact of proposed licensing basis changes by considering engineering issues and applying risk insights. Assessments generally consider relevant safety margins and defense-in-depth attributes, including consideration of success criteria as well as equipment functionality, reliability, and availability. The analyses generally reflect the actual design, construction and operational practices of the plant. Acceptance guidelines for evaluating the results of such assessments are provided in this regulatory guide. This guide also address implementation strategies and performance monitoring plans associated with licensing basis changes that will help ensure that assumptions and analyses supporting the change are verified.

A typical approach to analyzing and evaluating proposed licensing basis changes include four elements:

1. Define the Proposed Change
2. Perform Engineering Analysis
3. Define Implementation and Monitoring Program
4. Submit Proposed Change

Element 1 involves three activities. First, identify those aspects of the plant's licensing bases that may be affected by the proposed change. This includes but is not limited to rules and regulations, final safety analysis report, technical specifications, licensing conditions, and licensing commitments. Second, identify all structures, systems, components procedures and activities that are covered by the licensing basis change being evaluated and should consider the original reasons for including each program requirement. Third, identify available engineering studies, methods, codes, applicable plant specific and industry data and operational experience, PSA findings, and research and analysis results relevant to the proposed licensing basis change.

Element 2 involves the expectation that the scope and quality of the engineering analyses conducted to justify the proposed licensing basis change will be appropriate for the nature and scope of the change. Appropriate consideration is typically given to uncertainty in the analysis and interpretation of findings and to use judgement on the complexity and difficulty of implementing the proposed licensing basis change to decide upon appropriate engineering analyses to support regulatory decisionmaking. Consideration is typically given to the appropriateness of qualitative and quantitative analyses, as well as analyses using traditional engineering approaches and those techniques associated with the use of PSA findings.

Element 3 describes the consideration that is typically given to implementation and performance-monitoring strategies. The primary goal for element 3 is to ensure that no adverse safety degradation occurs because of the changes to the licensing basis.

Element 4 involves the submittal of the proposed change. Request for proposed changes to the plant's licensing basis typically take the form of requests for license amendments (including changes to or

removal of license conditions), technical specification changes, changes to or withdrawals of orders and changes to programs pursuant to 10 CFR 50.54 (e.g. QA program changes under 10 CFR 50.54(a)).

Regulatory Guide 1.177, An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications (Reference 2)

This regulatory guide describes methods acceptable to the NRC staff for assessing the nature and impact of proposed technical specification changes by considering engineering issues and applying risk insights. Recommendations are provided for utilizing risk information to evaluate changes to nuclear power plant technical specification allowed outage times and STIs in order to assess the impact of such proposed changes on the risk associated with plant operation.

A typical approach to integrated decisionmaking for TS changes include four elements:

1. Define the Proposed Change
2. Perform Engineering Analysis
3. Define Implementation and Monitoring Program
4. Submit Proposed Change

Element 1 states that the licensee needs to identify the particular TS that are affected by the proposed change and identify available engineering studies (e.g. topical reports), methods, codes and PSA studies that are related to the proposed change.

Element 2 considers how the plant and industry operating experience relates to the proposed change, and whether potential compensatory measures could be taken to offset any negative impact from the proposed change.

Risk informed evaluations of the proposed change are typically performed to determine the impact on plant risk. This evaluation considers the specific plant equipment affected by the proposed TS changes and the effects of the proposed change on the functionality, reliability and availability of the affected equipment. The scope and level of detail necessary for the analysis depends upon the particular systems and functions affected.

The rationale that supports the acceptability of the proposed changes by integrating probabilistic insights with traditional consideration to arrive at a final determination of risk is usually provided. This determination typically considers continued conformance to applicable rules and regulations, the adequacy of the traditional engineering evaluation of the proposed change and the change in plant risk relative to acceptance guidelines. These areas are typically addressed before the change is considered acceptable.

Element 3 is to ensure that no adverse safety degradation occurs because of the TS changes and that the engineering evaluation conducted to examine the impact of the proposed changes continues to reflect the actual reliability and availability of TS equipment that has been evaluated.

Element 4 involves documenting the analyses and submitting the license amendment request.

Industry Standards and Guides

ASME OM-S/G-2000, Standards and Guides for Operation and Maintenance of Nuclear Power Plants. (Reference 4) - Part 15, Performance Testing of Emergency Core Cooling Systems in Pressurized Water Reactor Power Plants.

This part of the ASME code establishes the requirements for inservice testing to assess the operational readiness of Emergency Core Cooling Systems (ECCS), including those systems required for long-term decay heat removal, used in PWRs. It establishes test methods, test intervals, parameters to be measured and evaluated, acceptance criteria, corrective actions, and records requirements for the purpose of assessing integrated system performance. Inservice testing is required to be conducted at a 5-year +/- 25% time interval, with certain exceptions as stated in the guide. In addition, applicable portions of the guide must be performed prior to returning a system to service following replacement, repair, maintenance, or modification to ECCS components or to systems that could affect the ability to meet system performance requirements as defined in the guide.

Related ESFAS CEOG Reports

CEN-327-A, RPS/ESFAS Extended Test Interval Evaluation. (Reference 5)

This report provides a basis for requesting changes to the Technical Specification surveillance testing requirement for selected components in the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). CEN-327-A presents an analysis to justify the extension of the channel functional and logic unit surveillance test intervals from 30 days to 60 days and 90 days for selected RPS parameters and from 30 days to 90 days for ESFAS actuation logic. Subsequently, Supplement 1 to CEN-327 was submitted and presents a re-evaluation of the RPS to justify a ninety (90) day test interval (for all RPS parameters) with sequential testing. These analyses evaluated the impact of the proposed extended test intervals on core melt frequency and system unavailability to demonstrate that the proposed changes did not increase the plant risk when compared with the current technical specifications requirements.

CEN-403, ESFAS Subgroup Relay Test Interval Extension (Reference 6)

This report justifies extending the ESFAS subgroup relay STI for Combustion Engineering (CE) Nuclear Steam Supply System (NSSS) plants. The study looked at the performance of these relays in plants with CE designed NSSS from different perspectives. The original CEN-403 looked at all relays generically, where Revision 1 of CEN-403 differentiates between rotary relays and other mechanical type relays.

Based on the findings in this document, it was recommended that the surveillance test interval for each ESFAS subgroup relay at any CE NSSS unit that was previously tested at an interval of less than the duration of a fuel cycle interval be extended to that longer interval. For those ESFAS subgroup relays that were gaining an STI extension, those relays that are testable at power should be tested on a staggered test basis to provide means for detecting common mode failure mechanisms. The proposed extension of STIs was based on the over testing of plant equipment from this surveillance, the potential for inadvertent ESF actuations, and the demonstrated reliability of ESFAS subgroup relays.

3.0 BACKGROUND

3.1 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS) SYSTEM DESCRIPTION

The safety-related instruments and controls of the Engineered Safety Features (ESF) Systems are those of the Engineered Safety Features Actuation System (ESFAS). The ESFAS generates those signals that actuate the required Engineered Safety Features Systems. ESFAS consists of electrical and mechanical devices and circuitry, from sensors to actuation device input terminals.

The ESFAS designs at plants with CE supplied NSSS can be divided into three groups. They are:

1. Plants with a non-CE ESFAS design with relay logic
2. Plants with a non-CE ESFAS design with solid state logic
3. Plants with an ESFAS designed by CE.

The first group of plants includes Palisades and Fort Calhoun. The second group includes Calvert Cliffs Units 1 and 2, Millstone Unit 2, and St. Lucie Units 1 and 2. The third group includes Waterford-3, ANO-2, San Onofre Units 2 and 3, and Palo Verde Units 1, 2 and 3. The primary difference between the groups is in the manner of processing the instrument signals from the field.

All systems implement the same regulatory requirements with respect to mitigating system action. There are differences in what is measured and what is the proper mitigation at each plant. But the processing of the signals and the actuation of equipment is common to all the plants.

All systems typically require 2 out of 4 parameters to be beyond setpoint to cause ESFAS.

All systems allow one measurement channel to be bypassed, leaving a 2 out of 3 condition to cause an ESFAS.

All systems allow for one measurement channel to go into test, leaving a 1 out of 3 condition to cause an ESFAS.

The later vintage plant designs combined RPS and ESFAS measurement channels. The older plants have a set of 4 pressurizer pressure channels feeding the EFSAS logic and another four feeding RPS logic. The later plant designs have only one set of four pressurizer pressure channels. Circuits in the later design PPS cabinet cause both an ESFAS output relay actuation as well as a reactor trip (interrupting power to the reactor trip breakers).

When plant PSA models include this level of detail, they show a dependency between ESFAS and mitigating systems, e.g. ESFAS starts of a HPSI pump. It is unusual to model the instrument strings corresponding to the bistable inputs. It is typical to show the dependency the ESFAS decision logic has on its power supplies.

3.1.1 Non-CE ESFAS Design

For non-CE ESFAS designs, the ESFAS consists of sensors and logic circuits which monitor selected plant parameters and provide an actuating signal to start the appropriate engineered safety features equipment when needed. In general, the ESFAS includes the following actuation signals:

1. Safety Injection Actuation Signal (SIAS)
2. Containment Spray Actuation Signal (CSAS)
3. Containment Isolation Actuation Signal (CIAS)
4. Recirculation Actuation Signal (RAS)
5. Steam Generator Isolation Signal (SGIS)
6. Auxiliary Feedwater Actuation Signal (AFAS)

A plant specific description of each of the above signals is presented in the FSARs (Reference 8, 9, 10, 11 and 12) for those plants that utilize the non-CE ESFAS design. Additional ESFAS system description is included in Section 2.0 of the plant specific Appendices of this document. The following paragraphs provide a brief comparison of the non-ESFAS designs.

In general, each ESFAS signal consists of four redundant measurement channels and two redundant actuation channels. Independence is provided between redundant channels to accomplish decoupling of the effects of unsafe environmental factors, electrical transients, and to reduce the likelihood of interactions between channels during maintenance operations or channel malfunction. Independence is obtained by electrical isolation and physical separation between redundant channels.

Fort Calhoun/Palisades – (non-CE ESFAS design with relay logic)

The Fort Calhoun-style simply tests for two-of-four signals being at or beyond a setpoint value (or for some reason out-of-service) using electromechanical relays. Fort Calhoun is the first of the CE plants to have the ESFAS in a specific control room cabinet. Although functionally, very similar, Palisades does not have an ESFAS cabinet otherwise typical of a CE plant. The Fort Calhoun design cleanly separates the process parameters of interest to ESFAS away from the electromechanical relays that bring the mitigating equipment on-line.

Palisades panel instruments (i.e. gauges) include a bistable that de-energizes an electromechanical relay involved in the two-out-of-four channel comparison logic. At Palisades, the ESFAS two-out-of-four logic is made from two-pairs of contacts from each process parameter channel. The arrangement accomplishes what is called ladder-logic at the more modern plants. Fort Calhoun is the first of the CE plants to examine analog sensor output versus a fixed signal in a separate bistable device.

At Palisades, there are multiple sets of actuation relays, e.g. a set of SIAS actuation relays derived from pressurizer low-pressure. At the Calvert-Cliffs-style and Waterford-style plants, there is a layer of abstraction between the bistable devices and the devices that actuate equipment that allows the plant to have a small set of equipment actuation relays.

In this early ESFAS design, there are four channels of electric power, one for each measurement channel. However, there are fundamentally only two actual sources of power (i.e. two channels have common components up to a point in the design).

At Palisades, the sequencing of loads in response to an undervoltage condition is done with digital programmable logic controllers rather than electromechanical relays as at the other CE plants.

Fort Calhoun requires electric power in the ESFAS scheme in order to actuate ECCS. Late designs are set up so that a lack of channel power would be as if a parameter exceeded a setpoint.

Calvert Cliffs / Millstone-2 / St. Lucie -- (non-CE ESFAS design with solid state logic)

Four instrument strings for each of ESFAS parameter feed the bistable decision logic. The bistable section of ESFAS compares the input signal to a setpoint and causes downstream contacts to open upon exceeding a setpoint. To assure that no single failure inadvertently actuates the ESFAS equipment, decision logic in the actuation cabinets only react when at least two bistables for the same parameter exceed the setpoint. The polling for multiple instruments measuring the same parameter as beyond the setpoint is done on with solid-state components, rather than the ladder-logic in the Waterford-style.

The Calvert Cliffs-style splits the power supply for ESFAS into four uninterruptible power-supply trains.

3.1.2 CE ESFAS Design

For the CE ESFAS design, the ESFAS consists of sensors, logic and actuation circuits which monitor selected plant parameters and provide an actuating signal to each actuated component in the Engineered Safety Features System required to be actuated. There is one actuation signal for each of the ESF System functions. Each actuation signal is identical except that specific inputs and logic vary from system to system and the actuated devices are different. The following actuation signals are generated by the ESFAS when the monitored variable reaches the levels that are indicative of conditions which require protective actions:

1. Containment Isolation Actuation Signal (CIAS)
2. Containment Spray Actuation Signal (CSAS)
3. Main Steam Isolation Signal (MSIS)
4. Safety Injection Actuation Signal (SIAS)
5. Recirculation Actuation Signal (RAS)
6. Emergency (Auxiliary) Feedwater Actuation Signal (EFAS/AFAS)

Four redundant measurement channels with electrical and physical separation are provided for each signal used in the direct actuation of an ESF System. A two-out-of-four coincidence of like parameter signals is required to actuate any of the ESFAS signals which in turn actuates an ESF System. The fourth channel is provided as a spare and allows bypassing one of channel while maintaining a two-out-of-four system. A plant specific description of each of the above signals is presented in the FSARs (Reference 13, 14, 15 and 16) for those plants that utilize the CE ESFAS design. A more detailed system description is included in each plant-specific Appendix (Section 2.0).

San Onofre / Waterford / Palo Verde -- (ESFAS designed by CE)

The Waterford-style is the most complex of the three, but also the most flexible in terms of testing and maintenance. The Waterford-style splits the power supply for ESFAS into effectively four trains. In the Waterford-style, the coincidence logic is carried out by electromechanical relays.

The measurement channels which generate low pressurizer pressure and high containment pressure signals for the SIAS also provide signals to the CIAS and CSAS.

Process measurement channels perform the following functions:

- Continuously monitor pressurizer pressure and containment pressure.
- Provide indication of operational availability of each sensor to the operator.

- Transmit analog signals to bistables within the ESFAS initiating logic.

The parameters are measured with four independent process instrument channels. The measurement channels consist of instrument sensing lines, sensors, transmitters, power supplies, isolation devices, indicators, computer inputs, current loop resistors and interconnecting wiring.

Each measurement channel is separated from the other like measurement channels to provide physical and electrical isolation of the signals to the ESFAS initiating logic. The output of each transmitter is a current loop. Signal isolation is provided for computer inputs. Each channel is powered by a redundant 120 volt vital ac distribution bus.

The initiating logic consists of bistables, bistable output relays, trip relays, matrix relays, initiation channel output relays, manual block controls, block relays, manual testing controls, indicating lights, power supplies and interconnecting wiring.

The initiating logic is physically located in the PPS cabinet.

Signals from the protective measurement channels connect to voltage comparator circuits (bistables). They compare the input signals to predetermined setpoints. Whenever a channel parameter reaches the predetermined setpoint, the channel bistable deenergizes the bistable output relay. The bistable output relay deenergizes the trip relays. Contacts of the trip relays form the SIAS initiating logic. Each set of trip relays (i.e. each channel) is powered from a redundant 120-volt vital ac distribution bus. The bistable setpoints are adjustable from the front of the PPS cabinet. Access is limited by means of a key-operated cover, with an annunciator indicating cabinet access. All bistable setpoints are capable of being read out on a meter located on the PPS cabinet and are sent to the plant-monitoring computer.

The initiation signals are generated in four channels, designated A, B, C and D. Two-out-of-four coincidence of initiating signals from the four protective measurement channels generates all four initiation signals.

Each initiation logic consists of a set of six logic matrix relay contacts in series, a power supply for the set of contacts and the initiation logic relays. The function of each initiation logic is to send a signal to the actuation logic if the selected plant parameter (or combination of parameters) reaches the trip condition. Each initiation logic interfaces with each logic matrix via the logic matrix relay contacts and with each actuation logic via the initiation relay contacts. The interface with the actuation logic is arranged in a manner which produces a selective two-out-of-four coincidence circuitry. Each initiation logic also interfaces with one of the four vital buses. The operator interfaces with initiation logic for testing, maintenance and initiation of a signal to actuate the actuation circuitry.

Each actuation logic consists of a set of four initiation logic relay contacts, two manual trip buttons, and a group of actuation relays. The initiation logic relay contacts are arranged in a manner which forms a selective two-out-of-four coincidence circuitry. The manual trip buttons are also arranged in a manner which requires both buttons to be depressed to manually actuate the actuated ESF System components. The group relays, which are included in the actuation circuitry, are used to actuate the individual ESF System. Components which should be actuated mitigate the consequences of the occurrence which caused the ESFAS. The actuated ESF System components generally consists of solenoid operated valves, motor operated valves or motors of pumps.

Each actuation logic interfaces with each of the initiation logic via the initiation logic relay contacts and with the individual actuated ESF System component via the group relay contacts.

The actuating logic is physically located in two ESFAS auxiliary relay cabinets. One cabinet contains the logic for ESF train A equipment, while the other cabinet contains the logic for ESF train B equipment.

4.0 APPROACH AND METHODOLOGY

4.1 OVERVIEW

This report demonstrates that changing the integrated Engineered Safety Features (ESF) test from once per refueling cycle on a sequential basis to once refueling every other cycle on a staggered basis results in a negligible change in risk. Currently, integrated ESF testing on both safeguards trains is performed each refueling cycle to satisfy Technical Specifications (TSs) surveillance requirements. The basic premise of the project was that the effect of this change in test frequency on risk is negligible because the integrated ESF test is not the primary/sole operability test for the majority of the components tested. Other surveillance tests are performed on many of these components and functions on the same or a more frequent basis. Therefore, there is considerable overlap between other tests and the integrated ESF test.

To document the overlap in testing, a systematic review of the integrated ESF test procedure was performed for each plant in order to identify all of the components and functions tested by the integrated ESF test. Then, other TS surveillances that test the same components were also reviewed for overlap. The result was a complete listing of the components and functions tested only by the integrated ESF test and a matrix that mapped the integrated ESF test to other tests to illustrate the amount of overlap.

Changes in the test interval for the integrated ESF test will have no effect on the reliability (or failure probability) of the components and functions which are tested more frequently by other tests. Increasing the test frequency would be expected to reduce the reliability (increase the failure probability) for those components and functions that are tested only by the integrated ESF test. Plant PSA models were reviewed to determine if and how these components and functions were addressed. In some cases, a deterministic rationale could be established for excluding the components or functions from the PSA model. Where this was not possible, the appropriate event frequencies in the PSA model were revised to account for the proposed change in the test frequency. In some cases, the model itself had to be revised in order to include the effect of changing the test frequency.

The effect of the proposed change in the integrated ESF test interval on risk was assessed by comparing the risk measures (CDF and LERF) as determined by analyses using PSA models at individual plants, and by the requantification of the revised model.

4.2 PROCEDURE REVIEW PROCESS

4.2.1 Functions Tested by the Integrated ESF Test

A systematic review of the integrated ESF test procedures for each unit was performed in order to identify all of the components tested by the integrated ESF test and the functions tested. The functions relate to specific TS surveillance requirements, test objectives and acceptance criteria. A separate review was performed for each plant because the test objectives and specific functions vary from one unit to the next.

The integrated ESF test is currently performed on both safeguards trains every normal refueling outage. Although the details vary by plant, the test is typically initiated by simulating a loss of offsite power on an emergency bus, and either simulating or manually actuating the SIAS actuation.

The test objectives typically include:

- EDG automatic start on UV and SIAS
- Load shedding
- EDG sequencer loading functions

- SIAS actuation verifications
- Response times associated with EDG starting and load sequencing

Table 4.2-1 shows a comparison of the functions tested by the integrated ESF test at each reviewed plant. The shaded areas show the functions specifically addressed by this report. Note that EDG testing as related to Loss-of-Power (LOP) events (with or without ESF actuation), automatic start verification, load shedding and sequencing was included in the review.

4.2.2 Diesel Generator Testing Included in the Integrated ESF Test

Some utilities have included additional EDG testing in the integrated ESF test when it makes sense to do so. This is done in an effort to minimize EDG wear and tear by limiting the number of times the EDG must be started for test purposes. A list of these tests is shown in Table 4.2-2. Note that changing the surveillance interval for these additional EDG tests is not within the scope of this report.

4.2.3 Review and Overlap with Other ESF Surveillance Tests

Once the integrated ESF test procedure was reviewed and the components being tested and function identified, other surveillances testing the same component were reviewed. These test procedures were used to identify other TS surveillance tests that overlap the integrated ESF test. An overlapping test is defined as one that tests the same component and function as the integrated ESF test at the same or greater frequency. Examples of overlapping tests include quarterly ISI/IST tests on valves and pumps; and quarterly ESFAS logic and relay testing.

Table 4.2-1
Functions Addressed by Integrated ESF Testing

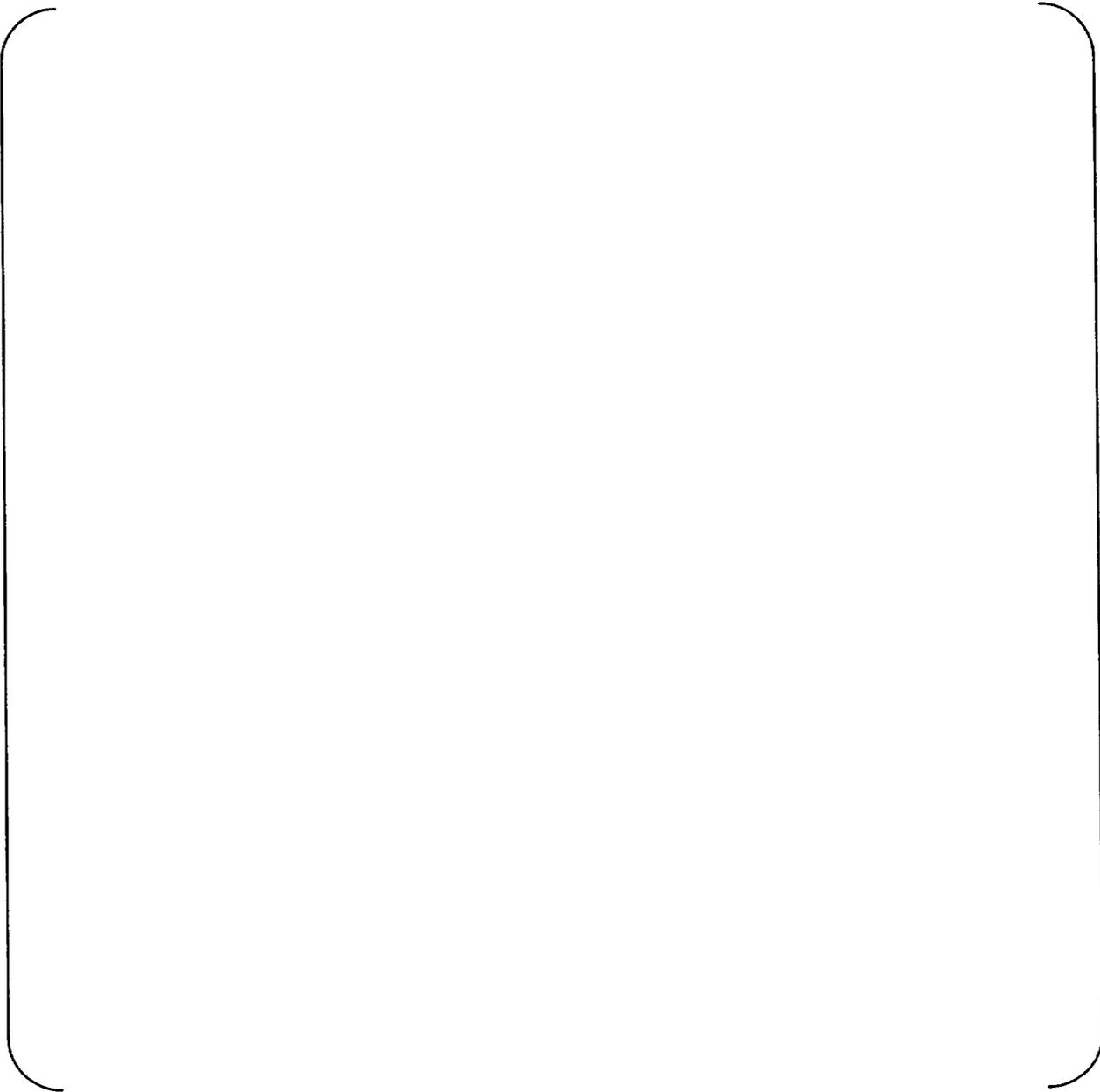


Table 4.2-2
Emergency Diesel Generator Testing Included in the Integrated Safeguards Tests
(Change In Test Frequency Not Proposed for these Functions)



4.2.4 Procedure Review Results

The procedure review process resulted in a matrix listing all the components and functions tested by the integrated ESF test. The matrix also includes other surveillance tests that were identified to test the same component or function. In addition to the matrix, a series of schematics was created to illustrate the overlap in testing. Note that these schematics are simplified illustrations and therefore depict only a rough approximation of overlap. They are not intended to provide engineering and system design detail. Figures 4.2-1 through 4.2-6 illustrate the overlap in ESF testing at Calvert Cliffs Units 1 and 2. A similar set of plant-specific schematics are included in the appendices for other utilities. They are included here for illustration purposes only. The figures start with the basic components of the logic path from the sensor to the end equipment. Then the tests covering various components in the string were added. Figures 4.2-1 through 4.2-4 address testing associated with SIAS, CIS, CSAS and RAS actuation. Figure 4.2-5 covers Under Voltage (UV) sensing. Figure 4.2-6 covers EDG load sequencers. The equivalent test procedures referenced in these figures are included in the plant-specific matrix and mapped to specific components tested by the integrated ESF test. This information was used to categorize each component in one of three basic categories (A, B or C). The initial categorization was further developed following an initial PSA assessment of the Category A and B components. The categorization process is described in detail in Section 4.3. Categorization was done using surveillance procedures, the list of basic events from the PSA, the Generic Letter 96-01 evaluations and responses as well as selected plant drawings (primarily electrical one-lines and P&IDs).

Figure 4.2-1
SIAS Actuation Testing at Calvert Cliffs Units 1 and 2



Figure 4.2-2
CIS Actuation Testing at Calvert Cliffs Units 1 and 2



Figure 4.2-3
CSAS Actuation Testing at Calvert Cliffs Units 1 and 2



Figure 4.2-4
RAS Actuation Testing at Calvert Cliffs Units 1 and 2



Figure 4.2-5
Undervoltage Sensing Testing at Calvert Cliffs Units 1 and 2



Figure 4.2-6
EDG Sequencer Testing at Calvert Cliffs Units 1 and 2



4.3 COMPONENT SCREENING AND PRELIMINARY CATEGORIZATION PROCESS

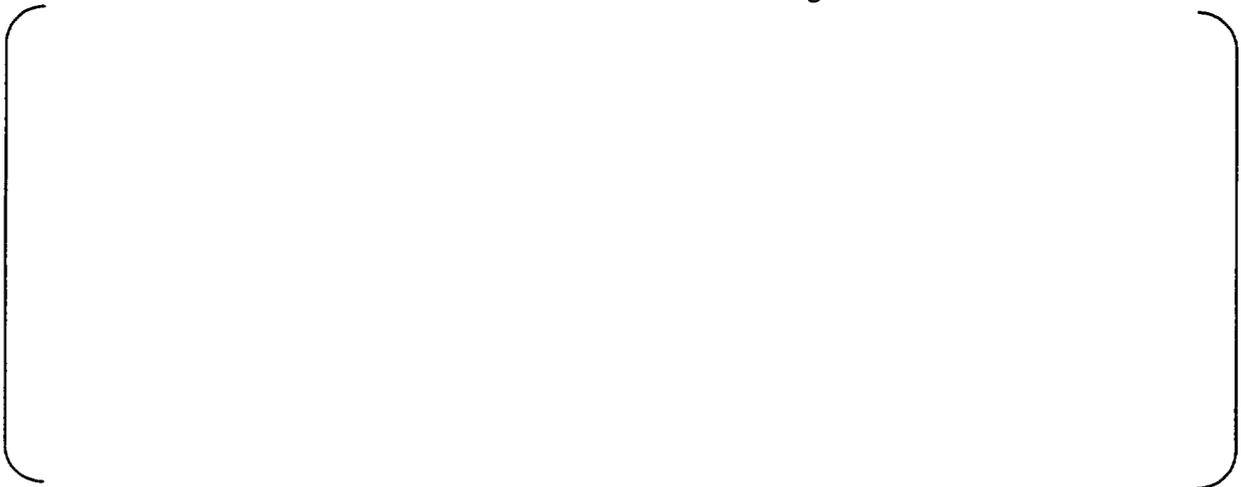
4.3.1 Category Definitions

As provided in the utility documentation for each unit, review of the surveillance procedures showed that many of the components tested by the integrated ESF test were also tested by other, more frequently performed tests. However, there were still many components tested only by the integrated ESF test. Therefore, a categorization process was developed and used to facilitate the evaluation of component testing and make recommendations for calculating the change in risk.

Figure 4.3-1 provides a graphical representation of this categorization process. The categorization is based on both the plant-specific procedure review described earlier in this report, and a review of the plant PSA. The three basic categories are defined as follows:

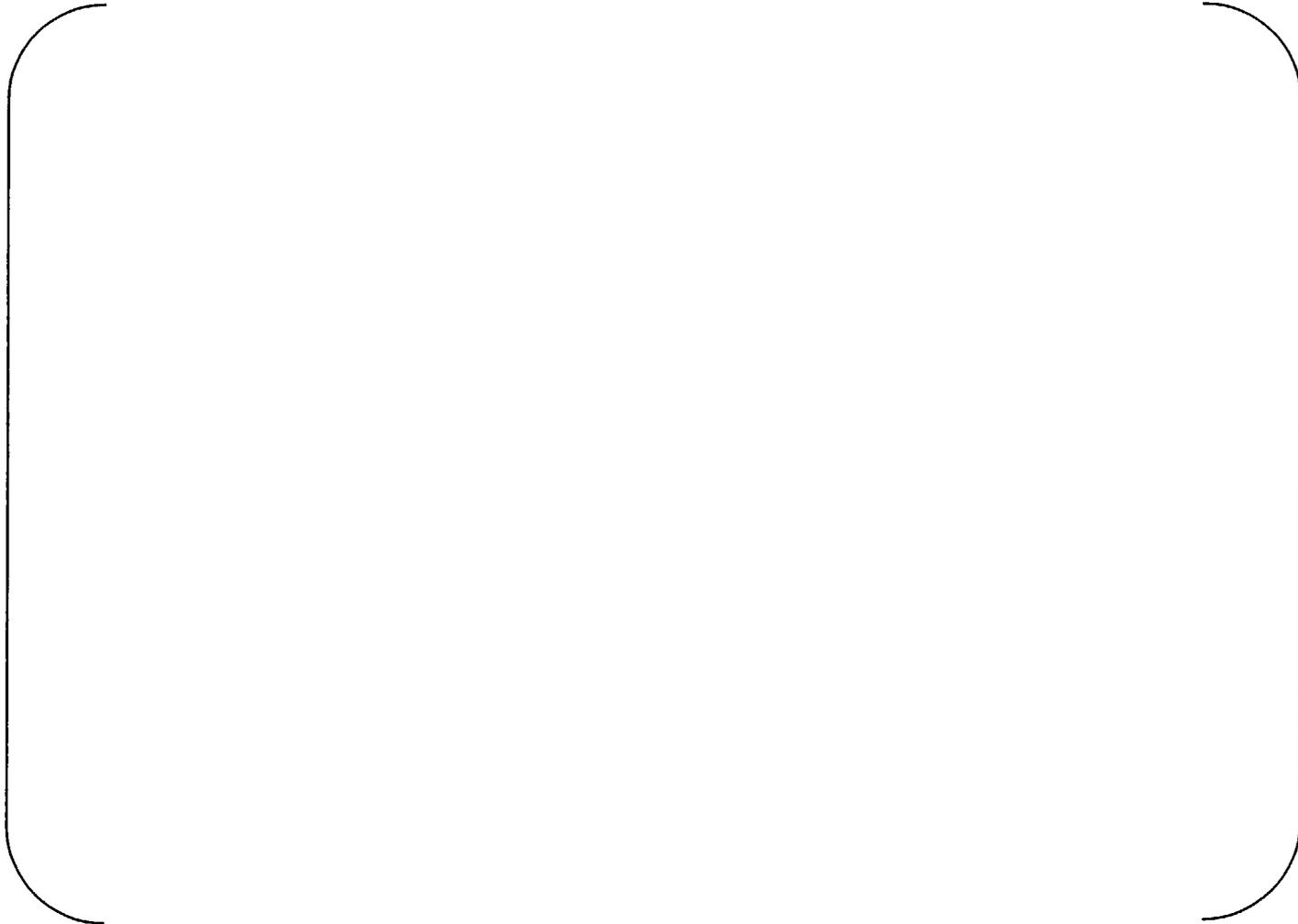
- Category A The integrated test is the sole / primary test which demonstrates the operability or function of these components. These components perform an engineered safety function. The PSA model addresses (or should address) failure of these components. They may be modeled explicitly, modeled via a subsuming component, or modeled via a surrogate event.
- Category B Similar to Category A, the integrated test is the sole / primary test which demonstrates the operability or function of these components. Unlike the Category A components, the Category B components are not included in the PSA model. Failure of these components therefore does not affect the calculated risk. The rationale for excluding them from the model is provided in the database. For example, valves which are normally in their safeguards-actuated position may not be modeled because the safeguards signal is "confirmatory" - the signal is necessary only if the event should occur while the associated system is in an unusual or infrequent configuration.
- Category C The integrated test is not the sole / primary test which demonstrates the operability or function of these components. Other, more frequently performed surveillance tests ensure that changes to the integrated ESF test frequency would not affect the failure probabilities for these components.

The Category A components were further divided into four sub-categories as follows:





**Figure 4.3-1
Component Categorization Process Flow Chart (Sheet 1)**



**Figure 4.3-1
Component Categorization Process Flow Chart (Sheet 2)**



4.3.2 Classification Results

Table 4.3-1 provides a numerical summary of the classification results for each unit. Note that for a given unit, the total number for all categories may be greater than the number of components; this is because a single component may be tested for more than one function. For example, there are many components which are tested to load shed on undervoltage, and then re-start when sequenced. The PSA model may address these functions differently, resulting in two subcategories for the single component.

**Table 4.3-1
Summary of Classification Results by Unit**

A large, empty rectangular area enclosed by a thin black line with rounded corners at the top and bottom. This area is intended for the content of Table 4.3-1 but is currently blank.

**4.4 GUIDELINES FOR PLANT SPECIFIC PSA MODEL ADJUSTMENTS AND
REQUANTIFICATION OF RISK**

4.4.1 Category A-1



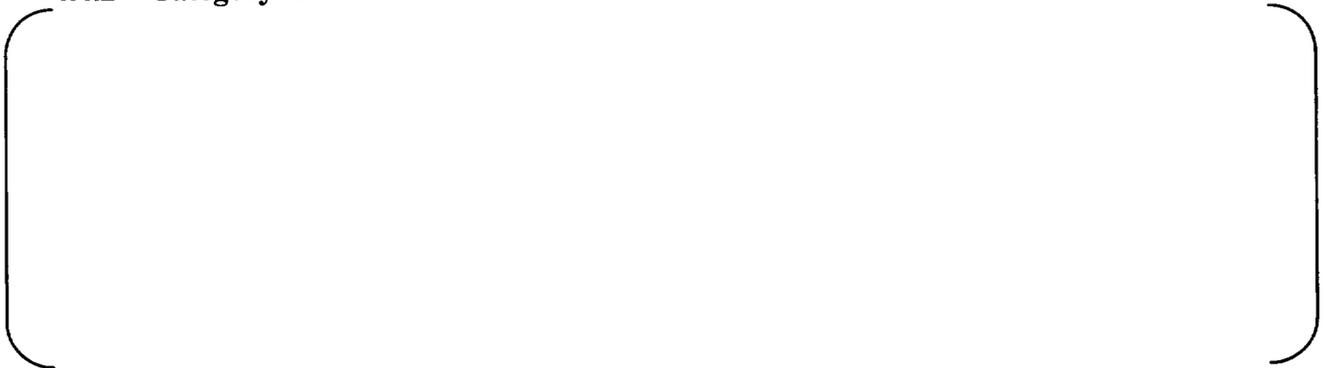
4.4.1.1 Standby-Time Dependent Events



4.4.1.2 Common Cause Factors



4.4.2 Category A-2



[]

4.4.3 Category A-3

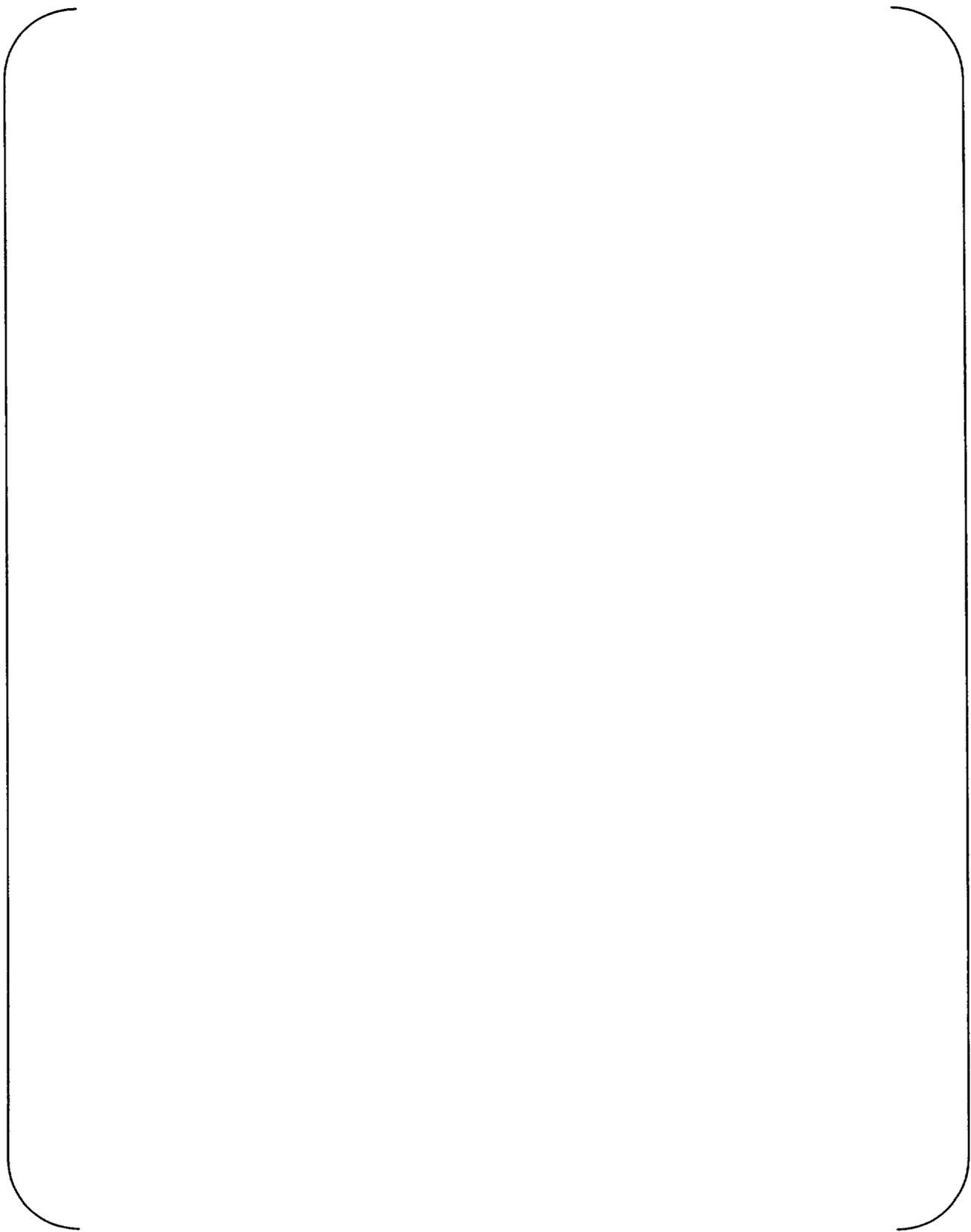
[]

4.4.4 Category A-4

[]

4.4.5 Category B

[]



4.5 COMMON CAUSE ADJUSTMENT WHEN INTRODUCING STAGGERED TESTING

4.5.1 Introduction



4.5.2 CCF for standby equipment

4.5.2.1 Derivation of Independent Failure-to-start Probability Model



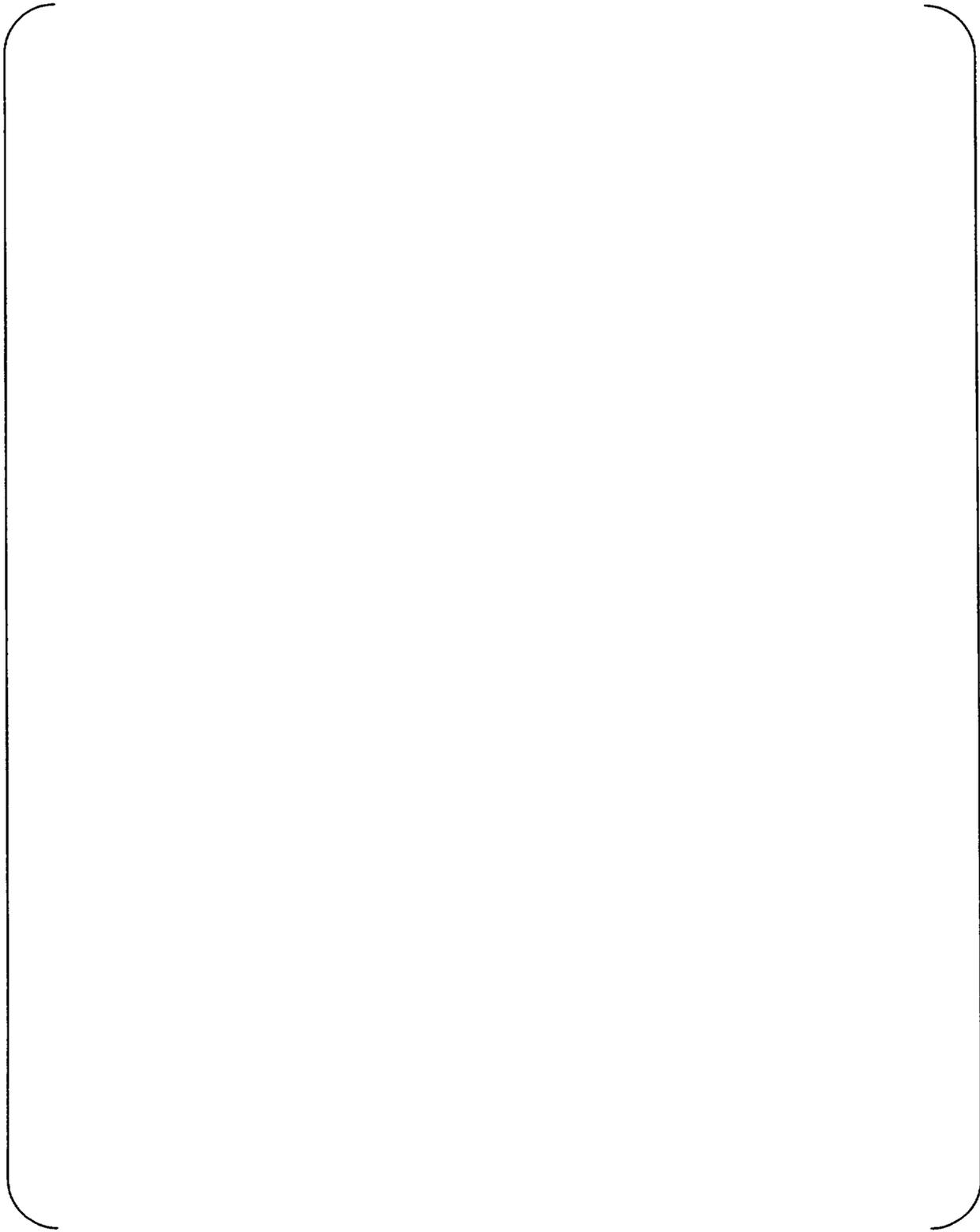
4.5.2.1.1 Standby model

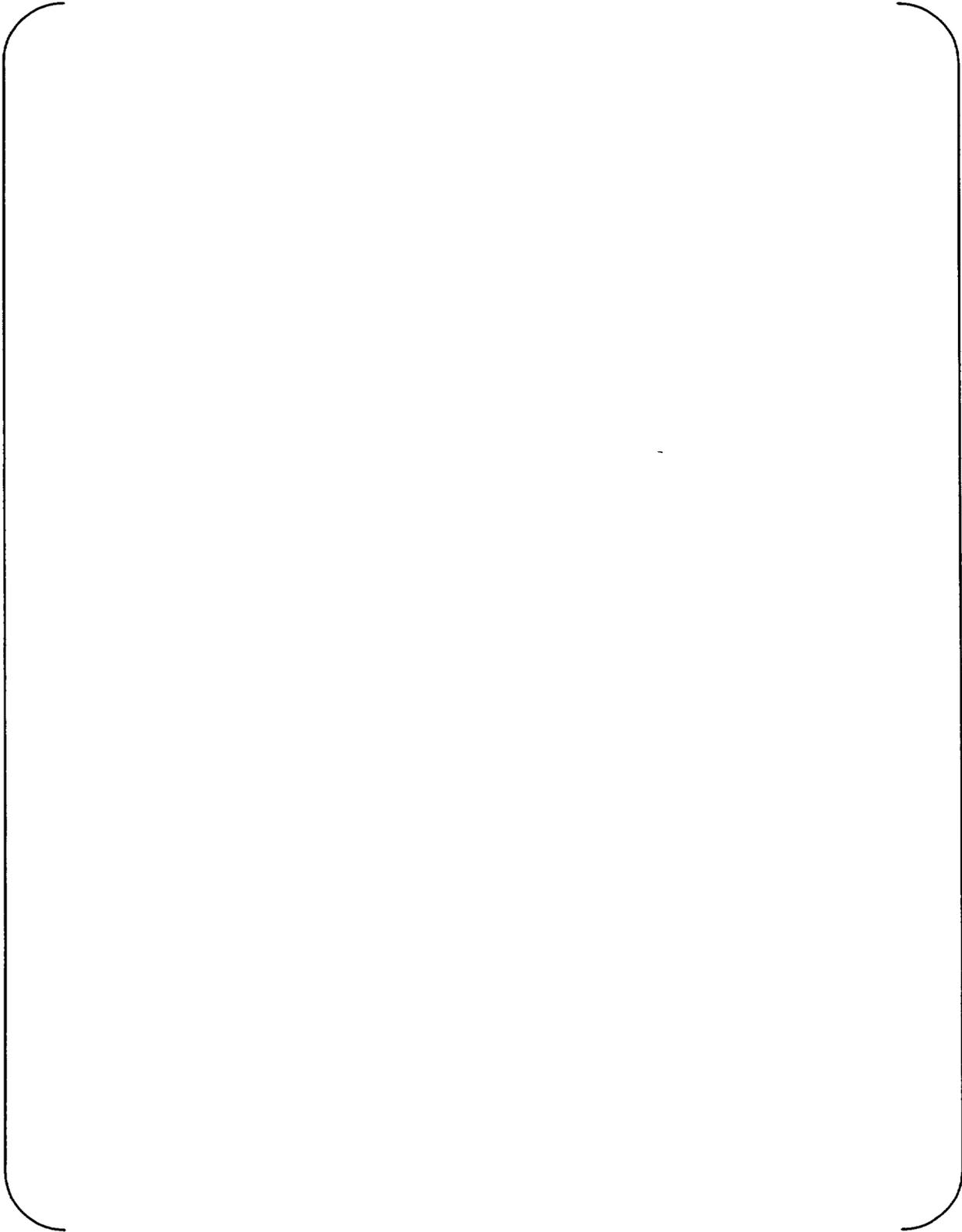


4.5.2.1.2 Inclusion of CCF under the standby regime



4.5.2.1.2 Adjusting failure-on-demand CCF to account for staggered test intervals under the standby regime





4.5.3 Conclusions

4.5.3.1 Fail to Run Common Cause Failure (CCF) Adjustment

4.5.3.2 Failure-on-demand CCF Adjustment

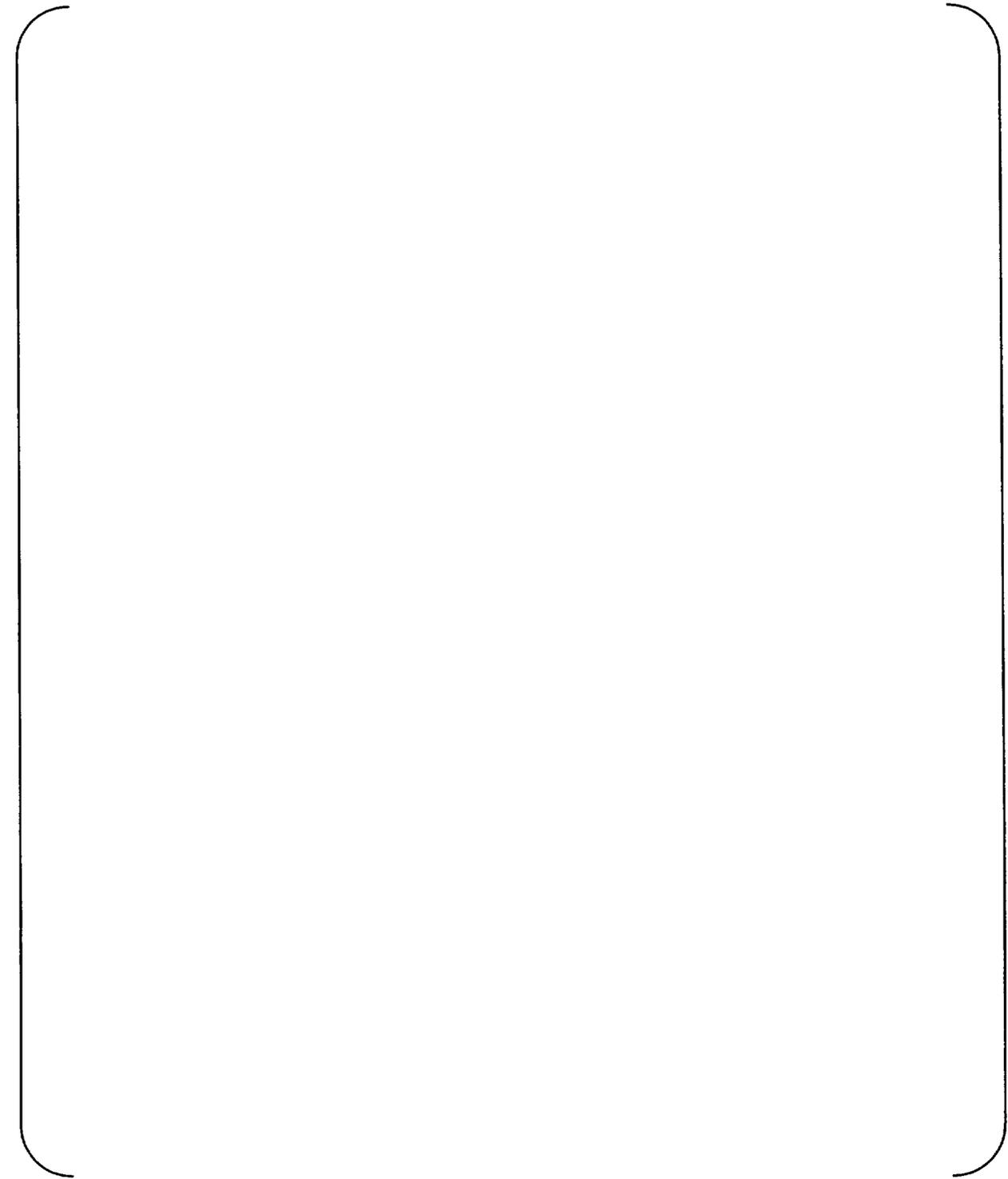
4.5.3.3 Standby Model

4.5.3.4 Binomial Model

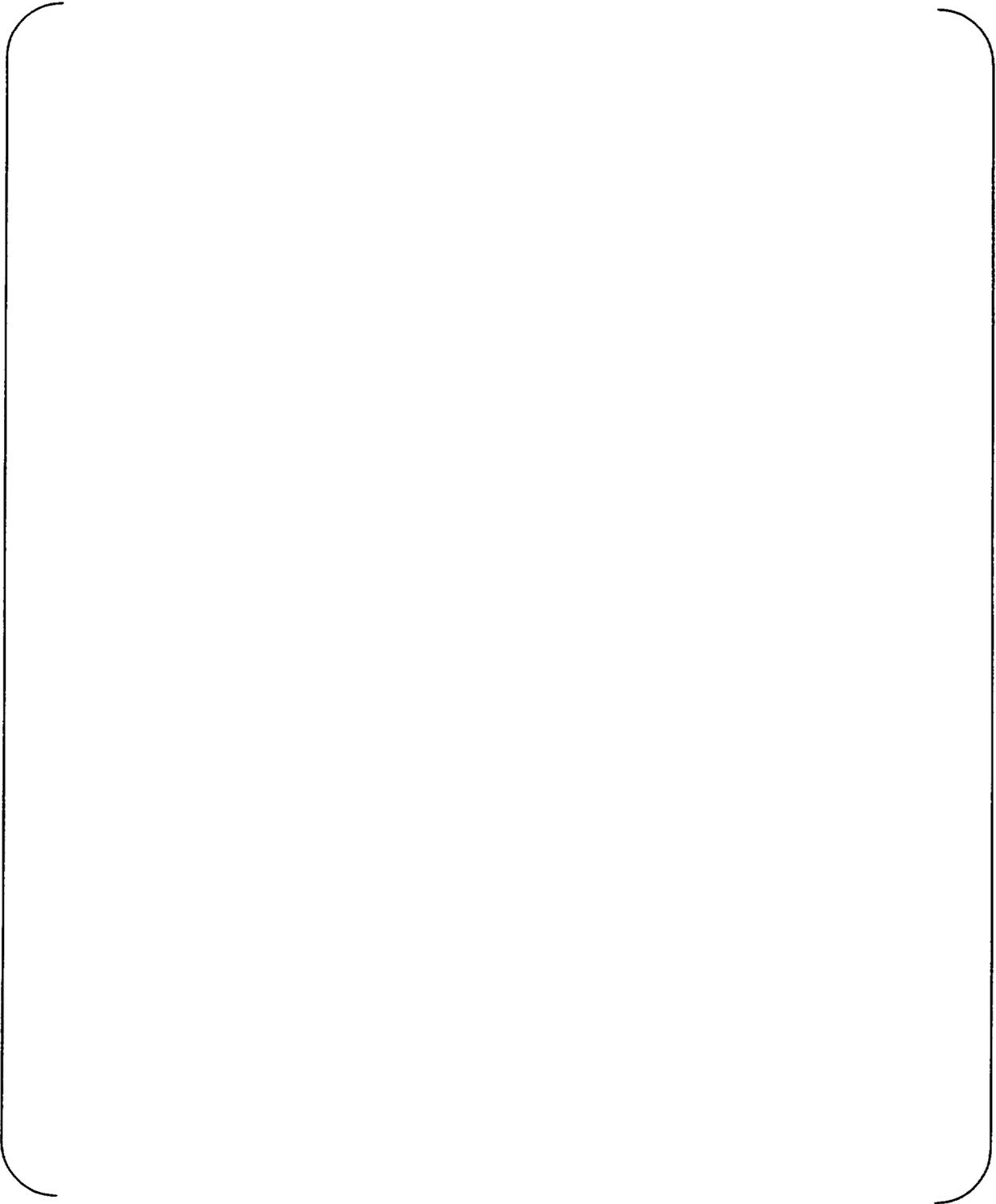
4.6 LOAD SHED AND BREAKER MODELING ISSUES AND CONSIDERATIONS

4.6.1 Breaker Modeling Issues

4.6.1.2 Safety-related Breakers



4.6.1.3 Non-Safety Related Breakers



5.0 TECHNICAL JUSTIFICATION

5.1 ASSESSMENT OF DETERMINISTIC FACTORS

5.1.1 Impact On Defense-In-Depth

The proposed change meets the defense-in-depth principle. The elements of defense-in-depth, and the impact of the proposed change on these elements follow.

- A reasonable balance among preventing core damage, preventing containment failure, and consequence mitigation is preserved.

The proposed STI change has only a small-calculated impact on CDF and LERF. The STI change does not affect containment integrity. The change neither degrades core damage prevention at the expense of containment integrity, nor does it degrade containment integrity at the expense of core damage prevention. The balance between preventing core damage and preventing containment failure is the same. Consequence mitigation remains unaffected by the proposed changes. Furthermore, no new accident or transient is introduced with the requested change, and the likelihood of an accident or transient is not impacted. Conversely, the increased STI may reduce the likelihood of a test-induced transient or accident. This last item is an unquantified benefit of the STI change.

- Over-reliance on programmatic activities compensates for weaknesses in plant design.

The plant design will not be changed to accommodate the proposed STI extension. All safety systems, including the ESFAS, will still function in the same manner with the same signals available to trip the reactor and initiate ESF functions, and there will be no additional reliance on additional systems, procedures, or operator actions. The calculated risk increase for these changes is very small and additional control processes are not required to compensate for any risk increase.

- System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system.

There is no impact on either the redundancy, independence, or diversity of the ESFAS or of the ability of the plant to respond to events with diverse systems. The ESFAS is a diverse and redundant sub-system and will remain so. There will be no change to the signals available to trip the reactor or initiate an ESFAS actuation.

- Defenses against potential common-cause-failures are maintained, and the potential for introduction of new common-cause-failure mechanisms have been assessed.

Defenses against common-cause-failures are maintained. The STI extension requested is not sufficiently long to expect new common-cause failure mechanisms to arise. In addition, the operating environment for these components remains the same, therefore no new common-cause-failure modes are expected. In addition, backup systems and operator actions are not impacted by these changes; and there are no common cause links between the ESFAS and these backup options.

- Independence of barriers is not degraded.

The barriers protecting the public and the independence of these barriers are maintained. With the extended STI, it is not expected that the plant will have multiple systems out-of-service

simultaneously that could lead to degradation of these barriers and an increase in risk to the public.

- Defenses against human errors are maintained.

No new operator actions related to the STI extension are required. No additional operating or maintenance procedures have been introduced, or have to be revised (except to note the new test frequency) because of the STI change and no new at-power test or maintenance activities are expected to occur as a result of the STI change

5.1.2 Impact On Deterministic Safety Margins

The safety analysis acceptance-criteria as stated in the Final Safety Analysis Report are not impacted by this STI change. Diversity with regard to signals, which provide reactor trip and actuation of engineered safety features, will also be maintained. The proposed STI change will not result in plant operation different from the design basis safety-limits and margins described in other submittals. All signals credited as primary or secondary and all operator actions credited in the accident analysis will remain the same.

5.2 ASSESSMENT OF RISK FACTORS

Five plants completed a plant specific risk analysis to determine impact of the integrated ESF test change from once per cycle on a sequential basis to once every other cycle on a staggered basis. The results of the analyses are shown in Table 5.2-1. ANO-2 did not need to perform a risk analysis because all components covered by integrated ESF testing were also tested by other required tests that had a test frequency of once per cycle or more frequently. Component reliability was not affected by the proposed change.

**Table 5.2-1
Results from Sequential to Staggered Integrated ESF Testing**

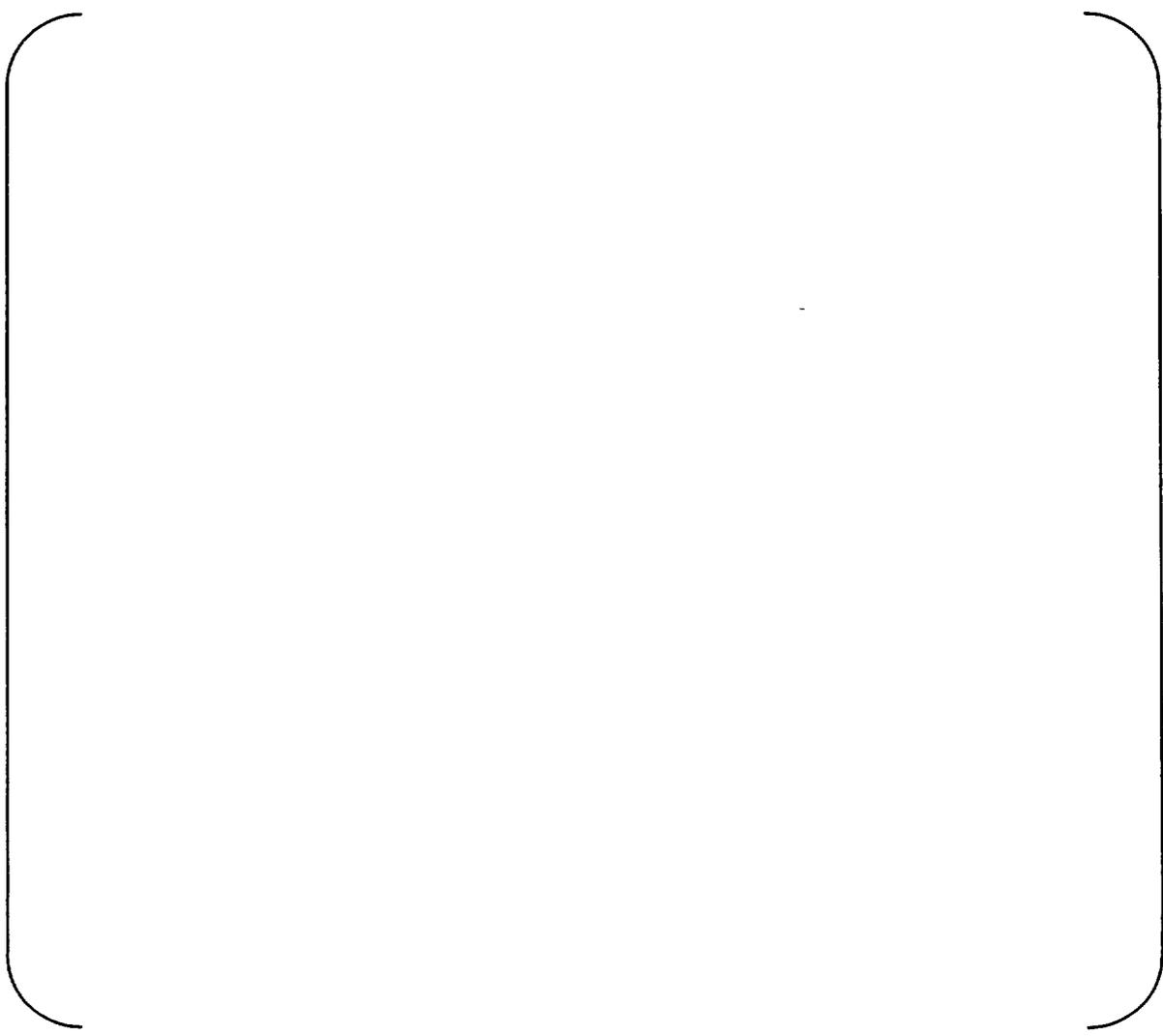


5.2.1 Process Summary

5.2.1.1 Categorization of Components

As discussed previously in Section 4.3, the first main step was to identify all of the components that were tested by the integrated ESF test. This was done by reviewing the integrated ESF test procedures for each participating plant to identify the components that were covered by the integrated ESF for each plant.

The second main step was to review the test procedures for other tests to determine if these tests covered any of the components covered by the integrated ESF test. The criteria were: (1) that the tests had to be tests that were required by the Technical Specifications (TS) and not purely under administrative control, and (2) that the test frequency had to be once per cycle or less (i.e. quarterly or semi-annually). Based on this review and comparison, the list of components covered by the integrated ESF test was parsed into three categories. The main category of interest was components for which the integrated ESF test is the sole/primary test for operability or functionality (Category A). Category A components were further divided into four sub-categories to address the impact of the change in risk.



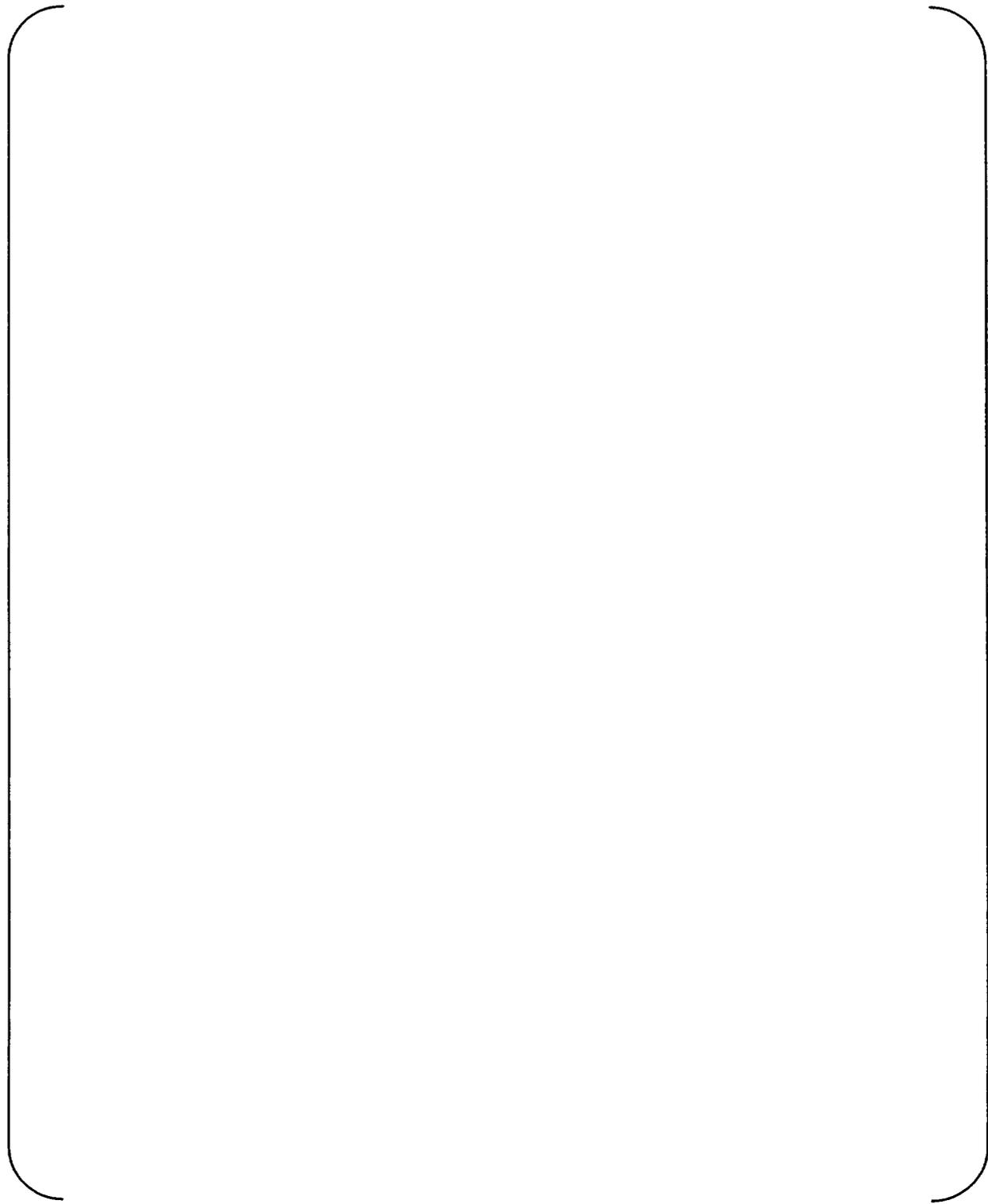
5.2.1.2 Base Case Modification

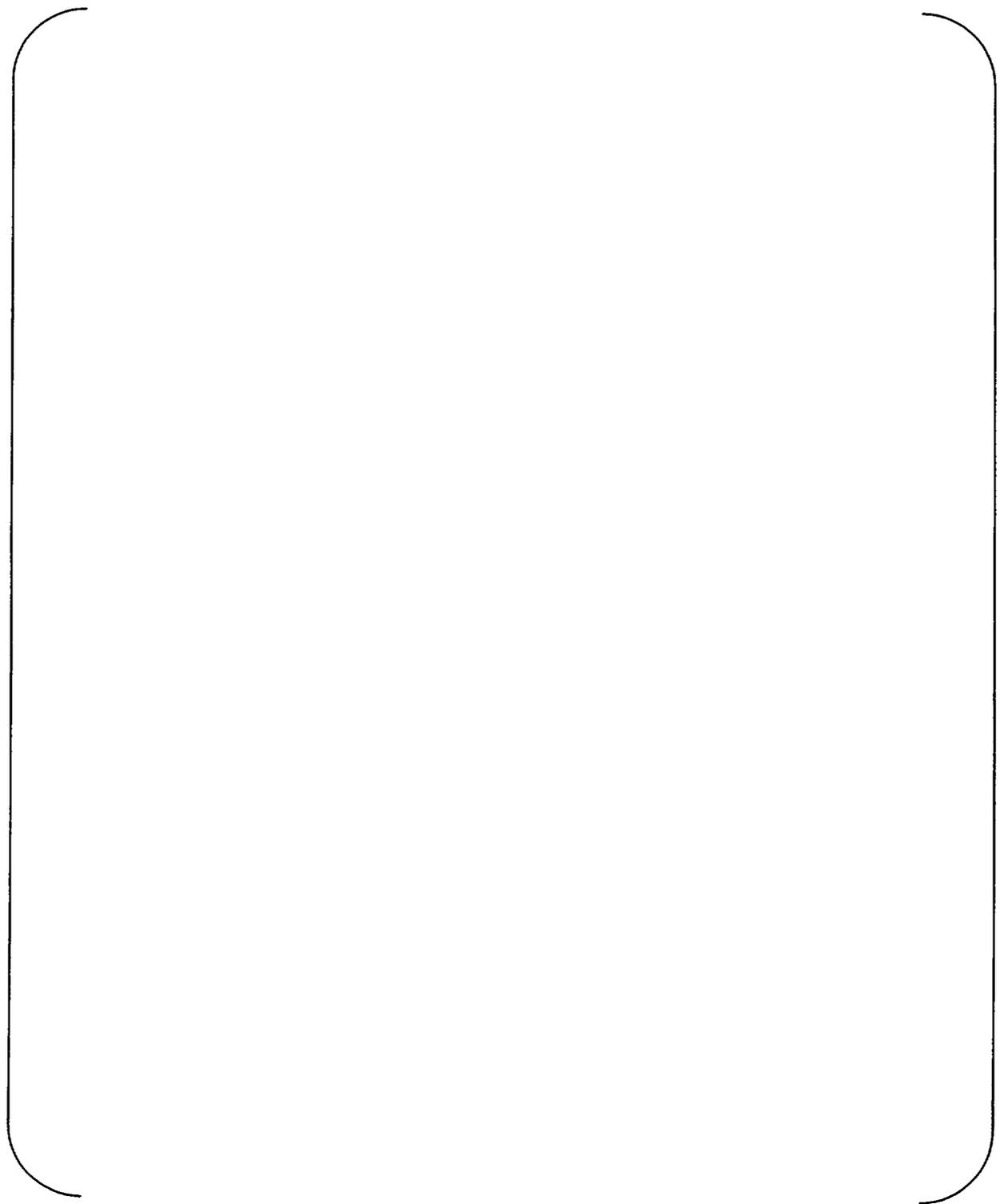
As described above, some components (Category A-3 and Category A-4) are not included in the scope of the base PSA model. Thus, to address the impact of the change in risk associated with extending the integrated ESF test interval, the base PSA models had to be modified to incorporate these components.



5.2.1.3 Analyses to Evaluate Impact of STI







5.2.2 Evaluation of Results

5.2.2.1 Acceptance Criteria

Since these changes from sequential integrated ESF testing to staggered integrated ESF testing is to be a permanent change, per RG 1.174, the change in risk must be less than $1.0E-6/\text{yr}$ for CDF and less than $1.0E-7/\text{yr}$ for LERF.

5.2.2.2 Table Results

CC-1 results were a ΔCDF of { } and a ΔLERF of { } and CC-2 results were a ΔCDF of { } and a ΔLERF of { }. All of Calvert Cliffs results met the acceptance criteria. FCS, had results of ΔCDF of { } and ΔLERF of { } which both are below the acceptance criteria. Palisades, has a ΔCDF of { } which is also below the acceptance criteria. No LERF was calculated for Palisades. WSES-3, has a ΔCDF of { } and a ΔLERF of { } which both are below the acceptance criteria. ΔLERF for Waterford is calculated using the assumption that 10% of CDF is due to LERF. ANO-2 has no "A" components so there was no change in CDF and LERF.

5.2.2.3 Scope of PSAs

The four plants that performed risk evaluations used PSA models with scopes varying from site to site. The Calvert Cliffs PRA is a Level 2 at-power PSA that included internal events (including flood) and external events. The external events that were included are fire, seismic and high wind (hurricane and tornado). OPPD's PSA scope considered seismic, internal events and flood. Palisades and Waterford considered internal events only in their respective PSA scopes. Waterford is located in a very low seismic region, so the lack of a seismic model does not significantly impact their results.

5.2.2.4 Factors Affecting Results

The scope of the PSA can affect the results because other areas are being considered which could impact the PSA. For the most part, all of the results are of the same magnitude with variance coming from the scope. For example, Calvert Cliffs had a complete PSA scope, where Palisades and Waterford considered internal events only. Both are acceptable, but results varied partially due to the scope.

The number of "A" components affected the results because these components are tested only by the integrated ESF test. Since the integrated ESF testing is done during outages, these components are only tested over large time frames. With the assumption that failure probability is rising linearly over time, the "A" component failure rates keep rising over the cycle, where non "A" components are tested more frequently causing the failure rate not to rise as high over time.

These "A" components were based on plant design and testing philosophy. The plant design can have an affect on the testing methods due to configuration. This configuration can limit the number of components tested with a certain test. Testing philosophy refers to the number of tests done on the plants. Some plants have multiple tests that end up testing all of the components included in the integrated ESF test. Other plants have fewer tests that leave out components that are tested during the integrated ESF test (these become "A" components).

5.2.2.5 Shutdown Risk Assessment

The changes included in the proposed integrated ESF test STI amendment are focused on increasing the flexibility to operate and maintain the plant. Since the integrated ESF test is only performed while the unit is shutdown there is no transition risk associated with the proposed STI amendment.

5.2.2.6 PSA Detail Needed for Change

The PSA explicitly models the functions associated with ESFAS. Calvert Cliffs is the only site in this report to have multiple units, in which all unit-to-unit interactions have been considered. Common cause has been addressed earlier in Sections 4.4.1.2 and 4.5.

5.2.2.7 Sensitivity Studies

The lead plant, Calvert Cliffs, performed several sensitivity cases. The results of the sensitivity studies indicate that there is a high degree of confidence that the change in the integrated ESF testing to once every other cycle on a staggered basis will result in a Δ CDF of less than $1.0E-06$ /yr and a Δ LERF of less than $1.0E-07$ per year. The sensitivity studies involved varying the frequency for key parameters over a range of from one half the base frequency to double the base frequency where the base frequency is the frequency that is used for the given parameter in the base case of the PSA. The key parameters evaluated were: (1) the frequency of a hurricane, (2) the frequency for loss of off-site power and (3) the frequency for loss of a 500kV bus, the failure likelihood for RCP seals, and the failure likelihood for operators controlling AFW flow. A sensitivity case which evaluated the importance of the assumption as to whether an RCP motor failure would cause a reactor trip was also included."

For OPPD, Palsades and Waterford, no sensitivity studies were performed.

5.2.2.8 Unavailability Impacts

ESFAS logic, actuation, and sensor cabinets have no planned at-power unavailability. ESFAS may be removed from service when conditions are appropriate during a refueling outage. Since ESFAS must be available to conduct the integrated ESF test, unavailability does not impact this STI change submittal.

In addition, all the components tested by the integrated ESF test must be available (or nominally available if placed into a special testing configuration). Since any equipment tested by the integrated ESF test must be available to conduct the integrated ESF test, unavailability does not impact this STI change submittal.

The STI change request does not seek to alter ESF equipment unavailability.

5.3 OPERATING EXPERIENCE REVIEW AND ANALYSES

5.3.1 Analyses of All Failures and Issues Discovered during Integrated ESF Testing

The object of this evaluation was to determine the number of equipment failures discovered during actual integrated ESF testing. Five plants supplied Condition/Event Reports relating to integrated ESF testing. The search criterion used by the utility to select applicable reports was: (1) include reports going back at least five years, (2) include only reports specifically associated with the integrated ESF test and (3) include reports addressing test failures and problems encountered during the integrated ESF test.

Westinghouse reviewed the event reports and placed them in one of the following groups:

Group I – Equipment/Hardware Failures that most probably would only have been identified by the integrated ESF test (or by an actual demand).

Group II – Equipment/Hardware Failures that would likely have been detected by other tests or during normal operations.

Group III – Non-Equipment/Hardware Failure issues. Examples include: human performance issues, tolerance issues, configuration issues and procedure performance issues.

Group IV – Problems determined to be associated with or related to integrated ESF testing but unrelated to a specific test acceptance criteria or other occurrences that did not fit into any other group.

A total of 122 event reports were reviewed. Thirty-seven fell into Group IV. These reports were related to miscellaneous problems and issues unrelated to the integrated ESF test acceptance criteria.

Of the remaining eighty-five events, seventeen (or 20%) fell into Group I. These events were equipment failures that most probably would only have been identified by the integrated ESF test (or by an actual demand). The majority of the failures were breakers failing to open or close on SIAS, breakers failing to open for load shedding, relay failures resulting in failure of EDG auto load sequencer, and valves not moving to the required position on an ESFAS actuation.

Twenty-one (or 25%) were Group II. These failures were also equipment related. However, based on a high level review of event data, it is believed that these failures could likely have been detected by another test or during normal operations. The type of failure included: breaker failures, valves failing to respond, position indication failures, alarm or recorder problems

The remaining events fell into Group III, which were non-equipment failure issues.

Table 5.3-1 provides a summary of the results.

**Table 5.3-1
Integrated ESF Test Performance Summary**



5.3.2 Analyses of Equipment Failures Discovered during Integrated ESF Testing

The purpose of this analysis was to show the total number of verifications for each function tested during the integrated ESF test and the relationship of that number to the Group I and II equipment failures each function.

To simplify the analyses and focus just on functions usually verified only by the integrated ESF test, the following functions were analyzed (refer to Table 5.3-2): (1) failure to load shed, (2) failure of components to go to the required ESFAS position and (3) failure to sequence on the EDG properly. The data shows that the integrated ESF test has been instrumental in discovering only a very few significant equipment failures.

**Table 5.3-2
Verifications vs. Failures**

Function	Total Number of Verifications	Number of Group I Equipment Failures per Function	Number of Group II Equipment Failures per Function
Load shedding	2186	1	2
ESFAS actuation	6673	6 ⁽¹⁾	14
EDG sequencing	2535	5	6

- (1) One reported event was a sequencer output signal to open a HPSI valve that was out of the acceptance criteria. It was later determined that the acceptance criteria was overly conservative and the acceptance criteria was widened. There have been no subsequent occurrences of this type of failure.

6.0 RESULTS AND CONCLUSIONS

6.1 RISK EVALUATION

Plant-specific evaluations were performed by certain members of the CEOG to determine the risk impact of changing the integrated ESF testing frequency. The evaluations examined changing the surveillance test interval from once every refueling outage on a sequential basis to once every other refueling outage on a staggered basis.

The calculated Δ CDFs at the plants that performed risk evaluations varied from [] to [] (refer to Table 5.2-1). The Δ LERFs at these plants varied from [] to []. ANO-2 had no components for which the integrated ESF test was the sole test of operability, therefore that plant had no change in CDF or LERF associated with the proposed change to the integrated ESF test scheme. The acceptance guidelines for proposed changes as provided in Section 2.2.5 of Regulatory Guide 1.174 consider CDF changes and LERF changes of 1.0E-06/yr to 1.0E-07/yr respectively to be very small regardless of base CDF and LERF and that plant changes resulting in very small changes are acceptable from a risk perspective.

The conclusion is that changing the integrated ESF test from once per cycle with sequential testing to once every other cycle with staggered testing results in very small risk changes. Therefore the proposed changes are acceptable from a risk perspective.

7.0 REFERENCES

1. Regulatory Guide 1.174, "An approach for using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific changes to the Licensing Basis," July 1998.
2. Regulatory Guide 1.177, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," August 1998.
3. NUREG-1432, Revision 02, "CE Improved Standard Technical Specifications," June 2001.
4. ASME OM-S/G-2000, Part 15 "Performance Testing of Emergency Core Cooling Systems in Pressurized Water Reactor Power Plants".
5. CEN-327-A, Revision 000, "RPS/ESFAS Extended Test Interval Evaluation," May 1986.
6. CEN-403, Revision 000, "ESFAS Subgroup Relay Test Interval Extension," July 1991.
7. NUREG/CR-5485, "Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment," November 1998.
8. Calvert Cliffs Units 1 and 2 Final Safety Analysis Report, Revision 32, January 2003.
9. Millstone Unit 2 Final Safety Analysis Report, Change Number 61, June 2002.
10. St. Lucie Units 1 and 2 Final Safety Analysis Report, Amendment 18 and Amendment 14.
11. Fort Calhoun Final Safety Analysis Report, Revision 6, January 2002.
12. Palisades Final Safety Analysis Report, Revision 23, December 2001.
13. Waterford Unit 3 Final Safety Analysis Report, Revision 12A, October 2002.
14. Arkansas One Unit 2 Final Safety Analysis Report, Amendment 221, November 2000.
15. San Onofre Nuclear Generating Station Units 2 and 3 Final Safety Analysis Report, Revision 16, August 2001.
16. Palo Verde Nuclear Generating Station Units 1, 2 and 3 Final Safety Analysis Report, Amendment 14, September 2002.

APPENDIX A

**APPLICATION OF WCAP-15830-NP TO
CALVERT CLIFFS UNITS 1 AND 2**

TABLE OF CONTENTS

A1.0	ABSTRACT	A-4
A2.0	BACKGROUND	A-5
A2.1	ESFAS Description.....	A-5
A2.1.1	Sensor Subsystems	A-5
A2.1.2	Actuation Subsystems.....	A-5
A2.1.3	Cabinets.....	A-7
A2.2	CCNPP Configuration	A-7
A2.2.1	EDGs	A-7
A2.2.2	EDG Loading Shedding.....	A-7
A2.3	Current Technical Specifications	A-9
A2.4	Proposed Changes to Technical Specifications.....	A-11
A3.0	TEST MATRIX AND COMPONENT CATEGORIZATION.....	A-13
A3.1	Method Discussion.....	A-13
A3.1.1	Integrated ESF Test (STP-O-4A (B)-1(2)).....	A-13
A3.1.2	Method Discussion.....	A-13
A3.2	Input.....	A-15
A3.3	Evaluation, Analyses and Results	A-18
A4.0	PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE.....	A-26
A4.1	Model Analysis	A-26
A4.1.1	Components and Functions	A-26
A4.1.2	IESFT Data used in Analysis of Risk.....	A-28
A4.1.3	Assumptions	A-28
A4.1.4	PSA Model Implementation.....	A-29
A4.1.5	Analysis Results	A-32
A4.1.6	Impact of Other Pending/Approved Submittals.....	A-34
A4.2	Scope of PSA	A-35
A4.2.1	At-Power Model Structure.....	A-35
A4.2.2	Shutdown Risk Assessment.....	A-37
A4.2.3	PSA Detail Needed for Change	A-37
A4.2.4	Base PSA Results	A-37
A4.3	Quality of CCNPP PSA	A-38
A4.4	PSA Software.....	A-39
A4.4.1	Riskman.....	A-39
A4.4.2	Minimizer Version Z	A-39
A4.4.3	QSS Evaluator Version P	A-39
A4.5	Results and Conclusions	A-39

LIST OF TABLES

A2.2.1a	Emergency Diesel Generators	A-7
A2.3a	Existing Surveillance Test Intervals	A-9
A2.4a	Proposed Surveillance Test Intervals	A-11
A3.1a	Applicable Database Fields	A-13
A3.2a	ESF Surveillance Test Procedures.....	A-15
A3.3a	Categorization Summary for Calvert Cliffs Units 1 and 2	A-19
A4.1.4.1a	Example of Independent Split Fraction Adjustment	A-31
A4.1.4.1b	Example of Dependent Split Fraction	A-31
A4.1.5.1a	Expected Change in Average Risk	A-32
A4.1.5.3a	Risk Given a Single Load Would Fail a EDG.....	A-34
A4.1.6a	Change in Average Risk with EDG AOT in Effect.....	A-35
A4.2.1a	CCPSA Model Structure	A-36
A4.2.1b	Typical CCPSA Modules within each Model	A-36
A4.2.4a	CCPSA Revision 1 Results	A-38

LIST OF FIGURES

A3.3-1	SIAS Logic Path Components – Calvert Cliffs	A-20
A3.3-2	CIS Logic Path Components – Calvert Cliffs.....	A-21
A3.3-3	CSAS Logic Path Components – Calvert Cliffs.....	A-22
A3.3-4	RAS Logic Path Components – Calvert Cliffs	A-23
A3.3-5	UV Logic Path Components – Calvert Cliffs	A-24
A3.3-6	Sequence Logic Path Components – Calvert Cliffs	A-25
A4.1.4	Model Process	A-30

A1.0 ABSTRACT

Combustion Engineering Owners Group (CEOG) Task 2016, "Staggered Integrated ESF Testing," used a risk-informed approach to demonstrate that any change in risk would be negligible if a staggered test frequency were adopted for integrated Engineered Safety Features (ESF) testing. Currently, integrated ESF testing is performed on both trains each refueling cycle. Using a staggered approach, only one train would be tested each refueling outage. The basic premise of the proposed change is the belief that the integrated ESF test is not the primary/sole operability test for the majority of the components tested. Other surveillance procedures are performed on many of these components and functions on the same or more frequent basis. Therefore, there may be considerable overlap between the integrated ESF test and other testing. For the components/functions that are tested only by the integrated ESF test, the risk model was adjusted, the risk associated with the change recalculated, and the overall risk requantified. In some cases, it was possible to develop a reasonable deterministic basis for assuming the component failure mode addressed by the integrated ESF test was not risk-significant. These components were exempt from further Probabilistic Safety Analysis (PSA) review and analysis. The overall task was broken down into more manageable units of work. The first was the procedure review and matrix development. The second was the categorization of components and functions tested by the integrated ESF test. Third was the preliminary PSA assessment and Category "A" component sub-categorization. Last was the finalization of the PSA assessment, adjusting the PSA models and calculating the change in risk associated with the change in Surveillance Test Interval (STI).

This Appendix addresses application of staggered integrated ESF testing at Calvert Cliffs Units 1 and 2. It describes in detail the plant specific procedure review, component categorization and risk analyses as performed for Calvert Cliffs Units 1 and 2 to support the change to staggered integrated ESF testing. The Technical Specification Surveillance Requirements addressed by the integrated ESF Test are listed in Table A2.3a.

The risk contribution associated with the increased frequency, 24 months on a staggered basis, has been quantitatively evaluated using the current plant-specific PSA model for Calvert Cliffs Units 1 and 2. The change results in a small, but acceptable, risk increase. There is also some risk reductions associated with averting unnecessary plant transients and with reduced risk during shutdown operations, however, these reductions were not quantified.

A2.0 BACKGROUND

A2.1 ESFAS DESCRIPTION

Calvert Cliffs Units 1 and 2 the ESFAS consists of four sensor subsystems and two actuation subsystems. The four sensor sub-systems utilize solid-state bistable comparators to monitor independent process measurements. If a process measurement is unsatisfactory (above or below the setpoint depending on the application) the bistable sends a “tripped” signal to the actuation logic subsystems. A non-CE designed ESFAS is in place at Calvert Cliffs Units 1 and 2.

The actuation subsystem monitors the sensor subsystem trip outputs. Using coincident logic, the actuation subsystem will initiate the relevant protective action when two out of four sensor channels trip. The actuation logic interfaces with plant equipment and components by relay contacts.

The following is a brief description of ESFAS.

A2.1.1 Sensor Subsystems

Four sensor subsystems monitor redundant and independent process measurements. Using bistable comparators, the subsystem will initiate a trip signal when the process parameter is exceeded (above or below the setpoint depending on the application). Each sensor subsystem consists of one sensor channel for each of the following parameters:

- Containment pressure – one each for: Safety Injection Actuation Signal (SIAS), Containment Spray Actuation Signal (CSAS), Containment Isolation Signal (CIS)
- Pressurizer pressure – provides two signals: Safety Injection Actuation Signal (SIAS), Diverse Scram System Signal
- Containment radiation
- Refueling tank water level
- Steam generator pressure
- 4kV bus voltage
- West Penetration Room and Letdown Heat Exchanger Room Pressure
- Steam Generator level
- Reactor trip bus voltage

Each of the parameters is monitored by four redundant sensors, except containment pressure which is monitored by twelve sensors (four per signal) and the steam generator level which is monitored by eight sensors (four per steam generator).

A2.1.2 Actuation Subsystems

Two redundant and independent actuation subsystems monitor the sensor subsystem outputs and, using two out of four coincident logic, initiate the required protective action. Either subsystem channel controls sufficient equipment to protect the public from a loss of coolant incident, main steam line break, or loss of power incident.

A2.1.2.1 Actuation Inputs

ESFAS sensor and actuation channels produce signals to initiate equipment operation consistent with the type of protective action required. Actuation channels include the following actions:

- Safety Injection Actuation Signal (SIAS)
- Containment Spray Actuation Signal (CSAS)
- Containment Isolation Signal (CIS)
- Recirculation Actuation Signal (RAS)
- Containment Radiation Signal (CRS)
- Steam Generator Isolation Signal (SGIS)
- Undervoltage Signal (EFAS)
- Blocking and Sequencing Signals
- Chemical and Volume Control Isolation Signal (CVCIS)
- Diverse Scram System Signal

A2.1.2.2 Actuation Output

The plant equipment to ESFAS interface is accomplished using power relays. The relay coils are controlled by the actuation logic modules. Relay contacts provide the equipment switching function required for equipment control as well as isolation from other plant equipment and ESFAS internal components.

A2.1.2.3 Sequencer Operation

Bus undervoltage is sensed by four relays that monitor the 4kV bus potential transformer outputs. Note that the undervoltage relays respond to three conditions: loss of voltage, transient undervoltage and steady state undervoltage. The following actions occur when two out of four undervoltage relays actuate ESFAS:

- Trips the normal (or alternate) bus feeder breaker,
- Trips selected load breakers (referred to as non-permanent loads),
- Starts the EDG,
- After the EDG has repowered the bus, it repowers required loads in a sequential manner. The stepwise restoration of specific loads depends on the plant status.

On the loss of power or bus undervoltage condition ESFAS repowers selected loads depending on the plant status using one of the two sequencers described below:

- The Shutdown Sequencer (SDS) actuates following a bus undervoltage when no other ESFAS actuations are present. Repowered loads are those required to achieve and maintain reactor shutdown.

- The Loss of Coolant Incident (LOCI) sequencer actuates following the concurrent bus undervoltage and a Safety Injection Actuation Signal (SIAS). In addition to most of the shutdown loads, the LOCI sequencer starts and aligns the safety injection trains. The LOCI sequencer presents the heaviest total EDG loading.

A2.1.3 Cabinets

There are four sensor subsystem cabinets (ZD, ZE, ZF and ZG), each contains a sensor channel. Each cabinet is fed from one of the four 120 Volt Vital AC Buses (1Y01, 1Y02, 1Y03 and 1Y04).

There are also four actuation subsystem cabinets: (AL, BL, AR and BR). For each actuation channel (ZA and ZB) there is a logic cabinet (AL and BL) and a power relay cabinet (AR and BR). The "A" subsystem is fed from 120VAC Vital Bus 1Y01 and the "B" subsystem is fed from 120VAC Vital Bus 1Y02.

The cabinets also house power supplies, cooling fans, and various interface/control elements (such as switches, indicators, annunciators) required for operation.

A2.2 CCNPP CONFIGURATION

The ESF functions start/align equipment required to mitigate design basis accidents. A critical aspect of the ESFAS design addresses the loss of the normal (off-site) power supply.

A2.2.1 EDGs

At Calvert Cliffs, the four 4kV ESF buses are each supplied by a dedicated EDG. The table below shows the EDG to bus alignment and naming convention:

**Table A2.2.1a
Emergency Diesel Generators (EDGs)**

Emergency Diesel Generator	Manufacturer	4kV Bus	Channel Supported
1A EDG	SACM	11	1A
1B EDG	Fairbanks-Morse	14	1B
2A EDG	Fairbanks-Morse	21	2A
2B EDG	Fairbanks-Morse	24	2B

In addition, the 0C Station Blackout EDG (SACM) is available through operator (manual) alignment.

A2.2.2 EDG Load Shedding

As discussed in Section A2.1.2.3, on a loss of normal power ESFAS sheds loads and then re-starts equipment in a stepwise manner. The stepwise application of load ensures the bus voltage is sufficient to start and run new loads by providing time for the EDG engine and generator voltage regulator to stabilize at rated speed and voltage before the new loads are added. Bus loads are specified with a minimum starting voltage at seventy-five percent of bus rated voltage and minimum running voltage at ninety percent of bus rated voltage. In addition, the minimum allowable starting voltage for the SACM diesel is

eighty-two percent of rated voltage (Fairbanks-Morse is seventy-five percent).

The initial repowering step, Step 0, occurs when the EDG bus feeder breaker closes (when the EDG reaches rated speed and voltage). This repowers the 4kV bus and all “permanent” loads – loads intentionally not shed. Because Step 0 equipment includes numerous small to medium loads, Step 0 is the most limiting step from an EDG load perspective.

From the foregoing discussion, it is also clear that any loads that failed to shed as part of the ESFAS undervoltage response will also repower with Step 0. Application of such additional loads will impact only Step 0: If the EDG does succeed in Step 0 with the additional loads, it will be stabilized and ready to accept additional Step 1 loads within the five second step interval. Subsequent steps will succeed for the same reason.

An examination of ESFAS schematics in the UFSAR shows that for Channel 1A:

- Thirty-two loads are shed.
- Twenty-eight load shed relays are used:
 - One load has two relays (13 AFW Pump)
 - Three relays support two loads (per relay)
 - One relay supports three loads
- Approximately twenty loads are normally loaded.

Note that Channel 1A is the most heavily loaded ESF channel.

A2.3 CURRENT TECHNICAL SPECIFICATIONS

Table A2.3a lists all the Technical Specification Surveillance Requirements that apply to the Integrated ESF Test.

**Table A2.3a
Existing Surveillance Test Intervals**

	Surveillance	Frequency
SR 3.3.4.5	Verify ESF RESPONSE TIME is within limits. (Table 3.3.4.1, Item 1a): <ol style="list-style-type: none"> 1. Safety Injection Actuation Signal <ol style="list-style-type: none"> a. Containment Pressure-High 	24 Months
SR 3.3.5.2	Perform a CHANNEL FUNCTIONAL TEST on each ESFAS Manual Actuation Channel. (Table 3.3.5.1 Items 1.a, 2.a, 3.a, and 5.a) <ol style="list-style-type: none"> 1. Safety Injection Actuation Signal <ol style="list-style-type: none"> a. Manual Actuation 2. Containment Spray Actuation Signal <ol style="list-style-type: none"> a. Manual Actuation 3. Containment Isolation Signal <ol style="list-style-type: none"> a. Manual Actuation 5. Containment Sump Recirculation Actuation Signal <ol style="list-style-type: none"> a. Manual Actuation 	24 Months
SR 3.5.2.5	Verify each ECCS automatic valve that is not locked, sealed, or otherwise secured in position, in the flow path actuates to the correct position on an actual or simulated actuation signal.	24 Months
SR 3.5.2.6	Verify each ECCS pump starts automatically on a actual or simulated actuation signal.	24 Months
SR 3.5.2.7	Verify each low pressure safety injection pump stops on an actual or simulated actuation signal	24 Months
SR 3.6.3.5	Verify each automatic containment isolation valve that is not locked, sealed, or otherwise secured in position, actuates to the isolation position on an actual or simulated actuation signal.	24 Months
SR 3.6.6.5	Verify each automatic containment spray valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 Months

**Table A2.3a (continued)
Existing Surveillance Test Intervals**

Surveillance		Frequency
SR 3.6.6.6	Verify each containment spray pump starts automatically on an actual or simulated actuation signal.	24 Months
SR 3.6.6.7	Verify each containment cooling train starts automatically on an actual or simulated actuation signal	24 Months
SR 3.6.8.3	Verify each IRS train actuates on an actual or simulated actuation	24 Months
SR 3.7.12.3	Verify each PREVS train actuates on an actual or simulated actuation	24 Months
SR 3.7.5.2	Verify each CC automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 Months
SR 3.7.5.3	Verify each CC pump starts automatically on an actual or simulated actuation signal.	24 Months
SR 3.7.6.2	Verify each SRW automatic valve in the flow path that is not locked, sealed or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 Months
SR 3.7.6.3	Verify each SRW pump starts automatically on an actual or simulated actuation signal.	24 Months
SR 3.7.7.2	Verify each SW System automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to be correct position on an actual or simulated actuation signal.	24 Months
SR 3.7.7.3	Verify each SW System pump starts automatically on an actual or simulated actuation signal.	24 Months
SR 3.8.1.11	-----NOTE----- Momentary transients outside the load and power factor limits do not invalidate this test. ----- Verify each DG, operating at a power factor of ≤ 0.85 , operates for ≥ 60 minutes while loaded to > 4000 kW for DG 1A and ≥ 3000 kW for DGs 1B, 2A and 2B.	24 Months
SR 3.8.1.12	Verify each DG rejects a load ≥ 500 hp without tripping	24 Months
SR 3.8.1.14	Verify each DG: a. Synchronizes with offsite power source while loaded upon a simulated restoration of offsite power; b. Manually transfers loads to offsite power source; and c. Returns to ready-to-load operation.	24 Months
SR 3.8.1.15	-----NOTE----- All DG starts may be preceded by an engine prelube period. ----- Verify on an actual or simulated loss of offsite power signal in conjunction with an actual or simulated Engineered Safety Feature actuation signal: a. De-energization of emergency buses; b. Load shedding from emergency buses; c. DG auto-starts from standby condition and: 1. Energizes permanently connected loads in ≤ 10 seconds, 2. Energizes auto-connected emergency loads through load sequencer, 3. Maintains steady state voltage ≥ 4060 V and ≤ 4400 V, 4. Maintains steady state frequency of ≥ 58.8 Hz and ≤ 61.2 Hz, and 5. Supplies permanently connected and auto-connected emergency loads for ≥ 5 minutes.	24 Months

A2.4 PROPOSED CHANGES TO TECHNICAL SPECIFICATIONS

Table A2.4a shows the proposed changes that apply to Calvert Cliffs Units 1 and 2. The proposed frequency is based on the Calvert Cliffs TS definition for staggered testing.

**Table A2.4a
Proposed Surveillance Test Intervals**

	Surveillance	Frequency
SR 3.3.4.5	Verify ESF RESPONSE TIME is within limits. (Table 3.3.4 1 Item 1.a) 1. Safety Injection Actuation Signal a. Containment Pressure-High	24 Months on a STAGGERED TEST BASIS
SR 3.3.5.2	Perform a CHANNEL FUNCTIONAL TEST on each ESFAS Manual Actuation Channel. (Table 3.3.5.1 Items 1.a, 2.a, 3.a and 5.a) 1. Safety Injection Actuation Signal b. Manual Actuation 2. Containment Spray Actuation Signal a. Manual Actuation 3. Containment Isolation Signal a. Manual Actuation 5. Containment Sump Recirculation Actuation Signal a. Manual Actuation	24 Months on a STAGGERED TEST BASIS
SR 3.5.2.5	Verify each ECCS automatic valve that is not locked, sealed or otherwise secured in position, in the flow path actuates to the correct position on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.5.2.6	Verify each ECCS pump starts automatically on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.5.2.7	Verify each low pressure safety injection pump stops on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.6.3.5	Verify each automatic containment isolation valve that is not locked, sealed, or otherwise secured in position, actuates to the isolation position on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.6.6.5	Verify each automatic containment spray valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.6.6.6	Verify each containment spray pump starts automatically on an actual or simulated actuation signal	24 Months on a STAGGERED TEST BASIS
SR 3.6.6.7	Verify each containment cooling train starts automatically on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.6.8.3	Verify each IRS train actuates on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.7.12.3	Verify each PREVS train actuates on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.7.5.2	Verify each CC automatic valve in the flow path that is not locked, sealed or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.7.5.3	Verify each CC pump starts automatically on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS

**Table A2.4a (continued)
Proposed Surveillance Test Intervals**

Surveillance		Frequency
SR 3.7.6.2	Verify each SRW automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.7.6.3	Verify each SRW pump starts automatically on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.7.7.3	Verify each SW System pump starts automatically on an actual or simulated actuation signal.	24 Months on a STAGGERED TEST BASIS
SR 3.8.1.11	-----NOTE----- Momentary transients outside the load and power factor limits do not invalidate this test. ----- Verify each DG, operating at a power factor of ≤ 0.85 , operates for ≥ 60 minutes while loaded to ≥ 4000 kW for DG 1A and ≥ 3000 kW for DGs 1B, 2A and 2B.	24 Months on a STAGGERED TEST BASIS
SR 3.8.1.12	Verify each DG rejects ≥ 500 hp without tripping.	24 Months on a STAGGERED TEST BASIS
SR 3.8.1.14	Verify each DG: a. Synchronizes with offsite power source while loaded upon a simulated restoration of offsite power; b. Manually transfers loads to offsite power source; and c. Returns to ready-to-load operation.	24 Months on a STAGGERED TEST BASIS
SR 3.8.1.15	-----NOTE----- All DG starts may be preceded by an engine prelube period. ----- Verify on an actual or simulated loss of offsite power signal in conjunction with an actual or simulated Engineered Safety Feature actuation signal: a. De-energization of emergency buses; b. Load shedding from emergency buses; c. DG auto-starts from standby condition and: 1. Energizes permanently connected loads in ≤ 10 seconds, 2. Energizes auto-connected emergency loads through load sequencer, 3. Maintains steady state voltage ≥ 4060 V and ≤ 4400 V, 4. Maintains steady state frequency of ≥ 58.8 Hz and ≤ 61.2 Hz, and 5. Supplies permanently connected and auto-connected emergency loads for ≥ 5 minutes.	24 Months on a STAGGERED TEST BASIS

A3.0 TEST MATRIX AND COMPONENT CATEGORIZATION

A3.1 METHOD DISCUSSION

A3.1.1 Integrated ESF Test (STP-O-4A (B)-1(2))

The integrated ESF test is performed on both trains, one train at a time, every 24 months. The test is initiated by simulating a loss of offsite power on an emergency bus using the ESFAS UV function test circuitry. After the UV function trips on loss of power to the emergency bus, SIAS, CSAS, CIS and AFAS are simultaneously initiated with the manual actuation pushbuttons.

Objectives (functions) covered by the integrated ESF test include:

- Load Shed Verification
- SIAS/CIS/CSAS with LOP Actuation Verification
- RAS Actuation Verification
- SIAS with LOP Permanent Load Verification
- SIAS with LOP DG Load Sequencer Verification
- EDG Functional Test - > 60 min run with reduced (< 0.85) power factor
- EDG Functional Test - SIAS/CIS/LOP followed by > 500 hp Load Rejection
- Restoration of Normal Offsite Power Test
- EDG Operating Parameter(s) Verification
- AFAS Actuation Verification

A3.1.2 Method Discussion

An ESF Testing Matrix was prepared by Westinghouse for Calvert Cliffs Units 1 and 2 as part of CEOG Task 2016, Staggered integrated ESF Testing. A database was used to create the matrix and to document the results of the ESF procedure review. The primary function of the database is to map the components tested by Calvert Cliffs integrated ESF test procedures, STP O-4A and STP O-4B, to other surveillances that test the same components and functions. Units 1 and 2 procedures are basically the same. The database contains references to the integrated ESF test and other tests, as well as the initial component categorization. The categorization performed by Westinghouse provided the foundation for the plant specific PSA calculation performed by Calvert Cliffs.

The following table explains the portion of the database used to develop the procedure review matrix. Component categorization and assessments are addressed in Section A4.0 of this appendix.

Table A3.1a
Applicable Database Fields

Column Heading	Explanation
Component ID	Component ID used in STP-O-4A-1(2) and STP-O-4B-1(2)
Component Description	Component description used in STP-O-4A-1(2) and STP-O-4B-1(2)
Integrated ESF test	Integrated ESF test designation for this entry
Surveillance Requirement (24 MO)	Reference to Calvert Cliffs Technical Specifications

Column Heading	Explanation
Functions tested by the Integrated ESF test.	The large blue section of the database shows the location in (STP-O-4A-1(2) and STP-O-4B-1(2)) where a particular component was identified in the test for a particular ESF function. For each component, the database shows the position verified. A blank field indicates that the component / function is not tested by the integrated ESF test.
Integrated ESF test Summary	Summarizes the functions tested by the integrated ESF test for each component.
Cat	Component category, "A", "B" or "C". Categories are defined and explained below. The initial PSA assessment further divides Category "A" components into A-1, A-2, A-3 or A-4 to facilitate requantification of risk by Calvert Cliffs. The screening process used to sort components into subcategories is described in Section 4.0 of the topical report and is related specifically to Calvert Cliffs.
Assessment	An initial assessment that supports why the component is initially categorized "A", "B" or "C".
Notes	Reviewer notes relative to the assessment.
Other Test 1 through 5	Lists references to other Calvert Cliffs surveillance procedures that overlap the integrated ESF test.

The matrix was developed as follows: First, integrated ESF tests, STP O-4A-1(2) and STP O-4B-1(2) were reviewed to identify the components and functions being tested and the results entered into the database. To facilitate future sorting of the data, the component type, system identifier and number, and associated TS surveillance requirement were also added. Fields that are not needed to support this appendix have been hidden. To facilitate locating the component being tested, the procedure step or attachment was also recorded. Under each applicable function, the component end condition following the test was entered. Following the individual functions, a summary of all the functions tested was added.

Once all components and functions tested by the integrated ESF test were identified, other related TS surveillance tests were reviewed to determine if they tested any of the same components tested by the integrated ESF test on the same or more frequent bases. During this review, care was taken to ensure that the other more frequent test demonstrated operability of the same component and tested the same function. Those tests that satisfied the criteria were logged under an 'other test' column adjacent to the specific component. After reviewing all the candidate 'other test' procedures provided, Westinghouse made an assessment as to whether or not the integrated ESF test was the sole/primary test for each component. An initial categorization of the components was then made. The categories are defined as follows:

- Category A The integrated test is the sole/primary test which demonstrates the operability or function of these components. These components perform an engineered safeguards function. The PSA model addresses (or should address) failure of these components. They may be modeled explicitly, modeled via a subsuming component, or modeled via a surrogate event.
- Category B Similar to Category A, the integrated test is the sole/primary test which demonstrates the operability or function of these components. Unlike the Category A components, the Category B components are not included in the PSA model. Failure of these components therefore does not affect the calculated risk. The rationale for excluding

them from the model is provided in the database. For example, valves which are normally in their safeguards-actuated position may not be modeled because the safeguards signal is "confirmatory" - the signal is necessary only if the event should occur while the associated system is in an unusual or infrequent configuration.

Category C The integrated test is not the sole/primary test which demonstrates the operability or function of these components. Other, more frequently performed surveillance tests ensure that changes to the integrated test frequency would not affect the failure probabilities for these components.

The Category A and B components then became the focus and were reviewed further to determine the PSA impact. The PSA review and analysis is documented in Section A4.0.

A3.2 INPUT

Westinghouse used electronic copies of current TS surveillance procedures provide by Calvert Cliffs on a Compact Disc (CD) to perform the review and develop the matrix database (refer to Table A3.1a for an explanation of the key fields in the database). The following table provides a list of the surveillance procedures included in the review, including the integrated ESF procedures:

Procedure	Procedure Title	Frequency
STP O-4A-2, Revision 23	A TRAIN INTEGRATED ENGINEERED SAFETY FEATURES TEST	Once every 24 months
STP O-4B-2, Revision 23	B TRAIN INTEGRATED ENGINEERED SAFETY FEATURES TEST	Once every 24 months
STP O-107-1, Revision 00	SAFETY INJECTION TANK BORON VERIFICATION	Once every month
STP O-1-1, Revision 13	MSIV FULL STROKE TEST	Once every 24 months
STP O-13-1, Revision 2	SHUTDOWN ESFAS LOGIC TEST	Once every 24 months
STP O-36-1, Revision 7	SHUTDOWN COOLING HDR RETURN ISOLATION VALVE TEST	Once every 24 months
STP O-55-1, Revision 40	CONTAINMENT INTEGRITY VERIFICATION MODE 1 - 4	Once every month
STP O-56A-2, Revision 14	ESFAS EQUIPMENT RESPONSE TIME	Once every 24 months
STP O-56B-2, Revision 15	ESFAS EQUIPMENT RESPONSE TIME	Once every 24 months
STP O-56C-2, Revision 4	ESFAS EQUIPMENT RESPONSE TIME MODES 1 AND 2	Once every 24 months
STP-O-56D-2, Revision 4	ESFAS EQUIPMENT RESPONSE TIME MODES 1 AND 2	Once every 24 months

Table A3.2a ESF Surveillance Test Procedures		
Procedure	Procedure Title	Frequency
STP O-57-1, Revision 7	TEST OF ALTERNATE AC POWER SOURCES	Once every 24 months
STP O-5A-1, Revision 11	AUXILIARY FEEDWATER SYSTEM QUARTERLY SURVEILLANCE TEST	Once every Quarter
STP O-5B-1, Revision 1	AFW FLOW PATH VERIFICATION	Once after each shutdown prior to entering Mode 2
STP O-60-1, Revision 13	CONTAINMENT PURGE ISOLATION SYSTEM FUNCTIONAL TEST	Once every 24 months
STP O-62-1, Revision 39	MONTHLY VALVE POSITION VERIFICATION-UNIT 1	Once every month
STP O-64-1, Revision 7	SAFETY INJECTION TANK 31 DAY OPERABILITY VERIFICATION	Once every month
STP O-65A-1, Revision 7	CVCS VALVE QUARTERLY OPERABILITY TEST	Once every Quarter
STP O-65D-1, Revision 3	MISC CI VALVE QUARTERLY OPERABILITY TEST	Once every Quarter
STP O-65Q-1, Revision 5	SIS VALVE QUARTERLY OPERABILITY TEST	Once every Quarter
STP O-66A-1, Revision 2	CVCS VALVE QUARTERLY OPERABILITY TEST	Once every Quarter
STP O-66B-1, Revision 2	MISC CI VALVE QUARTERLY OPERABILITY TEST	Once every Quarter
STP O-66C-1, Revision 2	FEEDWATER ISOLATION VALVES OPERABILITY TEST	Once every 24 months
STP O-66D-1, Revision 2	CC ISOLATION VALVES OPERABILITY TEST	Once every 24 months
STP O-66G-1, Revision 5	MISCELLANEOUS COLD SHUTDOWN VALVE OPERABILITY TEST	Once every 24 months
STP O-66M-1, Revision 2	COLD SHUTDOWN OPERABILITY TEST OF SHUTDOWN COOLING RETURN ISOLATION VALVES	Once every 24 months
STP O-67B-1, Revision 4	AUXILIARY FEEDWATER/MAIN STEAM CHECK VALVE TEST	Once after each shutdown prior to entering Mode 2
STP O-69-1, Revision 11	SGIS AND CSAS-3 LOGIC TEST	Once every Quarter
STP O-70-1, Revision 14	MONTHLY TEST OF "A" TRAIN CONTAINMENT COOLING UNITS, IODINE REMOVAL UNITS & PENETRATION ROOM EXHAUST FILTER	Once every month

**Table A3.2a
ESF Surveillance Test Procedures**

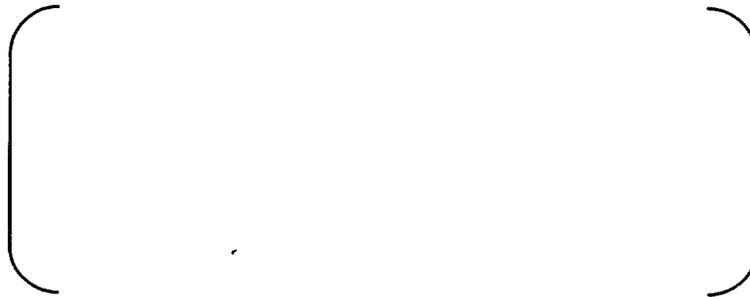
Procedure	Procedure Title	Frequency
STP O-71-1, Revision 16	MONTHLY TEST OF "B" TRAIN CONTAINMENT COOLING UNITS, IODINE REMOVAL UNITS & PENETRATION ROOM EXHAUST FILTER	Once every month
STP O-73D-1, Revision 10	CHARGING PUMP PERFORMANCE TEST	Once every Quarter
STP O-73G-1, Revision 3	HPSI PUMP LARGE FLOW TEST	Once every 24 months
STP O-73H-1, Revision 3	AFW PUMP LARGE FLOW TEST	Once every 24 months
STP O-73I-1, Revision 7	HPSI PUMP AND CHECK VALVE QUARTERLY OPERABILITY TEST	Once every Quarter
STP O-73J-1, Revision 7	LPSI PUMP OPERABILITY TEST	Once every Quarter
STP O-73K-1, Revision 8	CONTAINMENT SPRAY PUMP OPERABILITY TEST	Once every Quarter
STP O-73L-1, Revision 6	LPSI PUMP LARGE FLOW TEST	Once every 24 months
STP O-73M-1, Revision 2	CONTAINMENT SPRAY FLOW TEST	Once every 24 months
STP O-7A-1, Revision 53	"A" TRAIN ENGINEERED SAFETY FEATURES LOGIC TEST	Once every Quarter
STP O-7B-1, Revision 52	"B" TRAIN ENGINEERED SAFETY FEATURES LOGIC TEST	Once every Quarter
STP O-8A- Revision 21	TEST OF 1A DG AND 11 4KV BUS LOCI SEQUENCER	Once every month
STP O-8B-1, Revision 22	TEST OF 1B DG AND 14 4KV BUS LOCI SEQUENCER	Once every month
STP-9A-2, Revision 7	AFAS RESPONSE TIME TEST	Once every 24 months
STP-M-220A-1, Revision 3	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM CHANNEL ZD FUNCTION TEST	Once every 92 days
STP M-522-1, Revision 11	4KV UNDERVOLTAGE RELAY CALIBRATION AND RESPONSE TIME CHECK	Once every 24 months
STP-M-510EL-1, Revision 1	RPS PRESSURIZER PRESSURE AND THERAM MARGIN/LOW PRESSURE LOOP CALIBRATION	Once every 24 months

Table A3.2a ESF Surveillance Test Procedures		
Procedure	Procedure Title	Frequency
STP-M-510ET-1. Revision 1	RPS PRESSURIZER PRESSURE AND THERMAL MARGIN/LOW PRESSURE TRANSMITTER CALIBRATION CHECKS	Once every 24 months
STP-M-520A-1, Revision 2	ESFAS CONTAINMENT PRESSURE CHANNEL ZD CALIBRATION	Once every 24 months
STP-M-520G-1, Revision 0	REFUELING WATER TANK LOW LEVEL BISTABLE SETPOINT CALIBRATION CHECK	Once every 24 months

A3.3 EVALUATION, ANALYSES AND RESULTS

The component categorization process is described in detail in the body of the topical report, Section 4.0, therefore it shall not be repeated here. Table A3.3a provides a numerical summary of the classification results specifically for Calvert Cliffs Units 1 and 2.

Table A3.3a
Categorization Summary for Calvert Cliffs Units 1 and 2



Figures A3.3-1 through A3.3-6 illustrate where there is overlap in integrated ESF testing at Calvert Cliffs Units 1 and 2. They are simplified illustrations and therefore depict only a rough approximation of overlap. They are not intended to provide engineering and system design detail. The figures were constructed starting with the basic components of the logic path from the sensor to the end equipment. Then the tests covering various components in the logic path were added. Figures A3.3-1 through A3.3-4 address testing associated with SIAS, CIS, CSAS and RAS actuation. Figure A3.3-5 covers Under Voltage (UV) Sensing. Figure A3.3-6 covers EDG load sequencers. The test procedures referenced in these diagrams are also mapped to specific components in the project database under the headings of "Other Test 1, 2, 3" etc.

Figure A3.3-1
SIAS Logic Path Components - Calvert Cliffs

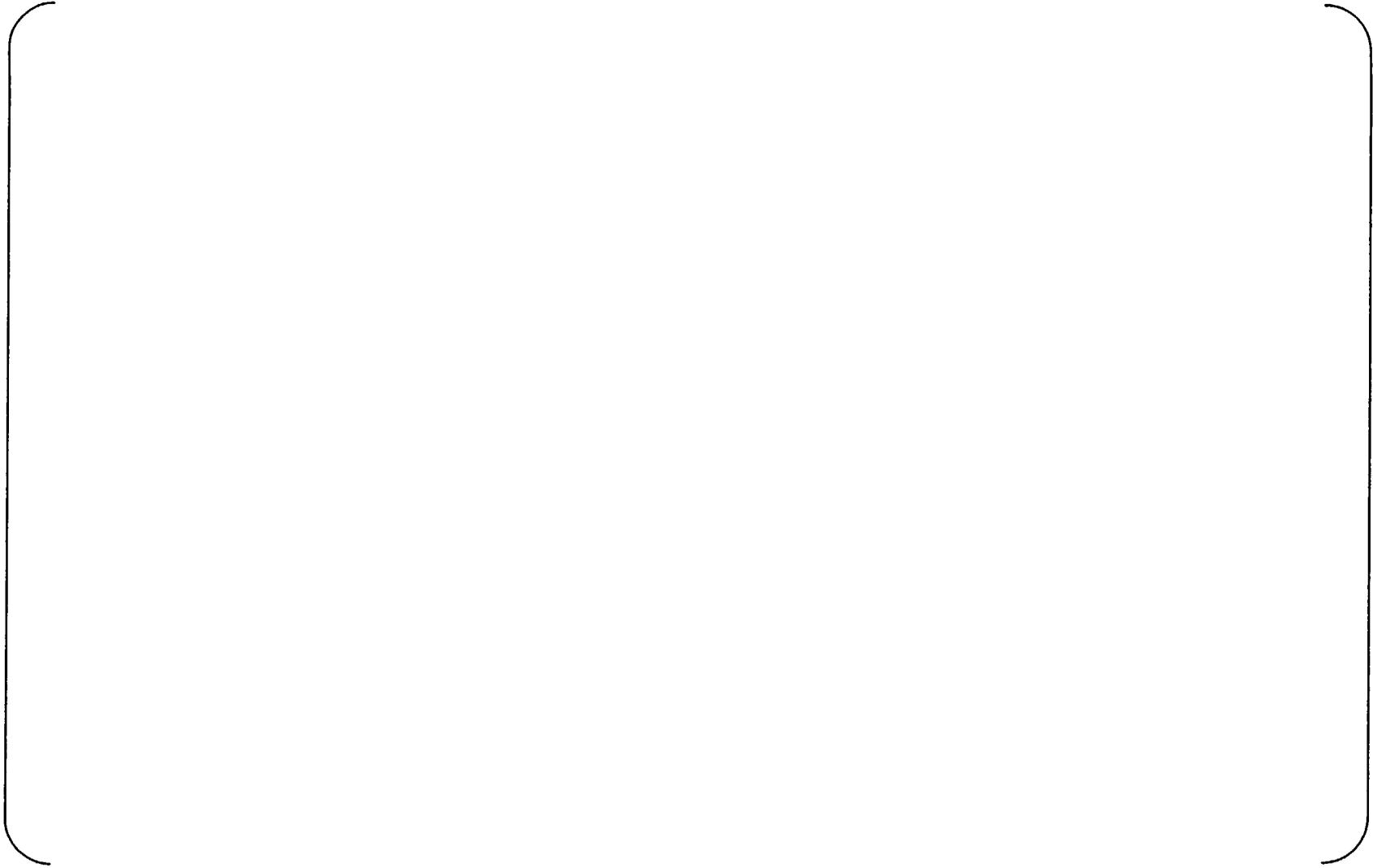


Figure A3.3-2
CIS Logic Path Components - Calvert Cliffs



Figure A3.3-3
CSAS Logic Path Components - Calvert Cliffs



Figure A3.3-4
RAS Logic Path Components - Calvert Cliffs



Figure A3.3-5
UV Logic Path Components - Calvert Cliffs



Figure A3.3-6
Sequence Logic Path Components - Calvert Cliffs



A4.0 PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE

As mentioned previously, Westinghouse performed a preliminary categorization and assessment of components tested by the integrated ESF test functions for Calvert Cliffs Units 1 and 2. Calvert Cliffs used the preliminary categorization as a foundation and starting point to perform the PSA analysis described in this section. The categorization begins with the testing matrix described in Section A3.0. The matrix was used to identify components whose reliability appears to be demonstrated primarily/solely by the integrated ESF test.

Westinghouse used the Calvert Cliffs PSA Master List of Basic Events to determine if and how the model addressed each such component or function. The results of the review were documented in a database which relates the components to the associated basic events. The components were categorized, based on the type of changes to the event frequencies or modeling details that would be needed in order to quantify the change in risk associated with the proposed change in the integrated ESF test frequency. The actual changes to the model and the requantification of the model was performed by Calvert Cliffs. The remainder of Section A4.0 is derived from the risk analyses performed by Calvert Cliffs.

A4.1 MODEL ANALYSIS

The analysis process identified all ESF components and functions tested by the integrated ESF test. These were then categorized for impact as described in Section A3.0. Calvert Cliffs reviewed the categorization and created another database to support their PSA analyses. Note that Calvert Cliffs also introduced a Category "D" component grouping which was not part of the generic categorization process described in the topical report.

A4.1.1 Components and Functions

The Calvert Cliffs integrated ESF is Surveillance Test Procedure O-004A(B)-1(2). The "A" and "B" refer to the train (facility) and "1" and "2" refer to the unit.

A4.1.1.1 Identification of Integrated ESF Test Components and Functions

The initial step in the risk analysis was to identify what ESF functions are tested by the integrated ESF and which surveillance requirement each test satisfies. To accomplish this, each STP-O-4A-1(2) and STP-O-4B-1(2) step was evaluated to determine what ESF function is being tested. This evaluation includes an equipment level examination of relevant electrical schematics and design documents to ensure that all the components required for the function being tested are identified.

The results of this process are captured in an ACCESS database. The STP O-4 database fields include:

- Device, Load, Description
- STP (Unit, Train)
- STP O-004 Attachment/Step
- Electrical data: Voltage, Bus, Horsepower, kW, kVA
- Load Shed

- Load Actuation
- Surveillance Requirement
- Initial State
- Activated State

A4.1.1.2 Categorization of Tests

Next, other plant surveillance test procedures were reviewed to identify any STP O-4 components tested in those procedures: If so, the applicable surveillance procedure was logged in the database. These items were then placed into one of three basic categories:

- Category A The IESFT is the sole test which demonstrates the operability or function of these components. These components perform an ESF function. The PSA model addresses failure of these components which may be explicitly modeled or modeled as a subsumed component. The PSA model will be modified to address the test interval change.
- Category B Similar to Category A, the IESFT test demonstrates the operability or function of these components. Unlike Category A components, the PSA model will not be modified for Category B components. A qualitative discussion explains why these components require no modeling adjustment.
- Category C The integrated test is not the sole test which demonstrates the operability or function of these components. Other more frequently performed surveillance tests ensure that changes to the integrated test frequency would not effect the failure probabilities of these components.
- Category D Test items not required to satisfy the Technical Specifications and not modeled in the PSA. Typically precondition checks or concerns associated with equipment operating parameters or components used only to perform the test itself.

The results of this process was also captured in the STP O-4 database. The STP O-4 database fields include:

- Category – As defined above.
- Additional STP(s) / Step – Alternative surveillance test(s) that prove a component function tested by STP O-4 and the
- Additional STP Frequency – If an additional surveillance test is identified (above), the test frequency is shown here.

Note that STP O-4B-1, STP O-4A-2 and STP O-4B-2 was developed along the same lines as STP O-4A-1. These STPs test equivalent components in the same manner and the database analysis results are similar. Because the inclusion of these database results will yield little additional information they are omitted from this submittal.

A4.1.2 IESFT Data used in Analysis of Risk

ESFAS logic, actuation and sensor cabinets have no planned at-power unavailability. ESFAS may be removed from service when conditions are appropriate during a refueling outage. Since ESFAS must be available to conduct the IESFT, unavailability does not impact this STI change submittal.

In addition, all the components tested by the IESFT must be available (or nominally available if placed into a special testing configuration). Since any equipment tested by the IESFT must be available to conduct the IESFT, unavailability does not impact this STI change submittal.

The STI change request does not seek to alter ESF equipment unavailability.

A4.1.3 Assumptions

The following assumptions are used in the modeling analysis:

- Both ESFAS channels are operating in the extended time frame

The analysis applies doubled failure rates to both ESFAS channels. This is conservative as by staggering the test interval only a single channel is actually operating beyond the base two year interval in a given refueling cycle.

- Equipment failure likelihood is proportional to test interval time

The risk evaluation is based on the premise that equipment failure likelihoods are considered proportional to the testing interval. Generally, this is considered a conservative position as some fraction of equipment failure likelihood is due to the shock of changing state. For this evaluation, given a specific component, doubling the test interval is considered to double the component failure rate.

- Step 0 SDS and LOCI loads are the same

The undervoltage loads (equipment) shed and Step 0 loads (equipment) are the same for either the SDS or LOCI sequencer actuates. Actual Step 0 bus loading will be somewhat higher for the LOCI case due to additional small loads associated with SIAS (for example, motor operated valves and saltwater air compressors). In total, these loads are approximately sixty horsepower. Note that the SIAS loads are maximized only when the SIAS and UV signals are nearly simultaneous, otherwise, the motor operated valves would have previously changed state. The likelihood of a LOOP – SIAS timed in this manner is considered very small. Thus, the Step 0 load margin is considered the same for either sequencer.

- Load margin is three large loads

The ESFAS undervoltage function is designed to shed the major loads on the safety related buses in the event non-safety related power is lost. The ESFAS SDS/LOCI sequencer then steps the loads on the safety related buses in time increments to prevent overloading the EDGs. The undervoltage function is considered failed when any three loads over one-hundred horsepower fail to shed. This is a relaxation of the design requirements. The design calculations consider that any single load greater than one-hundred horsepower failing to shed during a LOOP will fail the EDG. However, a failure that occurred at CCNPP during an

integrated ESF test resulted in a Fairbanks-Morse EDG picking up significant load. The bus impact was minimal. A three-load failure criteria is a compromise in that it is a slightly higher number of load failures than the design calculation shows as acceptable but much lower than the number of failures seen during an actual plant event in which the EDG performed acceptably. Note that the design calculations incorporate the more severe Step 0 load profile that will likely be implemented for Generic Letter 96-06 (places the service water pumps in Step 0).

- Common cause failure likelihood is unchanged within a unit

The conditional failure likelihood for channels in the same unit is considered unchanged. The requested change in test interval does not alter the existing factors that are relevant to common cause, factors such as equipment total time in service, equipment operating environment, or maintenance practices.

- Full model evaluation

The IESFT simulates SIAS conditions. However, the evaluation for the STI extension request is performed using the Calvert Cliffs internal and external event PSA model: this includes both SIAS and non-SIAS conditions. The evaluation of all initiating events is assumed to produce a more realistic impact evaluation (with higher Δ CDF) than a more limited analysis using only LOCA/SIAS model.

A4.1.4 PSA Model Implementation

Currently, STPs O-4 "A" and "B" are performed each refueling outage (a two year test interval). This tests both Channel A and Channel B ESF equipment. The proposal is to modify STP O-4 such that only a single ESFAS Channel is tested each refueling outage. This doubles the test interval of the equipment not already tested through other tests that is tested in STP O-4.

The equipment that is not tested through other tests but is tested in STP O-4 consists mainly of undervoltage equipment and a few of the SDS/LOCI relays associated with ventilation systems.

If a channel undervoltage function or SDS/LOCI function fails, then the CCPSA model considers that neither the dedicated EDG nor the 0C DG can be loaded onto the associated safety related bus. These ESFAS functions for 4kV Buses 11, 14, 21 and 24 are modeled in Top Events UA, UB, UC and UD (respectively) in the Unit 1 plant model. Top Event GC models that set of events that fails all five EDGs to all the safety related 4kV buses. This set of events includes the failure of all of the undervoltage functions. Additional impacts address the Control Room and Switchgear Room HVAC system Top Events HH and HS.

A general depiction of the model process and discussion follows.

**FIGURE A4.1.4
MODEL PROCESS**



A4.1.4.1 Model Resolution

To ensure adequate model resolution the CC PSA model is quantified with effected top event split fraction base values set to the maximum analyzed case value except as noted below. This precludes the truncation of cutsets that would otherwise fall below the selected truncation threshold when using the base values. Effected top events are treated as follows:

- ESFAS UV Channels (Top Events UA, UB, UC and UD)

For each top event, the independent split fraction base values are doubled to account for the doubled test interval, thirty additional relay failures are added (see discussion at EDG Load Shedding), and one circuit breaker (the 4kV bus feeder breaker) failure to open on demand is added.

Table A4.1.4.1a
Example of Independent Split Fraction Adjustment

Base failure likelihood of Split Fraction UA1	=	3.62E-04
Double of base UA1 failure rate	7.24E-04	(= 3.62E-04 * 2)
Thirty relay failures (BPRL1D)	+ 3.93E-03	(= 1.31E-04 * 30)
One breaker fail to open (BPCB4O)	+ <u>2.11E-04</u>	
Adjusted UA1 failure likelihood	=	4.87E-03

As discussed above in "Assumptions," the conditional failure likelihoods for the ESFAS channel top events (common cause) are considered to remain the same.

Table A4.1.4.1b
Example of Dependent Split Fraction

Base failure likelihood of Split Fraction UB3 (UB given UA failed)	=	2.48E-02
Adjusted base failure likelihood of Split Fraction UB3 (No change)	=	2.48E-02

- Global Common Cause (Top Event GC)

Top Event GC considers the common cause failure of components that fail all EDG top events. Components addressed are the EDGs, the EDG output breakers (fail to close), the ESFAS logic actuation relays associated with load shed, and the bus feeder breaker (fails to open on demand). Only the integrated ESF test undervoltage related components effected by staggered testing are of concern. Although this top event is a major contributor to the CDF it was not increased for the model run. An inspection of base model cutsets shows that Top Event GC has adequate resolution without any failure frequency adjustment.

A4.1.4.2 Model Quantification

Using a Master Frequency File (MFF) modified as described above, the model is quantified using RISKMAN. The resulting sequences are converted into minimal cutsets using the Minimizer. The cutsets are then post processed by the QSS Evaluator using the base MFF values to establish the base CDF and LERF.

All other evaluations are performed using the QSS Evaluator and change file macros that adjust the top event and split fraction values relevant to the specific analysis.

A4.1.5 Analysis Results

This section reports the adjustments and results of the analysis.

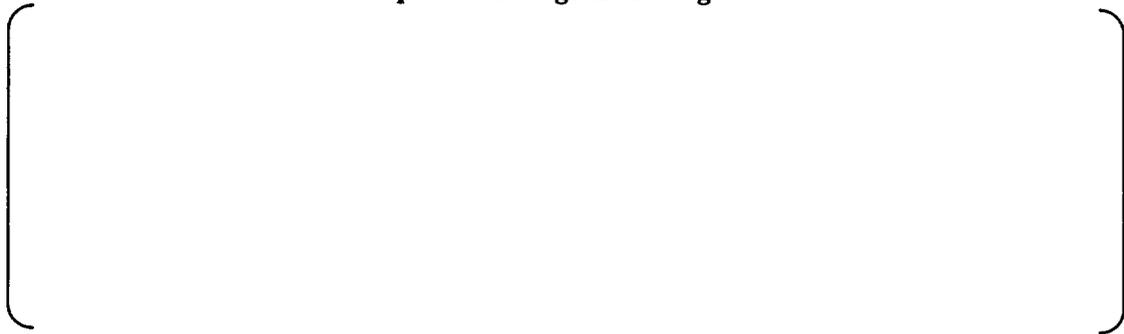
A4.1.5.1 Change in Average Risk

Based on the three load failure criteria (see assumptions):

- The base failure rate for ESF undervoltage channels (Top Events UA, UB, UC and UD) are doubled;
- The EDG global common cause (Top Event GC) ESFAS related components (logic modules, relays, and breakers) in a group of four are changed as explained in Section A4.1.4.1.

The changes are evaluated using the QSS Evaluator and the model described above. The change in average risk was evaluated by comparing the Pre-STI Submittal model with the Post-STI Submittal model.

Table A4.1.5.1a
Expected Change in Average Risk



RG 1.174 provides acceptance guidelines for the change in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). The guidelines are intended for comparison with a full-scope (including internal events, external events, full power, low power, and shutdown) assessment of the change in risk metric.

The guidelines are conditional on the value of the baseline risk metric in that if the CDF is considerably higher than 1.0E-04 per reactor year then the focus should be on finding ways to decrease rather than increase it. CCPSA Revision 1 has a calculated internal and external event CDF of less than 1.0E-04 per reactor year. The guidance considers increases in CDF and LERF that are less than 1.0E-06 and 1.0E-07 respectively as very small. Therefore, the change in average risk is acceptable.

A4.1.5.2 Sensitivity Study Results

A series of sixty-six sets of sensitivity cases have been evaluated per unit to assess the sensitivity of staggered ESFAS testing. The sensitivity cases are based on varying key contributing parameters. Each evaluation compares the pre-staggered case versus the post-staggered case for the varied parameters.

The results of the sensitivity study indicate that there is a high degree of confidence that the staggered ESFAS testing causes less than a 1.0E-06 increase in the CDF and less than a 1.0E-07 increase in LERF.

The sensitivity evaluation is based on varying these key parameters:

- The frequency of a hurricane (Base, Half, Double)
- The frequency of a loss of off-site power (Base, Half, Double)
- The frequency of a loss of a 500kV Bus (Base, Half, Double)
- Whether the RCP motor failure causes a RCP trip without operation action (Yes, No)
- The failure likelihood of the RCP seals (Base, Half, Double)
- The failure likelihood of the operators controlling AFW Flow (Base, Half, Double)

These parameters are developed from a cutset examination. The parameters dominate the cutsets that contain the functions impacted by staggered ESFAS testing. The six RCP seal cases (the two RCP motor trip cases times the three RCP seal failure likelihood cases) are used as the base framework of the sensitivity study. Each of the remaining four parameters are varied individually; two cases each (half and double). This results in a total of fifty-four ($= 2*3 + 4*2*6$) cases for each unit. The twelve additional cases are based on varying the initiating events while varying the RCP modeling and AFW flow control. Each of these cases is evaluated pre-staggered and post-staggered. This results in sixty-six sets of delta core damages for each unit.

Of the parameters evaluated, AFW flow control is the most important. When the human action failure rate is doubled the Δ CDF increases by about eighty percent for both Units 1 and 2. This is by far the most important parameter. AFW flow control during normal loss of decay heat removal scenarios is extremely reliable. Loss of indication or loss of remote flow control capability complicates AFW flow control. The dominant scenarios involve the common cause failure of multiple UV relays or sensors. As this disables multiple EDGs external events are not a big player. Typical LOOP scenarios primarily drive the risk.

For example, during an loss-of-off-site power, a load shed is required on all of the ESF 4kV buses. If the UV system fails globally (that is, Units 1 and 2 Channels A and B), then the EDGs are considered failed (damaged). Without EDGs, the 125VDC batteries lacking charger support will eventually deplete. Without 125VDC power operators would soon be trying to control the turbine driven AFW pumps locally with local indication only.

The next most important parameter is the frequency of Loss-of-Offsite Power (LOOP). When the LOOP frequencies are doubled, the Δ CDF increases by about sixty percent. As discussed, the LOOPS can lead to loss of AFW flow control.

The remaining parameters cause a five to ten percent increase in the Δ CDF for a doubling of the parameter in question.

A4.1.5.3 Maximum Change

The modeling of the UV load relays also plays a major role in the risk associated with staggered ESFAS testing. Currently, it is modeled that failure of three major loads on a single ESF 4kV to shed cause the failure of the EDG. Design calculations indicate that a single major load could fail the EDGs. This is examined by further increasing the doubled base failure rates (see Table A4.1.5.1a, Expected Change in Average Risk) by:

- Adding thirty additional relays and one breaker failure to Top Events UA, UB, UC and UD independent split fraction failure rates
- Adding twenty percent of thirty additional relays and one breaker failure to the GC1 split fraction value. Common cause for this group of four ($\beta * \gamma * \delta$) is conservatively assumed to be twenty percent. The relay β factor is approximately seven percent.

The changes are evaluated using the QSS Evaluator and the model described above. If a single undervoltage load relay causes the failure of the associated EDG, then the increase in risk would be:

Table A4.1.5.3a
Risk given a Single Load would fail a EDG



These results are extremely conservative for numerous reasons.

- The foremost of which is the actual experience of the EDGs where numerous loads where not shed and the EDG quickly returned to rate speed and voltage.
- Both channels of equipment are analyzed in the extended operating period whereas the staggering will result in only one channel actually be operating in the extended time frame at a given time.
- Finally, even if the UV relays fail and cause the failure of all the EDGs (1A, 1B, 2A and 2B), it is possible that operators recognize this and manually shed the ESF buses and then load the OC EDG. This is not credited in the model, but crediting this is likely to reduced the delta risk increases by over fifty percent (judgement based on cutset examination).

Based on the results of the sensitivity study, there is a high degree of confidence that the staggered ESFAS testing causes less than a 1.0E-06 increase in the CDF and less than a 1.0E-07 increase in LERF.

A4.1.6 Impact of Other Pending/Approved Submittals

Three items are identified in this area. Calvert Cliffs has:

- Submitted and received approval for an Integrated Leak Rate Test (ILRT) extension. The ILRT analysis results show only a scalar LERF increase of less than five percent [.]

- Since the Δ LERF is small and scalar, the ILRT submittal will have a negligible interaction with staggered ESF testing and is dismissed from further discussion.
- Submitted an In-Service Inspection (ISI) extension that is pending. The ISI analysis shows a potential small risk reduction. Therefore, an ISI – staggered ESF testing interaction is dismissed from further discussion.
- Submitted (or will soon submit) a EDG Allowed Outage Time (DG AOT) extension request. The IESFT results are re-calculated using the requested DG AOT model adjustments. The results are shown in the table below:

Table A4.1.6a
Change in Average Risk with EDG AOT in Effect

These results show that the proposed EDG AOT does not adversely impact the proposed ESF test interval change.

A4.2 SCOPE OF PSA

The CCPSA is an at-power, internal and external events PSA. Both Level 1 and Level 2 are addressed. The external events considered are fire, seismic, and high wind (hurricanes and tornadoes). Both Units 1 and 2 are modeled. The Unit 1 models were modified with over two hundred changes to provide a risk assessment model that reflects Unit 2.

A4.2.1 At-Power Model Structure

The accident sequences are developed with logic rules relating equipment functions and operator actions to initiating events and to other equipment functions and operator actions. These relationships are developed through the use of RISKMAN software that uses these rules to represent the event trees. An event tree is a logical network that begins with an initiating event and progresses through a series of branches that represent the expected system function or operator action that either succeeds or fails. The system functions or operator actions are referred to as top events. Each rule defines the selection criteria for a split fraction (the conditional failure probability of a top event) or a macro (a function that is set to true or false to indicate a plant status based on its associated rule). The values of the split fractions are contained in a file called a Master Frequency File (MFF). The bases for these values come from various sources including system analysis (fault-trees) and human action analysis.

Several sets of rules (eight models) using nine Master Frequency File values are used to represent the full scope of the CC PSA. These are summarized below:

**Table A4.2.1a
CCPSA Model Structure**

Internal/External	Model	Master Frequency File	Description
Internal	General Transient	Internal	Base file
Internal	LOCA	Internal	Base file
Internal	Steam Line Break	Internal	Base file
Internal	Flood	Internal	Base file
External	Fire – Auxiliary Building	Auxiliary Building	Human actions are degraded to reflect Auxiliary Building fires
		Intake Structure	Human actions are degraded to reflect Intake Structure fires
		Turbine Building (partial)	Human actions are degraded to reflect Turbine Building fires
		Yard Areas	Human actions are degraded to reflect Yard Area fires
External	Fire – Control Room/Cable Spreading Room	Control Room	Human actions are degraded to reflect Control Room fires
		Turbine Building (partial)	Human actions are degraded to reflect Turbine Building fires
External	Seismic	Bin 1	Human actions are degraded to reflect low g levels (0.013g to 0.281gs)
		Bin 2	Human actions are degraded to reflect mid g levels (0.282g to 1.02g)
		Bin 3	Human actions are degraded to reflect high g levels (0.664g to 1.5gs)
External	Wind	Wind	Base file with Wind Impact Top Events Added

Each of the eight models is constructed with a similar structure using six event-tree modules and a Plant Damage State (PDS) bin assignment module. These modules are seamlessly joined as though they are one event-tree within RISKMAN. The dividing point of each module reflects previous software limitations more than model structure concerns.

**Table A4.2.1b
Typical CCPSA Modules within each Model**

GT Modules	Model
SUPPORT1	Support Systems: Primarily Electrical Buses and EDGs
SUPPORT2	Support Systems: Primarily Mechanical Support Systems
GT1	Front-line Systems: Includes reactor and turbine trip functions
GT2	Front-line Systems: Includes AFW and HPSI in the injection mode
LT	Front-line Systems: Long-term: Includes CS and systems for re-circulation
PDS	Plant Damage State: Establishes the plant damage state binning for the Bin Assignment Rules.
Bin Assignment Rules	Uses the PDS Macros to assign core damage sequences to a PDS (each PDS has a fixed fraction associated with LERF)

Note that although the structure for each model is the same, the names for the modules are different.

A4.2.2 Shutdown Risk Assessment

The changes included in the proposed integrated ESF test STI amendment are focused on increasing the flexibility to operate and maintain the plant. Since the integrated ESF test is only performed while the unit is shutdown there is no transition risk associated with the proposed STI amendment.

A4.2.3 PSA Detail Needed for Change

The CCPSA explicitly models the functions associated with ESFAS in both the Units 1 and 2 PSA models. Key modeling features are discussed below.

A4.2.3.1 Event-Tree Modeling

Unit-to-Unit Interaction

To effectively model the role of the opposite unit ESFAS, both unit PSAs include all four ESFAS undervoltage/sequencer functions and associated electrical/mechanical systems. The model also includes the consideration that some initiators cause both units to trip (for example, LOOP, hurricane, some fires, loss of 125VDC Bus 11, etc.).

Common Cause

The ESFAS undervoltage/sequencer channel top events are modeled using common cause within the unit. The cross-unit common cause is modeled within the EDGs (including 0C DG) using a separate top event (Top Event GC) within the event tree. If this top event fails, then all the EDGs are set to failure. Top Event GC considers the potential for common cause failure of the 4kV feeder breakers or the common cause failure of multiple load shed relays.

This comprehensive treatment of common cause is not limited to the EDGs. This approach is used throughout the CCPSA. Other key common cause impacts related to the EDGs are 125VDC batteries, SRW pumps, SW pumps, ESFAS UV channels, 4kV load breakers and 120 VAC inverters.

A4.2.3.2 Truncation Limits

For each initiating event the CCPSA quantification process post-processes the RISKMAN sequence output to obtain accurate CDF/LERF values with a sufficient number of sequences to ensure resolution while simplifying the sequence results. The CDF and LERF values associated with each initiating event are extrapolated such that the CDF/LERF has less than a one-percent change in CDF/LERF for a decade deeper truncation limit.

The truncation limits are set per-initiating event based on the post-processed results. These truncation limits vary from 1.0E-10 to 1.0E-15.

A4.2.4 Base PSA Results

The base CCPSA used for this proposed amendment contains both internal and external events for Units 1 and 2. Table A4.2.4a shows the results of the Units 1 and 2 CCPSA Revision 1 model.

**Table A4.2.4a
CCPSA Revision 1 Results**



A4.3 QUALITY OF CCNPP PSA

CCNPP utility personnel have constructed the CCPSA with a strong commitment toward developing a complete and accurate PSA. This commitment can be seen through the following elements:

- Formal qualification program for the PSA staff
- Use of procedures to control PSA processes
- Independent reviews (checks) of PSA documents
- Comprehensive PSA Configuration Control Program
 - Quarterly plant change monitoring program
 - Process to control PSA quantification software
 - Active open items list
 - Interface with the site corrective action program
 - Process to maintain configuration of previous risk-informed decisions
- Peer reviews
- Participation in the CEOG cross comparison process
- Incorporation, where applicable, of CEOG PSA Technical Positions
- Commitment of continuous quality improvement

The CCPSA Revision 0 was peer reviewed in November 2001. The CC PSA Revision 1 Model contains several refinements, but uses techniques and practices similar to the peer reviewed revision.

A4.4 PSA SOFTWARE

A combination of commercial and in-house software programs are used for this analysis. All software executes on safety-related/configuration controlled computers.

A4.4.1 Riskman

The primary event-tree quantification computer program, RISKMAN Version 2.0 for Windows, used to support the CCPSA, is classified as safety-related. RISKMAN Version 5.0 for Windows, also classified as safety-related, was used for some fault tree requantification. RISKMAN is a commercial product.

A4.4.2 Minimizer Version Z

The Minimizer removes guaranteed failed top events and the success top events from the sequences and Boolean reduces the number of sequences. This minimization has the advantage of reducing the total number of sequences, reducing their complexity and improving the amount of risk contribution captured for a given truncation level. The results resemble cutsets in that each accident sequence contains only the initiating event and the split fractions that independently failed. The output of the Minimizer is a set of core damage cutsets and a set of LERF cutsets. These files are the input to the QSS Evaluator.

The Minimizer also automates many of the steps used in determining the proper truncation limit. This software is classified safety-related. Formal verification and validation of the changes made to enable this analysis, the ability to handle multiple models (internal events, fire, seismic, etc.) was in progress at the time of this submittal.

A4.4.3 QSS Evaluator Version P

The QSS Evaluator is a software tool that quantifies the CCPSA model using a set of minimized sequences. Its primary function is for the calculation of Maintenance Rule (a)4 risk assessment. The QSS Evaluator was used for the risk assessment of this proposed amendment to determine the change in the risk metrics resulting from implementation of the proposed ESF STI extension and for the included sensitivity studies.

This software is classified as safety-related. Formal verification and validation has been completed and documented consistent with the site processes and procedures.

A4.5 RESULTS AND CONCLUSIONS

The risk contribution associated with changing the integrated ESF test frequency from once per refueling outage (sequential basis) to once every other refueling outage (staggered basis) has been quantitatively evaluated using the current plant-specific probabilistic risk assessment for Calvert Cliffs Units 1 and 2. The change results in a small, but acceptable, risk increase. There is also some risk reductions associated averting unnecessary plant transients and with reduced risk during shutdown operations, however, these reductions were not quantified.

APPENDIX B

APPLICATION OF WCAP-15830-NP TO FORT CALHOUN STATION

TABLE OF CONTENTS

B1.0	ABSTRACT	B-4
B2.0	BACKGROUND	B-5
B2.1	ESCS Description	B-5
B2.1.1	ESCS Initiating Signals.....	B-5
B2.1.2	Actuation Subsystems.....	B-6
B2.1.3	Engineered Safeguards Control Panels AI-30A and AI-30B.....	B-7
B2.2	Fort Calhoun Configuration.....	B-8
B2.2.1	EDGs.....	B-8
B2.2.2	EDG Load Shedding	B-8
B2.3	Current Technical Specifications	B-9
B2.4	Proposed Changes to Technical Specifications.....	B-11
B3.0	TEST MATRIX AND COMPONENT CATEGORIZATION.....	B-12
B3.1	Method Discussion.....	B-12
B3.1.1	Integrated ESF Testing at FCS.....	B-12
B3.2	Input.....	B-15
B3.3	Evaluation, Analyses and Results	B-19
B4.0	PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE.....	B-28
B4.1	Model Analysis	B-28
B4.1.1	Discussion of Major Assumptions	B-28
B4.1.2	Acceptance Criteria.....	B-32
B4.1.3	Computer Codes Used in Analysis	B-32
B4.2	Scope of FCS PSA.....	B-32
B4.2.1	At-Power Model Structure.....	B-32
B4.3	Quality of FCS PSA.....	B-34
B4.4	PSA Software.....	B-34
B4.4.1	CAFTA	B-34
B4.4.2	PRAQuant.....	B-34
B4.4.3	FORTE.....	B-35
B4.5	Results and Conclusions	B-35

LIST OF TABLES

B2.2.1a	Emergency EDGs.....	B-8
B2.3a	Existing Surveillance Test Intervals.....	B-9
B2.4a	Proposed Surveillance Test Intervals	B-11
B3.1a	Applicable Database Fields	B-13
B3.2a	ESF Surveillance Test Procedures.....	B-15
B3.3a	Categorization Summary for Fort Calhoun Station.....	B-19
B4.5a	FCS Results.....	B-35

LIST OF FIGURES

B3.3-1	SIAS Surveillance Procedures – Fort Calhoun Station	B-20
B3.3-2	CIAS Surveillance Procedures – Fort Calhoun Station	B-21
B3.3-3	CSAS Surveillance Procedures – Fort Calhoun Station	B-22
B3.3-4	RAS Surveillance Procedures – Fort Calhoun Station	B-23
B3.3-5	SGIS Surveillance Procedures – Fort Calhoun Station	B-24
B3.3-6	VIAS Surveillance Procedures – Fort Calhoun Station.....	B-25
B3.3-7	Sequence Surveillance Procedures – Fort Calhoun Station.....	B-26
B3.3-8	OPLS Surveillance Procedures – Fort Calhoun Station	B-27

B1.0 ABSTRACT

Combustion Engineering Owners Group (CEOG) Task 2016, "Staggered Integrated ESF Testing," used a risk-Informed approach to demonstrate that any change in risk would be negligible if a staggered test frequency were adopted for integrated Engineered Safety Features (ESF) testing. Currently, integrated ESF testing is performed on both trains each refueling cycle. Using a staggered approach, only one train would be tested each refueling outage. The basic premise of the proposed change is the belief that the integrated ESF test is not the primary/sole operability test for the majority of the components tested. Other surveillance procedures are performed on many of these components and functions on the same or more frequent basis. Therefore, there may be considerable overlap between the integrated ESF test and other testing. For the components/functions that are tested only by the integrated ESF test, the risk model was adjusted, the risk associated with the change recalculated, and the overall risk requantified. In some cases, it was possible to develop a reasonable deterministic basis for assuming the component failure mode addressed by the integrated ESF test was not risk-significant. These components were exempt from further Probabilistic Safety Analysis (PSA) review and analysis. The overall task was broken down into more manageable units of work. The first was the procedure review and matrix development. The second was the categorization of components and functions tested by the integrated test. Third was the preliminary PSA assessment and Category "A" component sub-categorization. Last was the finalization of the PSA assessment, adjusting the PSA models and calculating the change in risk associated with the change in Surveillance Test Interval (STI).

This Appendix addresses application of staggered integrated ESF testing at Fort Calhoun Station (FCS). It describes in detail the plant specific procedure review, component categorization and risk analyses as performed for FCS to support the change to staggered integrated ESF testing. The FCS Station Technical Specification Surveillance Requirements addressed by integrated ESF testing are listed in Table B2.3a.

The risk contribution associated with the increased frequency, 18 months on a staggered bases, has been quantitatively evaluated using the current plant-specific PSA for FCS. Based on the changes in CDF and LERF the risk impact of extending the Integrated Engineered Safety Features test from once per fuel cycle on a sequential basis, to once every other fuel cycle on a staggered basis is not significant. The change results in a small, but acceptable, risk of core damage increase. There is also some risk reductions associated with averting unnecessary plant transients and with reduced risk during shutdown operations, however, these reductions were not quantified.

B2.0 BACKGROUND

The Engineered Safety Features system functions are controlled by the Safeguards Controls System (ESCS). Engineered Safeguards Equipment include Engineered Safety Features Systems, Essential Auxiliary Support Systems and Engineered Safeguards Controls and Instrumentation. A non-CE designed ESCSs is in place at FCS.

B2.1 ESCS DESCRIPTION

The Engineered Safeguards control and instrumentation system was designed to actuate safeguards and essential support systems automatically. Means for manual operation are also provided. The system includes control devices and circuits for automatic initiation, control, supervision and manual test of the Engineered Safeguards systems.

The control system was designed and installed as two, independent, functionally redundant systems called the "A" train and the "B" train. These trains are segregated physically and electrically throughout the plant. Cross connections between trains are held to the unavoidable minimum, and such connections are buffered and arranged to prevent communication of faults. In each train, the logic basis for initiation signals is two-out-of-four, with the exception of containment radiation high which is one-out-of-two.

Automatic sequencers for starting safeguards pumps, fans and support auxiliaries are duplicated in each of the A and B trains. Each of the four sequencers operates with a separate control power source and distribution system. Any one sequencer operating alone automatically actuates minimum set of safeguards equipment.

The following is a brief description of ESCS.

B2.1.1 ESCS Initiating Signals

Safeguards actuation signals result from the logical combination of initiating signals each of which is derived from a departure from the normal operating range (above or below the setpoint depending on the application) of one of the following critical parameters:

- Reactor coolant pressure (low-low) - PPLS
- Containment internal pressure (high) - CPHS
- Containment atmosphere radionuclide content (high) - CRHS
- Borated water tank level (SIRW tank low-low) - STLS
- 4kV bus voltage
- Steam generator pressure
- Steam Generator level

Initiating signals are logically combined to effect the required responses of safeguards and support systems. In every instance, two identical actuation signals are developed and applied separately via the functionally redundant A and B control trains.

B2.1.2 Actuation Subsystems

Two redundant and independent actuation systems monitor the sensor outputs and, using two out of four coincident logic, initiate the required protective action. Either train (A or B) controls sufficient equipment to protect the public from a loss of coolant incident, main steam line break, or loss of power incident.

B2.1.2.1 Actuation Inputs

ESCS sensor and actuation channels produce signals to initiate equipment operation consistent with the type of protective action required. At FCS the system is active, i.e. the system needs electric power to actuate the various ESCS signals. Actuation channels include the following actions:

- Safety Injection Actuation Signal (SIAS)
- Containment Spray Actuation Signal (CSAS)
- Containment Isolation Actuation Signal (CIAS)
- Recirculation Actuation Signal (RAS)
- Containment Radiation High Signal (CRHS)
- Steam Generator Isolation Signal (SGIS)
- Offsite Power Low Signal (OPLS)
- Auto-Start of EDGs
- Sequential Starting of ESF Equipment
- Ventilation Isolation Actuation Signal (VIAS)
- Auxiliary Feedwater System

B2.1.2.2 Actuation Output

The plant equipment to ESCS interface is accomplished using power relays. The relay coils are controlled by the actuation logic modules. Relay contacts provide the equipment switching function required for equipment control as well as isolation from other plant equipment and ESCS internal components.

B2.1.2.3 Auto-Start of EDG and Sequencer Operation

Automatic starting of Emergency Diesel Generators (EDGs) DG-1 and DG-2, is initiated by either a PPLS or a CPHS. If acceptable voltage were available at 4.16kV buses 1A3 and 1A4 from their normal 161-KV off-site power source, the EDGs are not connected to buses 1A3 and 1A4 but are run in reserve at idle speed. A PPLS or a CPHS also initiates load shedding of selected 4.16kV and 480-Volt loads.

With no SIAS signal present, if the voltage on either bus 1A3 or 1A4 were less than a predetermined value, the bus with inadequate voltage has to be disconnected from its normal sources. Motors and nonessential auxiliaries (i.e. lighting transformers) directly connected to that 4.16kV bus or to 480-Volt switch gear buses supplied by that bus are disconnected from the system as the associated EDG runs up,

and when the EDG speed and voltage reach operating range, the generator circuit breaker is closed automatically. Equipment loads are then connected manually.

When the SIAS signal is present, and if the voltage on bus 1A3 or 1A4 is less than a predetermined value, both buses are disconnected from the normal supply, unneeded loads at 4.16kV and 480-volts are disconnected from the system automatically as the EDG run up, and, when EDG speed and voltage reach operating range, the generator breakers are closed and the safeguards loads connected sequentially. The EDGs will not operate in parallel, (there being no bus-tie breaker between 4.16kV buses 1A3 and 1A4, and interlocks prevent interconnection at the 480-Volt level), to ensure the two systems supplying safeguards are independently operated.

If acceptable voltage is available at 4.16kV buses 1A3 and 1A4 from their normal off-site power source when a PPLS or a CPHS signal occurs, safeguards loads are started automatically and sequentially in groups with minimum initial delay.

The load connection sequence is the same whether off-site normal or on-site emergency power supply is used. When a EDG is used there is an additional delay after the initiating safeguards signal before load sequencing is started. The delay provides time during which the unit is run up and direct connected motor loads are shed.

If load sequencing were started with off-site power available and that supply were to fail, then the EDGs (idling in standby) are automatically run up to operating speed, loads are shed, and load sequencing repeated to restart loads.

All Component Cooling Water Pumps, Raw Water Pumps, Charging Pumps, and Containment Air Recirculation and Cooling Unit Fans are included in the basic sequence of loads automatically started in response to a DBA that actuates both PPLS and CPHS. These components have both normal and emergency functions. In the emergency mode, all available units in these categories are started; unneeded units may be subsequently shutdown manually by the operator.

B2.1.3 Engineered Safeguards Control Panels AI-30A and AI-30B

Two functionally redundant safeguards control trains, A and B, are provided to ensure high reliability and effective in-service testability. The A and B trains were designed for individual reliability and maximum attainable mutual independence both physically and electrically. Either train, operating alone, can automatically actuate the minimum set of safeguards and essential supporting systems.

A and B train segregation begins at the contact inputs to the trains. Such contacts, primary sensor or transmitter outputs, are arranged in individual A and B train logic matrices which produce Engineered Safeguards actuation signals. Physical and electrical segregation of the trains is carried out to remote A and B auto-start relays of the individual Safeguards loads. Contacts on A and B relays are wired in parallel into circuit breaker control circuits to ensure automatic start on demand.

Engineered Safeguards control panels AI-30A and AI-30B, installed in the control room, house the bulk of the control equipment for the A and B trains, respectively. Devices not installed in the panels include primary sensors and transmitters, individual equipment control circuits and load auto-start relays.

Panel assemblies AI-30A and AI-30B are separate structures. They are installed in the control room to provide direct access by the plant operators and a favorable, controlled environment at all times. Control

devices are conventional control switches, lamp indicators, time delay relays and electro-magnetic relays. Each panel assembly is subdivided into separate enclosures. Control power buses are carried across the top of the panel assemblies and each is in a separate enclosure and electrically insulated throughout.

B2.2 FORT CALHOUN CONFIGURATION

The ESCS functions start/align equipment required to mitigate design basis accidents. A critical aspect of the ESCS design addresses the loss of the normal (off-site) power supply.

B2.2.1 EDGs

At FCS, the two 4.16kV ESF buses are each supplied by a dedicated EDG. The table below shows the EDG to bus alignment and naming convention:

**Table B2.2.1a
Emergency Diesel Generators**

Emergency Diesel Generator	Manufacturer	4kV Bus	Channel Supported
DG-1	Fairbanks-Morse	1A3	A
DG-2	Fairbanks-Morse	1A4	B

B2.2.2 EDG Load Shedding

Automatic load shedding involves the following methods depending on the load category:

- a. The FCS Electrical Distribution System is equipped with an undervoltage relay protection scheme, which insures that adequate voltage exists on the station buses to permit safe reactor shutdown and maintain the reactor in a safe shutdown condition under all grid conditions. To accomplish this, a Loss of Voltage protection scheme is installed on 4.16kV buses 1A1, 1A2, 1A3 and 1A4. A degraded voltage protection scheme referred to as the Offsite Power Low Signal (OPLS) protection scheme is installed on the 4.16kV buses 1A3 and 1A4 to provide protection during accident conditions.

An undervoltage relay scheme is installed on the 480V buses. This 480V scheme provides motor protection and works in conjunction with both 4.16kV relay schemes. The 480V undervoltage relays are not actuated by the 4.16kV relays. Load shed initiation is based on the 480V bus voltage.

The loss of voltage scheme operates on a two-out-of-two-logic on all four 4.16kV buses in the event that bus voltage degrades due to degraded grid conditions. The relays act to protect large 4.16kV motors. If the station bus voltage were to fall below the relay setpoint (an inverse time vs. voltage characteristic), the buses will be load shed. Buses 1A3 and 1A4 will then be reenergized by DG-1 and DG-2 respectively.

The 480V undervoltage relays act (in a two out of two logic) independently to protect the large 480V motors and will, in addition, act to load shed the large 480V loads during the time the

EDGs are accelerating to full speed. The EDGs may then be loaded manually by the operator to maintain the plant in a safe shutdown condition.

The OPLS degraded voltage relay system provides undervoltage protection in the event of an accident in which Safety Injection is required. The OPLS lock-out relay is armed whenever the SIAS actuates. The OPLS scheme is based on a two out of four logic to actuate. The OPLS setpoints ensure that adequate voltage exists on the 4.16kV and 480V voltage levels to insure that the safety related loads which are sequenced on will have adequate voltage to accelerate to rated speed and operate within nameplate voltage limits.

In case the grid voltage falls below the OPLS setpoint, the same 4.16 kV relays which are actuated by the loss of voltage scheme will be actuated. This will load shed the 4.16kV safety buses (done independently) and at approximately the same time the 480V undervoltage relays will load shed the large 480V loads. The OPLS signal also directly (not through an undervoltage relay) load sheds selected nonessential 480V loads. Because an accident signal is present, the Engineered Safeguards load sequencers will be reset. When the EDG has accelerated to full speed and energized the bus, the sequencers will time back out automatically starting necessary Engineered Safeguards loads to maintain the reactor in a safe shutdown condition.

- b. In the event of a PPLS or CPHS, the resulting SIAS initiates shedding of selected non-essential waste disposal system loads which are supplied from 480-Volt motor control center. The SIAS actuation signal also initiates shedding of additional selected non-essential loads supplied from 480-Volt motor control centers as well as shedding of complete 480-Volt motor control centers serving loads which are not essential to support Engineered Safeguards systems. The load shed circuitry initiated by the SIAS signals is located in Load Shed panels AI-109A and AI-109B (East Electrical Switchgear Room).

B2.3 Current Technical Specifications

Table B2.3a lists all the Technical Specification Surveillance Requirements that apply to integrated ESF testing at FCS.

Table B2.3a Existing Surveillance Test Intervals		
SR	SR Description	Frequency
T.S.3.1, Table 3-2, Item 3b	Verify Safety Injection Actuation Logic.	18 months
T.S.3.1, Table 3-2, Item 5b	Verify Containment Spray Actuation Logic.	18 months
T.S.3.1, Table 3-2, Item 8a	Verify Isolation Valve Closure.	18 months
T.S.3.1, Table 3-2, Item 8b	Verify manual Containment Isolation Actuation.	18 months
T.S.3.1, Table 3-2, Item 9	Verify manual Containment Spray Actuation.	18 months
T.S.3.1, Table 3-2, Items 19	Verify manual Recirculation Actuation.	18 months
T.S.3.1, Table 3-2, and 20(b)	Verify Recirculation Actuation Logic.	18 months
T.S.3.1 Table 3-2,	Verify manual Emergency Off-site Power Low Trip Actuation	18 months

Table B2.3a		
Existing Surveillance Test Intervals		
SR	SR Description	Frequency
Item 22		
T.S. 3.2, Table 3-5, Item 10a.4	Verify automatic and manual actuation of Control Room Emergency Cleanup System.	18 months
T.S.3.2, Table 3-5, Item 14	Verify Pressurizer Heater control circuit operation for post-accident use.	18 months
T.S.3.6 (1)	Verify that the Safety Injection system will respond promptly and perform its intended functions.	18 months
T.S.3.6 (2)	Verify that the Containment Spray system will respond promptly and perform its intended functions.	18 months
T.S.3.6 (3)	Verify that the Containment Recirculating Air Cooling and Filtering System will respond promptly and perform its intended functions.	18 months
T.S.3.7(1)c and 3.7(1)d	<p>Verify satisfactory overall automatic operation of each EDG system. This test shall be conducted by:</p> <ul style="list-style-type: none"> i. Initiation of a simulated auto-start signal to verify that the EDG starts, followed by, ii. Initiation of a simulated simultaneous loss of 4.16 kV supplies to bus 1A3 (1A4). Proper operation will be verified by observation of: (1) De-energization of bus 1A3 (1A4), (2) Load shedding from bus (both 4160 V and 480 V), (3) Energization of bus 1A3 (1A4), (4) Automatic sequence start of emergency load and (5) Operation of > 5 minutes while its generator is loaded with the emergency load. iii. Verification that emergency loads do not exceed the 2000-HR kW rating of the engine. d. Manual control of EDGs and breakers shall also be verified during refueling shutdowns. 	18 months
T.S.3.8	Verify the ability of the main steam isolation valves to close upon signal.	18 months

B2.4 PROPOSED CHANGES TO TECHNICAL SPECIFICATIONS

Table B2.4a shows the proposed TS changes that apply to FCS. The proposed frequency is based on the FCS TS definition for staggered testing.

Table B2.4a
Proposed Surveillance Test Intervals

SR	SR Description	Frequency
T.S.3.1, Table 3-2, Item 3b	Verify Safety Injection Actuation Logic.	18 months on a Staggered Bases
T.S.3.1, Table 3-2, Item 5b	Verify Containment Spray Actuation Logic.	18 months on a Staggered Bases
T.S.3.1, Table 3-2, Item 8a	Verify Isolation Valve Closure.	18 months on a Staggered Bases
T.S.3.1, Table 3-2, Item 8b	Verify manual Containment Isolation Actuation.	18 months on a Staggered Bases
T.S.3.1, Table 3-2, Item 9	Verify manual Containment Spray Actuation.	18 months on a Staggered Bases
T.S.3.1, Table 3-2, Items 19	Verify manual Recirculation Actuation.	18 months on a Staggered Bases
T.S.3.1, Table 3-2, and 20(b)	Verify Recirculation Actuation Logic.	18 months on a Staggered Bases
T.S.3.1 Table 3-2, Item 22	Verify manual Emergency Off-site Power Low Trip Actuation	18 months on a Staggered Bases
T.S. 3.2, Table 3-5, Item 10a.4	Verify automatic and manual actuation of Control Room Emergency Cleanup System.	18 months on a Staggered Bases
T.S.3.2, Table 3-5, Item 14	Verify Pressurizer Heater control circuit operation for post-accident use.	18 months on a Staggered Bases
T.S.3.6 (1)	Verify that the Safety Injection system will respond promptly and perform its intended functions.	18 months on a Staggered Bases
T.S.3.6 (2)	Verify that the Containment Spray system will respond promptly and perform its intended functions.	18 months on a Staggered Bases
T.S.3.6 (3)	Verify that the Containment Recirculating Air Cooling and Filtering System will respond promptly and perform its intended functions.	18 months on a Staggered Bases
T.S.3.7(1)c and 3.7(1)d	Verify satisfactory overall automatic operation of each EDG system. This test shall be conducted by: i. Initiation of a simulated auto-start signal to verify that the EDG starts, followed by, ii. Initiation of a simulated simultaneous loss of 4.16 kV supplies to bus 1A3 (1A4). Proper operation will be verified by observation of: (1) De-energization of bus 1A3 (1A4), (2) Load shedding from bus (both 4160 V and 480 V), (3) Energization of bus 1A3 (1A4), (4) Automatic sequence start of emergency load and (5) Operation of > 5 minutes while its generator is loaded with the emergency load. iii Verification that emergency loads do not exceed the 2000-HR kW rating of the engine. d. Manual control of EDGs and breakers shall also be verified during refueling shutdowns.	18 months on a Staggered Bases
T.S.3.8	Verify the ability of the main steam isolation valves to close upon signal.	18 months on a Staggered Bases

B3.0 TEST MATRIX AND COMPONENT CATEGORIZATION

B3.1 METHOD DISCUSSION

B3.1.1 Integrated ESF Testing at FCS

The following is a brief description of the functions tested by each of the FCS surveillance procedures that are considered part of integrated ESF testing. Testing is performed on both trains, one train at a time, every 18 months.

Objectives (functions) covered by OP-ST-ESF-0002:

- Load Shed Verification
- EDG Start on Auto-Start Verification
- OPLS with ESF Actuation Verification
- Return to Normal Offsite Power
- DG Load Sequence Verification

Objectives (functions) covered by OP-ST-ESF-0006:

- OPLS with ESF Actuation Verification

Objectives (functions) covered by OP-ST-ESF-0011:

- Automatic SIAS Actuation Verification
- Manual SIAS Actuation Verification
- Automatic CIAS Actuation Verification
- Manual CIAS Actuation Verification
- Automatic CSAS Actuation Verification
- Manual CSAS Actuation Verification
- Automatic VIAS Actuation Verification
- Manual VIAS Actuation Verification
- Automatic SGIS Actuation Verification
- ESF Actuation Override Verification
- ESF Response Time Verification
- DG Load Sequence Verification

Objectives (functions) covered by OP-ST-ESF-0013:

- Manual SGIS Actuation Verification
- ESF Actuation Override Verification

Objectives (functions) covered by OP-ST-ESF-0019 are:

- Automatic RAS Actuation Verification

An ESF Testing Matrix was prepared by Westinghouse for FCS as part of CEOG Task 2016, Staggered Integrated ESF Testing. A database was used to create the matrix and to document the results of the ESF procedure review. The primary function of the database was to map the components tested by FCS integrated ESF test procedures to other surveillances that test the same components and functions.

The database contains references to the integrated ESF test and other tests, as well as a preliminary PSA evaluation and assessment. The preliminary PSA assessment performed by Westinghouse provided the foundation for the plant specific PSA calculation performed by FCS.

The following table defines the procedure review portion of the database used to develop the matrix. PSA evaluations and assessments are addressed in Section B4.0 of this appendix.

**Table B3.1a
Applicable Database Fields**

Column Heading	Explanation
Component Type	General component category
Component ID	Component ID used in surveillance procedure
Component Description	Component description used in surveillance procedure
Integrated test Procedure	Surveillance test associated with the entries to the right
Functions tested by the Integrated tests	The large blue section of the database shows the location in the integrated test procedures where testing of a particular component was identified for a particular ESF function. For each component, the database shows the position verified. A blank field indicates that the component / function is not tested by the integrated ESF test.
Integrated test Summary	Summarizes the functions tested by the integrated test procedures for each component.
Cat	Component category, "A", "B" or "C". Categories are defined and explained below. The initial PSA assessment further divides Category "A" components into A-1, A-2, A-3 or A-4 to facilitate requantification of risk by FCS. The screening process used to sort components into subcategories is described in Section 4.0 of the topical report and is related specifically to FCS.
Assessment	An initial assessment that supports why the component is initially categorized "A", "B" or "C". Where there are multiple records for the same component, the 'Assessment' is recorded only for the first record.
Comments	Reviewer notes relative to the assessment.
Other Test 1 through 5	Lists references to other FCS surveillance procedures that overlap the integrated test procedures.

The matrix was developed as follows: First, each of the subject surveillance procedures were reviewed to identify the components and functions being tested and the results entered into the database. To facilitate future sorting of the data, the component type, system identifier and number, and associated TS surveillance requirement were also added. To facilitate locating the component being tested, the procedure step or attachment was also recorded. Under each applicable function, the component end condition following the test was entered. Following the individual functions, a summary of all the functions tested was added. Fields that are not needed to support this appendix have been hidden.

Once all components and functions tested by the integrated ESF test were identified, other related TS surveillance tests were reviewed to determine whether or not they tested any of the same components tested by the integrated ESF test on the same or more frequent bases. During this review, care was taken to ensure that the other more frequent TS surveillance test demonstrated operability of the same

component and tested the same function. Those tests that satisfied the criteria were logged under an 'other test' column adjacent to the specific component. After reviewing all the candidate 'other test' procedures provided, Westinghouse made an assessment as to whether or not the integrated ESF test was the sole/primary test for each component. An initial categorization of the components was then made. The 'categories' are defined as follows:

- Category A The integrated test is the sole/primary test that demonstrates the operability or function of these components. These components perform an engineered safety function. The PSA model addresses (or should address) failure of these components. They may be modeled explicitly, modeled via a subsuming component, or modeled via a surrogate event.

- Category B Similar to Category A, the integrated test is the sole/primary test that demonstrates the operability or function of these components. Unlike the Category A components, the Category B components are not included in the PSA model. Failure of these components therefore does not affect the calculated risk. The rationale for excluding them from the model is provided in the database. For example, valves which are normally in their safeguards-actuated position may not be modeled because the safeguards signal is "confirmatory" - the signal is necessary only if the event should occur while the associated system is in an unusual or infrequent configuration.

- Category C The integrated test is not the sole/primary test that demonstrates the operability or function of these components. Other, more frequently performed surveillance tests ensure that changes to the integrated test frequency would not affect the failure probabilities for these components.

The Category 'A' and 'B' components then became the focus and were reviewed further to determine the PSA impact. The PSA review and analyses are documented in Section B4.0.

B3.2 Input

Westinghouse used electronic copies of current TS surveillance procedures provide by FCS on a Compact Disc (CD) to perform the review and develop the matrix database (refer to Table B3.1a for an explanation of the key fields in the database). The following table provides a list of the surveillance procedures included in the review, including the integrated ESF procedures:

Table B3.2a ESF Surveillance Test Procedures		
Procedure Number	Procedure Title	Frequency
OP-ST-ESF-0002, R23	EDG NO. 1 AND NO. 2 AUTO OPERATION	Once every 18 months
OP-ST-ESF-0011, R22	CHANNEL A AND B AUTOMATIC AND MANUAL ENGINEERED SAFEGUARD ACTUATION SIGNAL TEST	Once every 18 months
OP-ST-ESF-0013, R8	CHANNELS A AND B STEAM GENERATOR ISOLATION SIGNAL ACTUATION TEST (SGIS)	Once every 18 months
OP-ST-ESF-0019, R11	RECIRCULATION ACTUATION SIGNAL LOGIC AND SWITCH TEST	Once every 18 months
OP-ST-ESF-0006, R17	ENGINEERED SAFETY FEATURES OFF-SITE POWER LOW SIGNAL (OPLS) FUNCTIONAL TEST	Once every 18 months
EM-ST-ESF-0001, R7	QUARTERLY ENGINEERED SAFETY FEATURES OFFSITE POWER LOW SIGNAL (OPLS) SENSOR CHECK	Once every Quarter
EM-ST-RC-0001, R5	PRESSURIZER HEATERS CONTROL CIRCUIT OPERATIONAL TEST	Once every 18 months
IC-ST-AFW-0001, R8	AUTO INITIATION OF AUXILIARY FEEDWATER FUNCTIONAL CHECK OF INITIATION CIRCUITS	Once every 92 Days
IC-ST-ESF-0001, R7	FUNCTIONAL TEST OF PRESSURIZER PRESSURE LOW SIGNAL (PPLS) ACTUATION AND BLOCKING LOGIC	Once every 18 months
IC-ST-ESF-0002, R9	LOGIC CHANNEL TEST OF CONTAINMENT PRESSURE HIGH SIGNAL (CPHS)	Once every 18 months
IC-ST-ESF-0003, R5	FUNCTIONAL TEST OF STEAM GENERATOR LOW PRESSURE SIGNAL (SGLS)	Once every 18 months

Table B3.2a		
ESF Surveillance Test Procedures		
Procedure Number	Procedure Title	Frequency
IC-ST-ESF-0004, R4	CHANNEL FUNCTIONAL TEST OF CONTAINMENT PRESSURE HIGH SIGNAL (CPHS) SWITCHES	Once every 92 Days
IC-ST-ESF-0005, R4	QUARTERLY FUNCTIONAL TEST OF PRESSURIZER PRESSURE LOW SIGNAL P-102 CHANNELS	Once every 92 Days
OP-FT-DG-0001, R6	MASTER ELECTRICAL SWITCH 183-MES/D2 FUNCTIONAL TEST	Once every 18 months
OP-FT-DG-0002, R9	EMERGENCY EDG ENDURANCE FUNCTIONAL TEST	Once every 18 months
OP-ST-AFW-0004, R21	AUXILIARY FEEDWATER PUMP FW-10 OPERABILITY TEST	Once every 18 months
OP-ST-AFW-0006, R4	AFW OPERABILITY VERIFICATION FROM AI-179	Once every 18 months
OP-ST-DG-0001, R34	EDG 1 CHECK	Once every month
OP-ST-DG-0002, R35	EDG 2 CHECK	Once every month
OP-ST-ESF-0001, R18	DIESEL AUTO START INITIATING CIRCUIT CHECK	Once every Startup
OP-ST-ESF-0008, R18	13.8 KV EMERGENCY POWER PERIODIC TEST	Once every 18 months
OP-ST-ESF-0009, R35	CHANNEL A SAFETY INJECTION, CONTAINMENT SPRAY AND RECIRCULATION ACTUATION SIGNAL TEST	Once every 92 Days
OP-ST-ESF-0010, R33	CHANNEL B SAFETY INJECTION, CONTAINMENT SPRAY AND RECIRCULATION ACTUATION SIGNAL TEST	Once every 92 Days
OP-ST-ESF-0015, R14	480 VOLT LOAD SHED AND ENGINEERED SAFEGUARDS ACTUATION SIGNAL RETEST	Once every 18 months
OP-ST-ESF-0022, R18	S1-2 AUTOMATIC LOAD SEQUENCER TEST	Once every 92 Days
OP-ST-ESF-0023, R19	S2-2 AUTOMATIC LOAD SEQUENCER TEST	Once every 92 Days
OP-ST-CH-3003, R34	CHEMICAL & VOLUME CONTROL SYSTEM PUMP/CHECK VALVE INSERVICE TEST	Once every 92 Days

Table B3.2a		
ESF Surveillance Test Procedures		
Procedure Number	Procedure Title	Frequency
OP-ST-CH-3005, R12	CHEMICAL AND VOLUME CONTROL SYSTEM (CVCS) CATEGORY A AND B VALVE EXERCISE TEST	Once every 18 months
OP-ST-RW-3002, R8	RAW WATER SYSTEM CATEGORY A AND B VALVE EXERCISE TEST	Once every 92 Days
OP-ST-CCW-3001, R6	COMPONENT COOLING CATEGORY B VALVE EXERCISE TEST	Once every 92 Days
OP-ST-BD-3000, R7	BLOWDOWN SYSTEM CATEGORY A & B VALVE EXERCISE TEST	Once every 92 Days
OP-ST-DW-3001, R9	DEMINERALIZED WATER/DEAERATED WATER SYSTEM CATEGORY A VALVE EXERCISE TEST	Once every 92 Days
OP-ST-CA-3001, R9	COMPRESSED AIR CATEGORY A INSERVICE VALVE EXERCISE TEST	Once every 92 Days
OP-ST-SL-3002, R5	SAMPLING SYSTEM CATEGORY A AND B VALVE EXERCISE TEST	Once every 92 Days
OP-ST-NG-3001, R9	NITROGEN GAS SYSTEM CATEGORY A QUARTERLY VALVE EXERCISE TEST	Once every 92 Days
EM-ST-DG-0001, R7	EDG AND EMERGENCY 4.16 kV BUS PROTECTIVE RELAYS	Once every 18 months
OP-ST-RW-3011, R23	AC-10B RAW WATER PUMP QUARTERLY INSERVICE TEST	Once every 92 Days
OP-ST-RW-3021, R24	AC-10C RAW WATER PUMP QUARTERLY INSERVICE TEST	Once every 92 Days
OP-ST-RW-3031, R24	AC-10D RAW WATER PUMP QUARTERLY INSERVICE TEST	Once every 92 Days
OP-ST-CCW-3002, R17	AC-3A COMPONENT COOLING WATER PUMP INSERVICE TEST	Once every 92 Days
OP-ST-CCW-3012, R14	AC-3B COMPONENT COOLING WATER PUMP INSERVICE TEST	Once every 92 Days
OP-ST-CCW-3022, R13	AC-3C: COMPONENT COOLING WATER PUMP INSERVICE TEST	Once every 92 Days
OP-ST-AFW-0007, R2	AUXILIARY FEEDWATER PUMP FW-6 OPERABILITY TEST	Once every 30 days
OP-ST-MS-3002, R9	MAIN STEAM SYSTEM CATEGORY B VALVE EXERCISE TEST	Once every 18 months
OP-ST-FW-3002, R12	FEEDWATER SYSTEM CATEGORY A AND B VALVE EXERCISE TEST	Once every 18 months
OP-ST-SI-3001, R25	SAFETY INJECTION SYSTEM CATEGORY A AND B VALVE EXERCISE TEST	Once every 92 Days

Table B3.2a ESF Surveillance Test Procedures		
Procedure Number	Procedure Title	Frequency
OP-ST-SI-3002, R15	SAFETY INJECTION SYSTEM CATEGORY A, B AND C VALVE EXERCISE TEST	Once every 92 Days
OP-ST-CCW-3004, R16	COMPONENT COOLING CATEGORY A AND B VALVE EXERCISE TEST	Once every 18 months
OP-ST-WDL-3001, R12	WASTE DISPOSAL SYSTEM CATEGORY A AND B VALVE EXERCISE TEST	Once every 92 Days
OP-ST-VA-3001A, R3	VENTILATING AIR SYSTEM QUARTERLY CATEGORY A VALVE EXERCISE TEST	Once every 92 Days
OP-ST-SI-3022, R10	ROOM 22 SAFETY INJECTION/CONTAINMENT SPRAY PUMPS AND VALVE EXERCISE IN SERVICE TEST	Once every 92 Days
OP-ST-VA-0003, R5	CONTAINMENT VENTILATION SYSTEM CONTAINMENT AIR COOLING AND FILTERING UNITS FILTER CIRCUIT OPERATION	Once every 92 Days
IC-ST-SI-0003, R3	FUNCTIONAL TEST OF SIRWT LOW LEVEL SIGNAL (STLS) ACTUATION	Once every 18 months
OP-ST-SHIFT-0001, R79	OPERATING TECHNICAL SPECIFICATION REQUIRED SHIFT SURVEILLANCE	Once every day
Various – (Procedure reference listed were used in the database)	FCS ISI/IST EQUIPMENT TEST SURVEILLANCE'S AND PMS	Various - (Frequency listed were used in the database)

B3.3 EVALUATION, ANALYSES AND RESULTS

The component categorization process is described in detail in the body of the topical report, Section 4.0, therefore it shall not be repeated here. Table B3.3a provides a numerical summary of the classification results specifically for FCS.

Table B3.3a
Categorization Summary for Fort Calhoun Station



Figures B3.3-1 through B3.3-8 illustrate where there is overlap in the integrated ESF testing at FCS. They are simplified illustrations and therefore depict only a rough approximation of overlap. They are not intended to provide engineering and system design detail. They include the most significant tests. The quarterly pump and valve operability tests were not included because they are too numerous. The figures were constructed starting with the basic components of the logic path from the sensor to the end equipment. Then the tests covering various components in the logic path were added. Figure B3.3-1 through B3.3-6 address testing associated with SIAS, CIAS, CSAS, RAS, SGIS and VIAS actuations. Figure B3.3-7 covers EDG load sequencers. Figure B3.3-8 covers under voltage sensing (OPLS). The surveillance procedures referenced in these diagrams are also mapped to specific components in the project database under the headings of "Other Test 1, 2, 3" etc.

Figure B3.3-1
SIAS Surveillance Procedures - Fort Calhoun Station



Figure B.3.3-2
CIAS Surveillance Procedures - Fort Calhoun Station



Figure B3.3-3
CSAS Surveillance Procedures - Fort Calhoun Station



Figure B3.3-4
RAS Surveillance Procedures - Fort Calhoun Station



Figure B3.3-5
SGIS Surveillance Procedures - Fort Calhoun Station



Figure B3.3-6
VIAS Surveillance Procedures - Fort Calhoun Station



Figure B3.3-7
Sequence Surveillance Procedures - Fort Calhoun Station



Figure B3.3-8
OPLS Surveillance Procedures - Fort Calhoun Station



B4.0 PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE

As mentioned previously, Westinghouse performed a preliminary categorization and assessment of components tested by the integrated ESF test functions for FCS. FCS used the preliminary assessment as a foundation and starting point to perform the PSA analysis described in this section. The categorization began with the testing matrix described in Section B3.0. The matrix was used to identify components whose reliability appears to be demonstrated primarily/solely by the integrated ESF test.

The FCS PSA Master List of basic events was reviewed to determine if and how the model addresses each such component or function. The results of the review were documented in a database that relates the components to the associated basic events. The components were categorized, based on the type of changes to the event frequencies or modeling details that would be needed in order to quantify the change in risk associated with the proposed change in the integrated ESF test frequency. Actual changes to the model were performed by FCS. The remainder of Section B4.0 is derived from the risk analyses.

B4.1 MODEL ANALYSIS

This analysis evaluates the risk impact of extending this test from once per refueling cycle on a sequential basis to once every other fuel cycle on a staggered basis. This is done by adjusting the unavailability for the affected components to reflect the increase in the test interval and requantifying the FCS PSA. (For this analysis, it was assumed that the current test interval is 18 months and the revised test interval is a staggered 36-month scheme with one or the other train being tested every 18 months.)

The conclusions drawn in this appendix are applicable only to the FCS. Those conclusions are a strong function of the FCS PSA Model used to generate the base-case CDF and LERF values as well as the event probabilities for the nominal and extended STI cases. The FCS PSA Model includes the classic at-power Level 1 internal-event initiators as well as logic to create at-power fire-event and at-power seismic-event sequences. It also includes a gate that captures all of the Level 2 LERF sequences.

B4.1.1 Discussion of Major Assumptions

The major assumptions of this calculation are discussed below.

4.16kV Load Shedding

The loads on 4.16kV Buses 1A4 and 1A3 have several ways of being load shed. The general way that the breakers are tripped is that a relay will energize a main undervoltage relay, which in turn energizes the trip coil. (The main undervoltage relay can be characterized as being the relay that energizes the trip coil for the individual 4.16kV load breakers.) The trip coil then is energized and opens the breaker. One way the loads can be shed is by OPLS. If there were an OPLS, two different relays sense the low signal. This low signal is sensed on the secondary side of the transformer. The two relays are in parallel with each other, so if one relay were to fail and the other one were to work, it would still energize the main undervoltage relay that energizes the trip coil. There are two different lockout relays, either of which is sufficient to trigger load shed because they too are in parallel and separate from each other. The lockout relays depend on the position of the breaker connected to the 22/4.16 kV transformer and the breaker connected to the 161/4.16 kV transformer. There is also an undervoltage relay on each bus to produce

load shed. All five of these relays or contacts failing would still not cause a failure to load shed because there is also a backup loss of voltage trip.

The backup system has an undervoltage signal coming from the secondary side of the transformer. This signal is received by one of the same OPLS relays in the main loss of voltage trip circuit, but it has its own set of contacts. Once the relay picks up the signal and the contact closes, it will energize another undervoltage relay that energizes the main undervoltage relay for each trip coil. The backup loss of voltage trip also has the relays associated with AC circuit breakers coming off the 161/4.16kV transformer, the 22/4.16 kV transformer, and the breaker to the EDG. Each of these breakers has a relay that is in series with one another. When the 161/4.16kV breaker is opened, power is lost to the relay causing its contact to close. The other two AC circuit breakers should be open so there is no power holding relay contacts open anyway. This means that when the normally-closed 161/4.16kV circuit breaker opens, that completes the backup loss of voltage trip circuit and allows an undervoltage relay to be energized. The OPLS and the AC circuit breaker relays are in parallel with the undervoltage relay that energizes the main undervoltage relays. This means that there is a single failure possibility in the backup system with this relay. The circuit breaker from the 161/4.16kV transformer would have to fail to open in order to contribute to the overall failure to load shed. This means that a total of five different relays or contacts must fail to prevent load shedding.

There is only one main undervoltage relay for the loss of voltage trip and one main relay for the backup loss of voltage trip. The minimum number of relays that have to fail in order to cause load shed failure is five. The first two ways involve failure of the two OPLS relays. The next failure was an undervoltage relay. The third and fourth main failures are the lockout relays from the AC circuit breakers. The last failure that would have to occur is the undervoltage relay in between the main undervoltage relays and the OPLS and AC circuit breakers. All five of these ways to energize the main relays would have to fail for a failure to load shed to occur. The only single failure device for the 4.16kV loads is the trip coil and circuit breaker itself. The circuit breakers and their associated trip coils are already in the FCS PSA Model. There are so many redundant signals to initiate load shed it is more probable that the two main undervoltage relays (the main one and the backup) would fail to close the contacts that allow the trip coil to be energized.

480V Load Shedding

On the 480V buses there are two types of loads. There are single components and there are Motor Control Centers (MCC). There are nine different buses that feed these loads (three on the 1A3 side, three on the 1A4 side, and three island buses).

The single components are load shed by undervoltage relays that sense low voltage on a bus. Each single load on a bus connects to the same UV relay, so if the UV relay for a bus were to fail, then all of the loads on that bus will be picked up as dead load by the EDG. These undervoltage relays are the only way that the single 480V loads can be automatically load shed. There are four of these undervoltage relays in series so if one fails, the components on that bus will not be load shed. All of these relays are modeled because a single failure causes the associated bus loads to be picked up by the EDG. FCS identified this as a single failure. An evaluation was performed to ensure that each EDG could handle the 480V components, supplied by one bus, being picked up as dead load. Each EDG is able to handle a single bus failing to be load shed but it may not handle two buses failing to be load shed.

Each single failure for a 480V bus was identified because it only takes a failure of two undervoltage relays on different buses to potentially cause failure of the EDG. Some of the loads on the bus are not normally running and some of the loads on each bus require more horsepower than others, so it is still

possible for the EDG to handle two undervoltage relays on different buses failing. It takes particular combinations to cause failure of the EDG so modeling all the combinations would be overly conservative.

The 480V loads were modeled based on what bus the loads were on and what EDG they affected. The load on each 480V bus was added up based on the amount of horsepower that was required to run them (as opposed to starting them). The normally running components were the only ones considered because they are the ones that would be picked up as dead load if load shedding were to fail. When the horsepower required for each bus was obtained, it was compared with the bus on DG-1 that had the highest horsepower requirements (for DG-1, bus 1B3B that requires 650hp for all normally running components). Since the evaluation that was done on the EDG determined it could handle one bus failing, it is assumed that DG-1 can pick up at least 650hp of dead load in a single load block. Combinations were modeled based on whether or not the total horsepower (after failing to load shed two 480V buses) was greater or less than 650hp. If the normally running components for the two buses added up to 650hp or more, then it was modeled. The same philosophy applied for DG-2. More than two buses were not modeled because it would require three or more relays failing. A common-cause event in this part of the model would not appear in a CDF cutset or LERF cutset at the truncation values typically used by the FCS PSA. Having a double bus failure is effectively improbable in a PSA sense, even when considering common-cause, and therefore not modeled.

The MCCs on the nine buses could also fail to be load shed. Failure of a single MCC to be load shed, along with failure of an additional 480V load to load shed, could cause failure of a EDG. This again could be overly conservative because the MCCs do not require a lot of power (compared to the 480V single loads) for components that are normally running on the MCC.

The MCCs are load shed by a tripping relay. A single failure would cause the MCC not to be load shed. The motor contactors for many of the MCC loads "drop out" when power is removed. There are however some components on the MCC that do not drop out. The power requirements for most of these components are small when compared to the individual 480V loads on the buses. The EDG is able to handle at least one entire 480V bus as dead load. Again, depending on what is picked up as dead load, adding another MCC as dead load does not necessarily cause failure of the EDG.

The MCCs were modeled based on three different criteria. First, components on the MCCs that are supposed to be load shed were identified, and it was decided whether the components are normally running. Next the total running-horsepower that the components would require was calculated. Since in a single load-block, DG-1 can handle at least 650hp dead load and DG-2 can handle at least 600hp, components requiring 10 horsepower or less were ignored. Last, it was determined whether or not the component on the MCC "dropped out". Some of the components cannot be restarted following a loss of power without a manual operation. MCCs were modeled based on the total horsepower of all components that (1) are normally running, (2) are greater than 10hp and (3) do not "drop out". The same criteria were used as for the 480V components. If an MCC and a bus were to fail to be load shed, and if the combined horsepower would fail the EDG, then the relays for the MCC are in the FCS PSA Model. Some MCCs require failure of two different OPLS relays and were not considered because it would then require triple failure or a low-probability common-cause event to overload the EDG.

There are no single failures that are capable of failing the EDG from too much dead load.

480-Volt Assumptions

Based on FCS documentation the EDGs can handle at least two buses, two MCCs, or an MCC and a bus as dead load initially.

Buses 1B3A-4A, 1B3B AND 1B3C are buses (if not load shed) that alone could cause failure of the EDG. MCC-3A4, MCC-3C3 and MCC-3B2 are MCCs that (if not load shed) alone could cause failure to the EDG.

It is not likely that the MCC-3B2 will cause failure of the EDG alone (upon a failure to load shed) because of how many components drop out (the running loads have under-voltage protection; if the undervoltage protection were broken, that would be one failure) and because two OPLS relays must fail (two more relays). The nominal failure probabilities for relays are relatively small. Any cutset that would include ANDing three relay failures (or a small common-cause event) would be below typical quantification truncation limits.

Because DG-1 has failed with 150hp of non-sequenced loads (over and above the total amount normally sequenced on to DG-1) from bus 1B3A-4A, a key assumption is that any single non-shed load of more than 150hp causes a failure of DG-1.

Because DG-2 has handled the non-sequenced loads (over and above the total amount normally sequenced on to DG-2) of 1B4B without a failure, any single non-shed load of more than 300hp is conservatively assumed to be enough to cause a failure of DG-2.

Other Assumptions

Control room ventilation is required only for situations when the core has already melted and control room habitability is under threat. This is based on no PSA-related functions needing "inside the control room actions" that are assumed to occur post-core melt.

Failure of relays that disconnect all engine and generator protective devices except overspeed trip would have to combine with an actual non-emergency DG trip signal in order to appear as part of a valid cutset. This type of assumption prevents the quantifier and the analyst from having to spend time creating and evaluating, respectively, unimportant cutsets, i.e. those cutsets that have frequencies several orders of magnitude below the sequence frequency. Combining the conditional probability of relay failures (in the range of $3E-6$ to $2E-3$) and a condition causing a non-emergency DG trip (typically between $1E-2$ to $1E-1$ for a 24-hour run, but these conditions are usually not modeled because realistic sequences involve emergency-mode operation of the DG) with a typical loss-of-offsite power initiator (in the range of $3E-4$ to $3E-3$) would yield a core damage sequence cutset line item potentially several orders of magnitude below typical important OPPD core damage sequence values (i.e. $1E-7$ to $1E-6$).

Schemes where success depends on automatically (fail-safe) open valves, or normally open (or partially open) valves are treated as non-risk significant. Combining the low probability of failure of these types of valves with a typical initiator would yield a cutset line item with a frequency below typical quantification truncation value used in the FCS PSA.

The spent fuel storage pool cannot contribute meaningful heat load on the CCW heat exchangers even if HCV-748 fails to close on CIAS. A CIAS signal would also cause the spent fuel pool recirculating pump to be load shed. Two issues are relevant. One, the spent fuel pool would have no active way of moving its water through a heat exchanger cooled by CCW. Two, during design basis accidents, the CCW

temperature would exceed spent fuel pool cooling temperatures and thus the spent fuel pool would act as a CCW heat sink. Therefore, the failure to successfully close HCV-748 does not contribute to the risk measured in this analysis.

For the analysis, it is assumed that the current ESCS relay surveillance test interval is 18 months for all of the relays and the revised test interval is 36 months with one train being tested every 18 months. This assumption maximizes the estimated Δ CDF and Δ LERF.

B4.1.2 Acceptance Criteria

The goal of risk assessment modeling is to produce realistic results that are self-consistent. Fault tree quantification must yield realistic combinations of equipment failures that actually would cause the event described by the top gate. In this case, there are two top gates, one for CDF and the other for LERF.

The goal of this evaluation is to determine the change in CDF and the change in LERF as a result of putting FCS ESCS relay testing on a staggered test schedule. Regulatory Guide 1.174 suggests that a change is not significant when the increase in CDF and increase in LERF is less than $1E-6$ and $1E-7$, respectively.

B4.1.3 Computer Codes Used in Analysis

This evaluation uses the suite of CAFTA products to develop and quantify the FCS PSA model. The principal packages are listed below.

B4.2 SCOPE OF FCS PSA

The FCS PSA is an at-power, internal and external events PSA. Both Level 1 and Level 2 are addressed. The external events considered are fire, seismic, as well as internal floods. The model is routinely updated as a result of plant changes, increasing fidelity for particular applications and new quantification techniques.

B.4.2.1 At-Power Model Structure

Typical large-linked fault tree techniques underlie the analysis. For illustration purposes, FCS has small even trees that capture the sequences quantified with the model. These illustrations became the basis for the top logic employed in the large fault tree model created for FCS.

The model has detailed trees for each of the front-line systems identified in the top logic illustrated on the event trees. Likewise, the front-line systems spawn the need for support system trees. To ensure traceability, FCS keeps a set of documents that catalogue data values and assumptions for the front-line and support system trees.

The model is quantified with a mix of generic and FCS plant-specific data. The scope of the plant-specific data analysis included initiating event frequencies and equipment for which plant-specific data allows for statistically meaningful estimates of failure rates and failure probabilities. The plant-specific data arises, in part, from a review of Licensee Event Reports, monthly plant reports and in internal Incident Reports. These capture important plant failure modes, events and trends.

The model includes a gate that captures LERF cutsets. That part of the top logic arose from plant walkdowns, a containment ultimate pressure/strength analysis, and a literature study on severer accident phenomenology. FCS used Modular Accident Analysis Program (MAAP) computer analyses to simulate severe accidents at the plant.

The containment ultimate pressure/strength analysis used finite element analysis of critical parts of the containment structure to estimate the pressure at which the limiting component fails.

The model includes a seismic initiator. That initiator is associated with the modeled components that are important and also non-seismic Category I. In general, the seismic initiator becomes another balance of plant transient initiator.

The model includes flood initiators for various rooms throughout the plant. Flood-induced failures included components that would be unavailable due to loss of inventory or isolation of the flood source as well as components susceptible to the effects of steam (if applicable) or immersion and spray. It was initially assumed that all components in the room where the source is located would be subjected to the effects of spray unless there were easily justifiable spatial or other arguments. Component failures for rooms in the propagation paths were determined based on the bounding flood levels in each room of the propagation path. Splashing, such as water tumbling down a stairwell or falling from an open hatchway, was assumed to affect components within a distance of 30 feet with the exception of motor control centers, which are assumed to provide adequate protection of internal components.

The model includes quantified human failure events. The methods created conservative screening values for human failure events with additional study made of those events that are important to typical plant risk metrics.

The FCS PSA explicitly models the functions associated with ESCS. Key modeling features are discussed below.

B4.2.1.1 Modeling and Quantification

Common Cause

The beta factor method and the Multiple Greek Letter method, as appropriate, are used to model common-cause failures in the FCS PSA. Common cause basic events have been directly incorporated into the fault tree models, and represent the failure of all components within a defined group by a specified failure mode, e.g. all safety injection pumps fail to start on demand due to common causes. This approach is used throughout the FCS PSA. Other key common cause impacts related to the EDGs are 125VDC batteries, SW pumps, ESCS UV channels and 4kV load breakers.

Quantification

The large linked-fault-tree model for FCS is configured, edited, and analyzed with the CAFTA suite of codes from EPRI. The quantification was done with the powerful FORTE engine.

B4.2.1.2 Truncation Limits

The truncation for both CDF and LERF was set at $1.0E-10$. That is three to four orders of magnitude below the most significant sequences identified in the analysis.

B4.3 QUALITY OF FCS PSA

FCS utility personnel have constructed the FCS PSA with a strong commitment toward developing a complete and accurate PSA. This commitment can be seen through the following elements:

- Formal qualification program for the PSA staff
- Use of procedures to control PSA processes
- Independent reviews (checks) of PSA documents
- Comprehensive PSA Configuration Control Program
 - Quarterly plant change monitoring program
 - Process to control PSA quantification software
 - Active open items list
 - Interface with the site corrective action program
 - Process to maintain configuration of previous risk-informed decisions
- Peer reviews
- Participation in the CEOG cross comparison process
- Incorporation, where applicable, of CEOG PSA Technical Positions
- Commitment of continuous quality improvement

Considering the scope (internal and external events), level of detail and processes, the FCS PSA is sufficient to support a technically defensible and realistic evaluation of the risk associated with this amendment request.

B4.4 PSA SOFTWARE

A variety of MS Windows executables and DLLs from the CAFTA suite are used for this analysis. All software executed in a configuration documented according to the plant's QA procedures.

B4.4.1 CAFTA

CAFTA is a commercial product. It comprises a fault tree editor and event data base editor built to easily edit and create input files for any number of cutset quantification engines. CAFTA also includes a cutset editor, which is used to analyze the results of a quantification.

B4.4.2 PRAQuant

PRAQuant is an executive program for the CAFTA suite. In this analysis it was used to direct a serial quantification of CDF and LERF for the base case and the hypothetical case.

B4.4.3 FORTE

FORTE is the powerful quantification engine that allows rapid quantification of cutsets from large linked fault trees down to user selected truncation limits.

B4.5 RESULTS AND CONCLUSIONS

Table B4.5a
FCS Results

A large pair of empty parentheses, (\quad) , is centered on the page. This indicates that the content of Table B4.5a, which would normally be placed between these parentheses, is missing from this document.

Risk is measured by two figures-of-merit, which are proxies for the actual risk posed to the public health and safety as a result of the proposed change in testing strategy. The base situation is having the integrated ESF test once per fuel cycle on a sequential basis. The proposed situation is having the integrated ESF test once every other fuel cycle on a staggered basis.

Regulatory Guide 1.174 suggests that a change is not significant when the change in CDF and change in LERF is less than $1E-6$ /year and $1E-7$ /year, respectively. Thus, the proposed STI situation modeled is not risk significant. Based on the changes in CDF and LERF shown for the proposed STI (Table B4.5a), the risk impact of extending the integrated ESF test from once per fueling cycle on a sequential basis, to once every other fueling cycle on a staggered basis is not significant.

APPENDIX C

APPLICATION OF WCAP-15830-NP TO PALISADES

TABLE OF CONTENTS

C1.0	ABSTRACT	C-3
C2.0	BACKGROUND	C-4
C2.1	ESFAS Description	C-4
C2.1.1	Safety Injection Initiating Signals	C-4
C2.1.2	Containment Isolation Initiation	C-6
C2.2	Palisades Configuration	C-6
C2.2.1	Diesel Generators	C-7
C2.2.2	Automatic transfer system	C-7
C2.2.2	Automatic Load Shedding and Sequencing	C-8
C2.3	Current Technical Specifications	C-9
C2.4	Proposed Changes to Technical Specifications	C-10
C3.0	TEST MATRIX AND COMPONENT CATEGORIZATION	C-12
C3.1	Method Discussion	C-12
C3.1.1	Integrated ESF Test (RT-8C and RT-8D)	C-12
C3.2	Input	C-14
C3.3	Evaluation, Analyses and Results	C-16
C4.0	PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE	C-20
C4.1	Model Analysis	C-21
C4.2	Scope of PSA	C-25
C4.2.1	At-Power Model Structure	C-25
C4.2.2	Shutdown Risk Assessment	C-25
C4.2.3	PSA Detail Needed for Change	C-25
C4.3	Quality of Palisades PSA	C-26
C4.4	Results and Conclusions	C-27

LIST OF TABLES

C2.2.1a	Emergency Diesel Generators	C-7
C2.3a	Existing Surveillance Test Intervals	C-9
C2.4a	Proposed Surveillance Test Intervals	C-10
C3.1.a	Applicable Database Fields	C-12
C3.2a	ESF Surveillance Test Procedure	C-15
C3.3a	Categorization Summary	C-16

LIST OF FIGURES

C3-1	SIAS Surveillance Procedures - Palisades	C-17
C3-2	Under Voltage/Load Shed Surveillance Procedures – Palisades	C-18
C3-3	EDG Load Sequence Surveillance Procedures – Palisades	C-19

C1.0 ABSTRACT

Combustion Engineering Owners Group (CEOG) Task 2016, "Staggered Integrated ESF Testing" used a risk-Informed approach to demonstrate that any change in risk would be negligible if a staggered test frequency were adopted for integrated Engineered Safety Features (ESF) testing. Currently, integrated ESF testing is performed on both trains each refueling cycle. Using a staggered approach, only one train would be tested each refueling outage. The basic premise of the proposed change is the belief that the integrated ESF test is not the primary/sole operability test for the majority of the components tested. Other surveillance procedures are performed on many of these components and functions on the same or more frequent basis. Therefore, there may be considerable overlap between the integrated ESF test and other testing. For the components/functions that are tested only by the integrated ESF test, the risk model was adjusted, the risk associated with the change recalculated, and the overall risk requantified. In some cases, it was possible to develop a reasonable deterministic basis for assuming the component failure mode addressed by the integrated ESF test was not risk-significant. These components were exempt from further Probabilistic Safety Analysis (PSA) review and analysis. The overall task was broken down into more manageable units of work. The first was the procedure review and matrix development. The second was the categorization of components and functions tested by the integrated ESF test. Third was the preliminary PSA assessment and Category "A" component sub-categorization. Last was the finalization of the PSA assessment, adjusting the PSA models and calculating the change in risk associated with the change in Surveillance Test Interval (STI).

This Appendix addresses application of staggered integrated ESF testing at Palisades. It describes in detail the plant specific procedure review, component categorization and risk analyses as performed for Palisades to support the change to staggered integrated ESF testing. The Palisades Technical Specification Surveillance Requirements addressed by the Integrated ESF Test are listed in Table C2.3a.

The risk contribution associated with the increased frequency, 18 months on a staggered bases, has been quantitatively evaluated using the current plant-specific PSA for Palisades. The safety significance is based on the increase in Core Damage Frequency (CDF) for the assumed change in the test interval for specified components. Based on changes to the model necessary to evaluate the test interval extension and adjustments made as a result of the review of the results, the change in CDF is considered to be of low safety significance.

C2.0 BACKGROUND

The engineered safeguards controls consist of equipment to monitor and select the available power sources and to initiate operation of certain load groups, and will initiate containment isolation when required. The system is designed on a two-independent-channel basis with each channel capable of initiating the safeguards equipment load groups to meet the minimum requirements to safely shut down the reactor and provide all functions necessary to operate the system associated with the Plant's capability to cope with abnormal events. The system is provided with the necessary redundant circuitry and physical isolation so that a single failure within the system will not prevent the proper system action when required. A non-CE designed engineered safeguards control system is in place at the Palisades plant.

C2.1 ESFAS DESCRIPTION

The Engineered Safeguards control and instrumentation system was designed to actuate Safeguards and essential support systems automatically. Means for manual operation are also provided. The system includes control devices and circuits for automatic initiation, control, supervision and manual test of the Engineered Safeguards systems. The controls are interlocked to automatically provide the sequence of operations required to initiate engineered safeguards system operation with or without offsite power.

Certain critical parameters have four sensors utilizing a two-out-of-four logic to provide reliable operation with a minimum of spurious actuations. Initiation level settings and their bases are provided in the Technical Specifications. The four sensors are physically isolated and operation of any two-out-of-four will initiate the appropriate engineered safeguards action. This action is provided by combining the four sensors into relay matrices that provide dual-channel initiation signals. Actuation Channel A has all odd numbered relays. Channel B has all even numbered relays. Channel A receives its power from preferred AC Panel Y1 0; Channel B from Panel Y20. Instruments Channel C has odd numbered devices and Instruments Channel D has even numbered devices. Channel C receives its power from preferred AC power Panel Y30; Channel D from Panel Y40.

Testing of major portions of the engineered safeguards control circuits is accomplished while the Plant is at power. More extensive circuit sequence and load testing may be done with the reactor shut down. The test circuits are designed to test the redundant circuits separately so that the correct operation of each circuit may be verified by either equipment operation or by sequence lights. The test circuit design is such that, should an accident occur while testing is in progress, the test will not interfere with initiation of the safeguards equipment required.

C2.1.1 Safety Injection Initiating Signals

The control system is designed to automatically initiate the necessary engineered safeguards equipment upon a Safety Injection Signal (SIS) with or without offsite power available. To assure reliability, the control system is designed on a two-channel concept with each channel initiating the operation of separate and redundant engineered safeguards load groups.

The SIS is derived from pressurizer low-low pressure or containment high pressure. The pressurizer low-low pressure signal is derived from four pressure sensors installed on the pressurizer. Each sensor supplies a pressurizer pressure signal to a pressure indicator/alarm instrument. Each pressure instrument is connected to a latching-type auxiliary relay. The containment pressure signal is derived from four containment pressure sensors. Each containment pressure sensor is connected to a latching-type auxiliary

relay. One pressure sensor and associated pressure instrument, as well as one containment pressure sensor, are supplied from each of the four preferred ac sources.

Either two out of four pressurizer low-low pressure or two out of four containment high-pressure signals initiate the SIS signal which, in turn, actuates two safety injection control circuits, each of which is supplied by a separate preferred ac source.

Within each control circuit, relays are provided to initiate redundant devices so that individual relay failure will not cause a complete circuit failure. Actuation of each safety injection control circuit can be performed manually via a safety injection initiate push button, one push button for each safety injection circuit. The SIS relay logic circuits control the loading sequence in duplicate control circuits. Failure of the control power on any one redundant circuit will be annunciated in the control room.

Containment spray activation requires the containment high-pressure signal to ensure the containment is sprayed only when needed.

If a SIS is accompanied by a loss of offsite power, the load sequencers will be initiated. There are two of these sequencers with each connected to a separate control circuit. The sequencers load the required equipment in sequence on the Emergency Diesel Generators (EDGs) so as to not exceed the EDG capacity.

Operation: These circuits are safeguards circuits and operate only during shutdown or accident conditions. They have no function while the Plant is under normal operation. The shutdown sequence will vary depending on the presence or absence of an SIS signal and offsite power availability.

Shutdown Upon a Reactor Trip With Offsite Power Available: If no SIS condition exists at the time of the reactor trip, all auxiliary equipment will continue to operate from the offsite power source. Plant shutdown will be performed as necessary by the operator.

Shutdown Upon a Reactor Trip Without Offsite Power: Upon loss of offsite power during normal operation, each EDG will be started through its own separate control circuit. The emergency generator start is dependent upon undervoltage on the engineered safeguard buses. The bus loads will be shed by the pre-diesel load shedding relays. When the pre-diesel load shed relays have operated and the emergency generator voltage reaches a preset value, the buses will then be energized from the emergency generators. The sequencers will be energized to automatically start required normal shutdown equipment.

Safety Injection With Offsite Power Available: If offsite power is available at the time of initiation of the SIS, the SIS relays will initiate the simultaneous start of the engineered safeguards equipment.

Safety Injection Without Offsite Power: If offsite power fails, all loads will be shed at the time the EDGs receive an automatic start signal. With load shedding completed, the EDG breakers will close automatically when generator voltage approaches a normal operating value. Closing of the breakers will reset the load shedding signals and start the sequencers. The sequencers will initiate operation of the engineered safeguards equipment required for design basis accident response.

C2.1.2 Containment Isolation Initiation

The containment isolation control system is designed to isolate the containment upon occurrence of either containment high pressure or containment high radiation. The Containment Spray System is initiated upon containment high-pressure signal. The system is also designed to prevent inadvertent opening of the containment isolation valves. The control system is designed on a two-channel concept with redundancy and physical separation. Each channel is capable of initiating containment isolation and operation of certain engineered safeguards.

The controls consist of two independent and isolated groups of circuits. The four radiation sensors and four pressure sensors are each connected to an auxiliary relay. Four separate control circuits each consisting of one pressure and one radiation level sensor and their two auxiliary relays are connected to separate preferred AC buses. There are two separate initiation circuits which consist of two-out-of-four logic matrices and necessary auxiliary relays.

The containment isolation valves operate from the 125 volt DC source and are normally energized. It requires two high-radiation or two high-pressure signals to close the isolation valves. This prevents spurious signals from causing containment isolation.

Coincident two-out-of-four high-radiation or two-out-of-four high-containment pressure signals from the auxiliary relays will trigger an alarm in the main control room, close all containment isolation valves not required for engineered safeguards except the component cooling line valves which are closed only by containment high pressure, and will isolate the control room ventilation system. High radiation detected by the refueling accident high-radiation monitors will also close all containment isolation valves not required for engineered safeguards when locked in by the respective refueling monitor key switches.

Coincident two-out-of-four high-radiation or two-out-of-four high-containment pressure signals from the auxiliary relays locks in the high-pressure and high-radiation circuits, respectively.

Containment high-pressure signal will initiate SIS, and start containment spray. Containment high-pressure signal will also initiate a reactor trip with a two-out-of-four logic. This trip is in addition to the thermal margin/low-pressure trip to ensure that the reactor is tripped before SIS and containment spray is initiated.

Containment High Pressure (CHP) signal will initiate closure of the main steam isolation valves to reduce the inventory blowdown from the intact steam generator in the case of a main steam line break, reducing the peak containment pressure and temperature as required in the accident analysis. CHP also closes the main and bypass feedwater regulating valves.

C2.2 PALISADES CONFIGURATION

The ESF functions start/align equipment required to mitigate design basis accidents. A critical aspect of the Engineered Safeguards Control System (ESCS) design addresses the loss of the normal (off-site) power supply.

C2.2.1 Diesel Generators

At Palisades, the two 2,400V ESF buses are each supplied by a dedicated EDG. The table below shows the EDG to bus alignment and naming convention:

**Table C2.2.1a
Emergency Diesel Generators**

Emergency Diesel Generator	Manufacturer	2400V Bus	Channel Supported
DG-1-1	Fairbanks-Morse	1C	A
DG-1-2	Fairbanks-Morse	1D	B

The EDGs are designed to provide a dependable onsite power source capable of starting and supplying the essential loads to safely shut down the plant and maintain it in a safe shutdown condition under all conditions. The reliability of this onsite power is provided by its duplication wherein each EDG redundant loads and each is capable of providing power to the minimum necessary safeguards equipment.

The two EDGs are of equal size. The EDGs have static-type excitation and are provided with field flashing for quick voltage buildup. Each EDG is connected via a generator breaker to a separate 2,400 volt bus. Synchronizing equipment is provided to permit connecting the generator to the 2,400 volt bus for parallel operation with the onsite or offsite power sources during testing of the EDGs. The synchronizing equipment is automatically bypassed by breaker position interlocks to permit manual and automatic closing of the EDG breaker on a dead bus. The four 2,400 volt bus safeguard/station power and start-up transformer incoming breakers are interlocked to prevent automatic closing when the associated EDG breaker is closed. The incoming breakers can be closed manually only by using synchronizing equipment when the associated EDG breaker is closed.

Support systems associated with each EDG include a fuel oil system, air starting system, lube oil system, jacket water system, crankcase exhaust, two starting circuits and a load sequencer. Supply of electric power for this system is obtained from the EDG they are supporting. Each system is located in a separate room from its redundant counterpart, except for the load sequencers which are located separate from one another in the main control room.

C2.2.2 Automatic transfer system

The automatic transfer control system is designed to monitor and select available offsite power sources and permit transfer of the 4,160 volt and 2,400 volt loads to the available offsite source upon loss of the normal power source. Redundant control circuits are provided for transfer of source power for the redundant 2,400 volt emergency buses (1C and 1D).

The controls for the safety-related 2,400 volt Buses 1C and 1D consist of redundant transfer, voltage protection and load shedding circuits connected to separate plant batteries. Circuit breaker controls for Bus 1C are fed from one battery and controls for Bus 1D from the other battery. Separate voltage sensing units on each bus are utilized for each of the circuits.

During emergency conditions, a turbine or generator trip will trip circuit breakers for the non-vital 4,160 volt Station Power Transformers 1-1 and 1-3, initiating transfer to the 4,160 volt Start-Up Transformers

1-1 and 1-3. The transfer to the start-up source will be completed within ten cycles after initiation with a bus dead time of approximately one-and-one-half cycles. The fast transfer will permit auxiliaries to continue to operate normally. During normal shutdown conditions, the 4,160 volt auxiliary power system is manually transferred to the start-up source.

The 2,400 volt system, which includes the emergency buses, is normally powered directly from offsite power via Safeguards Transformer 1-1. In this configuration, a turbine or generator trip will not result in a fast transfer of the 2,400 volt buses to the alternate source. Capability is provided in the design to allow powering the 2,400 volt buses from Station Power Transformer 1-2. When operating in this configuration, a turbine or generator trip will initiate a fast transfer to Start-Up Power Transformer 1-2. The transfer to the standby source will be completed within 10 cycles after initiation with a bus dead time of approximately one-and-one-half cycles. The fast transfer will permit auxiliaries to continue to operate normally.

The 2,400 volt auxiliary power system normally remains on the Safeguard Transformer source but can be manually transferred to the start-up source or, after transferring to the start-up source, can be manually transferred to the station power source.

In order to permit the main transformer backfeed mode of operation, the fast transfer on turbine trip is blocked by opening the generator isophase bus disconnect switch. No automatic transfer is provided for a transfer from the start-up transformers to the station or safeguard transformers. This operation must be done manually.

C2.2.2 Automatic Load Shedding and Sequencing

The reliability of the automatic transfer control system is assured by two independent and separate circuits controlling their respective auxiliary system breakers. The circuit is designed so that a loss of control power will not cause a false transfer; loss of control power will be annunciated. This circuit is also designed to prevent both offsite power and emergency power from being paralleled automatically. During 2,400 volt system automatic transfer, if the standby (alternate) power source is not available, the standby power source incoming breaker is prevented from closing and the emergency generator is used to energize the engineered safeguards bus. When offsite power returns, the start-up or safeguard/station power transformer incoming breakers may be closed manually through the synchronizing circuit.

The voltage protection and load shedding systems meet the criteria as described below:

The voltage trip set point has been set low enough such that spurious trips of the offsite source due to operation of the undervoltage relays are not expected for any combination of unit loads and normal grid voltages.

This set point at the 2,400 volt bus and reflected down to the 480 volt buses has been -verified through an analysis to be greater than the minimum allowable motor voltage (90% of nominal voltage). Motors are the most limiting equipment in the system. MCC contactor pickup and drop-out voltage is also adequate at the set-point values. The analysis ensured that the distribution system is capable of starting and operating safety-related equipment within the equipment voltage rating at the allowed source voltages. The power distribution system model used in the analysis has been verified by actual testing.

The time delays involved will not cause any thermal damage as the set points are within voltage ranges recommended by ANSI C8.4.1-1 971 for sustained operation. They are long enough to preclude trip of

the offsite source caused by the starting of large motors and yet do not exceed the time limits of safeguards actuation assumed in accident analyses.

Once the EDG is connected to its bus, load shed is blocked and is reinstated upon a trip of the EDG.

Load shedding of 2,400 volt Bus 1E and other nonessential loads provide a more than adequate margin on Start-Up Transformer 1-2 and Safeguard Transformer 1-1 to ensure reliable power is available for engineered safeguards loads.

Load shedding on offsite power trip and load sequencing once the EDG is supplying the safety buses are tested periodically. The load shed bypass circuit and a simulated loss of the EDG with subsequent load shedding are also tested. Calibration of the undervoltage relays verify that the time delay is sufficient to avoid spurious trips.

If an SIS is accompanied by a loss of offsite power, the load sequencers will be initiated. There are two of these sequencers with each connected to a separate control circuit. The sequencers load the required equipment in sequence on the EDGs so as to not exceed the EDG capacity.

C2.3 CURRENT TECHNICAL SPECIFICATIONS

Table C2.3a lists all the Technical Specification Surveillance Requirements that apply to Integrated ESF Testing at Palisades.

Table C2.3a Existing Surveillance Test Intervals		
SR	SR Description	Frequency
S.R.3.3.4.3	Verify a CHANNEL FUNCTIONAL TEST on each ESF Logic and Manual Initiation. (Functions: SIS, SGLP, RAS, AFAS, CHP and CHR per Table 3.3.4-1)	18 months
S.R.3.3.5.1	Verify a CHANNEL FUNCTIONAL TEST on each DG-UV start logic channel	18 months
S.R.3.5.2.5	Verify each ECCS automatic valve that is not locked, sealed, or otherwise secured in position, in the flow path actuates to the correct position on an actual or simulated actuation signal.	18 months
S.R.3.5.2.6	Verify each ECCS pump starts automatically on an actual or simulated actuation signal.	18 months
S.R.3.6.6.8	Verify each containment cooling train starts automatically on an actual or simulated actuation signal.	18 months
S.R.3.7.7.2	Verify each CCW automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	18 months
S.R.3.7.7.3	Verify each CCW pump starts automatically on an actual or simulated actuation signal.	18 months
S.R.3.7.8.2	Verify each SWS automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	18 months
S.R.3.7.8.3	Verify each SWS pump starts automatically on an actual or simulated actuation signal.	18 months
S.R.3.8.1.7	Verify on an actual or simulated loss of offsite power signal, a. De-energization of emergency buses	18 months

Table C2.3a Existing Surveillance Test Intervals		
SR	SR Description	Frequency
	<ul style="list-style-type: none"> b. Load shedding from emergency buses c. DG auto starts from Standby condition and: <ul style="list-style-type: none"> 2. energizes auto- connected emergency loads through automatic load sequencer 5. supplies permanently connected and auto connected loads for > 5 minutes. 	
S.R.3.8.1.9	Verify each EDG: <ul style="list-style-type: none"> a. Synchronizes with offsite power source while loaded with emergency loads upon a simulated restoration of offsite power; b. Transfer loads to offsite power source; and c. Returns to ready-to-load operation. 	18 months
S.R.3.8.1.10	Verify the time of each sequenced load is within + 0.3 second of design timing for each automatic load sequencer.	18 months
S.R.3.8.1.11	Verify on an actual or simulated loss of offsite power in conjunction with an actual or simulated safety injection signal; <ul style="list-style-type: none"> a. De-energization of emergency buses b. Load shedding from emergency buses c. DG auto starts from Standby condition and: <ul style="list-style-type: none"> 1. energizes permanently connected loads in < 10 seconds, 2. energizes auto- connected emergency loads through automatic load sequencer, 3. achieves steady state voltage > 2280 V and < 2520 V, 4. achieves steady state frequency > 59.5 Hz and < 61.2 Hz, and 5. supplies permanently connected and auto connected loads for > 5 minutes. 	18 months

C2.4 PROPOSED CHANGES TO TECHNICAL SPECIFICATIONS

Table C2.4a shows the proposed TS changes that apply to Palisades. The proposed frequency is based on the Palisades TS definition for staggered testing.

Table C2.4a Proposed Surveillance Test Intervals		
SR	SR Description	Frequency
S.R.3.3.4.3	Verify a CHANNEL FUNCTIONAL TEST on each ESF Logic and Manual Initiation. (Functions: SIS, SGLP, RAS, AFAS, CHP and CHR per Table 3.3.4-1)	18 months on a STAGGERED TEST BASIS
S.R.3.3.5.1	Verify a CHANNEL FUNCTIONAL TEST on each DG-UV start logic channel	18 months on a STAGGERED TEST BASIS
S.R.3.5.2.5	Verify each ECCS automatic valve that is not locked, sealed, or otherwise secured in position, in the flow path actuates to the correct position on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS
S.R.3.5.2.6	Verify each ECCS pump starts automatically on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS
S.R.3.6.6.8	Verify each containment cooling train starts automatically on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS

Table C2.4a Proposed Surveillance Test Intervals		
SR	SR Description	Frequency
S.R.3.7.7.2	Verify each CCW automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS
S.R.3.7.7.3	Verify each CCW pump starts automatically on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS
S.R.3.7.8.2	Verify each SWS automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS
S.R.3.7.8.3	Verify each SWS pump starts automatically on an actual or simulated actuation signal.	18 months on a STAGGERED TEST BASIS
S.R.3.8.1.7	Verify on an actual or simulated loss of offsite power signal, d. De-energization of emergency buses e. Load shedding from emergency buses f. DG auto starts from Standby condition and: 2. energizes auto- connected emergency loads through automatic load sequencer 5. supplies permanently connected and auto connected loads for > 5 minutes.	18 months on a STAGGERED TEST BASIS
S.R.3.8.1.9	Verify each EDG: d. Synchronizes with offsite power source while loaded with emergency loads upon a simulated restoration of offsite power; e. Transfer loads to offsite power source; and f. Returns to ready-to-load operation.	18 months on a STAGGERED TEST BASIS
S.R.3.8.1.10	Verify the time of each sequenced load is within + 0.3 second of design timing for each automatic load sequencer.	18 months on a STAGGERED TEST BASIS
S.R.3.8.1.11	Verify on an actual or simulated loss of offsite power in conjunction with an actual or simulated safety injection signal; d. De-energization of emergency buses e. Load shedding from emergency buses f. DG auto starts from Standby condition and: 6. energizes permanently connected loads in < 10 seconds, 7. energizes auto- connected emergency loads through automatic load sequencer, 8. achieves steady state voltage > 2280 V and < 2520 V, 9. achieves steady state frequency > 59.5 Hz and < 61.2 Hz, and 10. supplies permanently connected and auto connected loads for > 5 minutes.	18 months on a STAGGERED TEST BASIS

C3.0 TEST MATRIX AND COMPONENT CATEGORIZATION

C3.1 METHOD DISCUSSION

C3.1.1 Integrated ESF Test (RT-8C and RT-8D)

Integrated ESF testing is performed on both Right and Left channel every 18 months. The undervoltage condition on the class IE bus is initiated by pulling the Undervoltage Potential Transformer fuses. The SIS actuation is initiated by removing a current source jack to complete the two-out-of-four logic for PCS pressure <1605 psia.

Objectives (functions) covered by the integrated ESF test include:

- SIS actuation with Loss of Offsite Power
- SIS actuation without Loss of Offsite Power
- EDG Load Sequencer Response Time verification
- EDG Load Sequence verification
- Load Shed verification
- EDG Start on Auto-Start Verification
- Return to Normal Offsite Power Test Verification

An ESF Testing Matrix was prepared by Westinghouse for Palisades as part of CEOG Task 2016, Staggered Integrated ESF Testing. A database was used to create the matrix and to document the results of the ESF procedure review. The primary function of the database is to map the components tested by Palisades Engineered Safeguards System left and Right Channel tests (RT-8C and RT-8D) to other surveillances that test the same components and functions. The database contains references to the integrated ESF test and other tests, as well as a preliminary component categorization. The preliminary screening and categorization performed by Westinghouse provided the foundation for the plant specific PSA risk analysis performed by Palisades.

The procedure review portion of the database used to develop the matrix is defined by the following table. Component categorization and PSA assessments are addressed in Section C4.0 of this appendix.

Table C3.1a	
Applicable Database Fields	
Column Heading	Explanation
Document Number	Integrated Safeguards Test Procedure, RT-8C or RT-8D
Component ID	Component ID used in RT-8C and RT-8D
Related Component Information	Typically this field contains the breaker ID or actuation relay associated with the end component.
Component Description	Component description used in RT-8C and RT-8D
Functions tested by the Integrated ESF test.	The large blue section of the database shows the location in RT-8C and RT-8D where a particular component was identified in the test for a particular ESF function. For each component, the database shows the position verified. A blank field indicates that the component / function is not tested by the integrated ESF test.
Summary of functions tested by Integrated ESF test	Summarizes the functions tested by the integrated ESF test RT-8C and RT-8D for each component.
Palisades Comment	Feedback provided by Palisades relating to system/component design,

Table C3.1a Applicable Database Fields	
Column Heading	Explanation
	function or component assessment or category.
Cat	Component category, "A", "B" or "C". Categories are defined and explained below. The initial PSA assessment further divides Category "A" components into A-1, A-2, A-3 or A-4 to facilitate requantification of risk by Palisades. The screening process used to sort components into subcategories is described in section 4.0 of the topical report and is related specifically to Palisades.
Assessment	An initial assessment that supports why the component is initially categorized "A", "B" or "C".
Other Test 1 through 5	Lists references to other Palisades surveillance procedures that overlap the integrated ESF test (RT-8C and RT-8D).

The matrix was developed as follows: First, Integrated Engineered Safeguards Tests, RT-8C and RT-8D were reviewed to identify the components and functions being tested and the results entered into the database. To facilitate locating the component being tested, the procedure step or attachment was also recorded. Under each applicable function, the component end condition following the test was entered. Fields that are not needed to support this appendix have been hidden. Following the individual functions, a summary of all the functions tested was added.

Once all components and functions tested by the integrated ESF test were identified, other related TS surveillance tests were reviewed to determine if they tested any of the same components tested by the integrated ESF test on the same or more frequent bases. During this review, care was taken to ensure that the other more frequent test demonstrated operability of the same component and tested the same function. Those tests that satisfied the criteria were logged under an 'other test' column adjacent to the specific component. After reviewing all the candidate 'other test' procedures provided, Westinghouse made an assessment as to whether or not the integrated ESF test was the sole/primary test for each component. An initial categorization of the components was then made. The 'categories' are defined as follows:

- Category A The integrated ESF test is the sole/primary test which demonstrates the operability or function of these components. These components perform an engineered safety function. The PSA model addresses (or should address) failure of these components. They may be modeled explicitly, modeled via a subsuming component, or modeled via a surrogate event.

- Category B Similar to Category A, the integrated ESF test is the sole/primary test which demonstrates the operability or function of these components. Unlike the Category A components, the Category B components are not included in the PSA model. Failure of these components therefore does not affect the calculated risk. The rationale for excluding them from the model is provided in the database. For example, valves which are normally in their safeguards-actuated position may not be modeled because the safeguards signal is "confirmatory" - the signal is necessary only if the event should occur while the associated system is in an unusual or infrequent configuration.

- Category C The integrated ESF test is not the sole/primary test which demonstrates the operability or function of these components. Other, more frequently performed

surveillance tests ensure that changes to the integrated ESF test frequency would not affect the failure probabilities for these components.

The Category 'A' and 'B' components then became the focus and were reviewed further to determine the PSA impact. The PSA review and analyses are documented in Section C4.0.

C3.2 INPUT

Westinghouse used electronic copies of current TS surveillance procedures provide by Palisades to perform the review and develop the matrix database. The following table provides a list of the surveillance procedures included in the review, including the integrated ESF procedures:

**Table C3.2a
ESF Surveillance Test Procedure**

Procedure Number	Procedure Title	Frequency
RT-8C, Revision 12	Engineered safeguards System – Left Channel	Once Every 18 Months
RT-8D, Revision 12	Engineered safeguards System – Right Channel	Once Every 18 Months
QO-1, Revision 47	The Safety Injection System	Once Every Quarter
QO-5, Revision 61	Valve Test Procedure	Once Every Quarter
QO-27, Revision 8	CVCS Control, Motor Operated and Check Valves.	Once Every 18 Months
RE-137, Revision 1	Calibration of Bus IC Undervoltage and Time Delay Relays	Once Every 18 Months
RE-138, Revision 1	Calibration of Bus ID Undervoltage and Time Delay Relays	Once Every 18 Months
RE-139-1, Revision 1	Test Starting Time of DG 1-1	Once Every 18 Months
RE-139-2, Revision 1	Test Starting Time of DG 1-2	Once Every 18 Months
RI-6B, Revision 2	Containment Pressure Channel Calibration	Once Every 18 Months
RI-7, Revision 10	Low Pressure SIS Initiation Logic Channel Calibration	Once Every 18 Months
RO-97, Revision 11	Auxiliary Feedwater Automatic Initiation Test	Once Every 18 Months
RT-129, Revision 3	Functional Test of Bus 1C Undervoltage Relays.	Once Every 18 Months
RT-130, Revision 3	Functional Test of Bus 1D Undervoltage Relays	Once Every 18 Months
QO-6, Revision 36	Cold Shutdown Valve Tests	Once Every 18 Months
MO-7A-1, Revision 56	EDG 1-1	Once Every Month
MO-7A-2, Revision 54	EDG 1-2	Once Every Month
RO-12, Revision 26	Containment High Pressure (CHP) and Spray System Tests	Once Every 18 Months
RO-28, Revision 19	Control Room/TSC Ventilation	Once Every 18 Months

C3.3 EVALUATION, ANALYSES AND RESULTS

The component categorization process is described in detail in the body of the topical report, Section 4.0, therefore it shall not be repeated here. Table C3.3a provides a numerical summary of the classification results specifically for Palisades.

Table C3.3a
Categorization Summary



Figures C3-1, C3-2 and C3-3 illustrate where there is overlap in the integrated ESF testing at Palisades. They are simplified illustrations and therefore depict only a rough approximation of overlap. They are not intended to provide engineering and system design detail. The figures were constructed starting with the basic components of the logic path from the sensor to the end equipment. Then the tests covering various components in the logic path were added. Figure C3-1 illustrates testing that addresses SIAS actuation. Figure C3-2 covers Undervoltage sensing and Load shedding. Figure C3-3 covers EDG load sequencing. The test procedures referenced in these diagrams are also mapped to specific components in the project database under the headings of "Other Test 1, 2, 3" etc.

Figure C3.3-1
SIAS Surveillance Procedures - Palisades

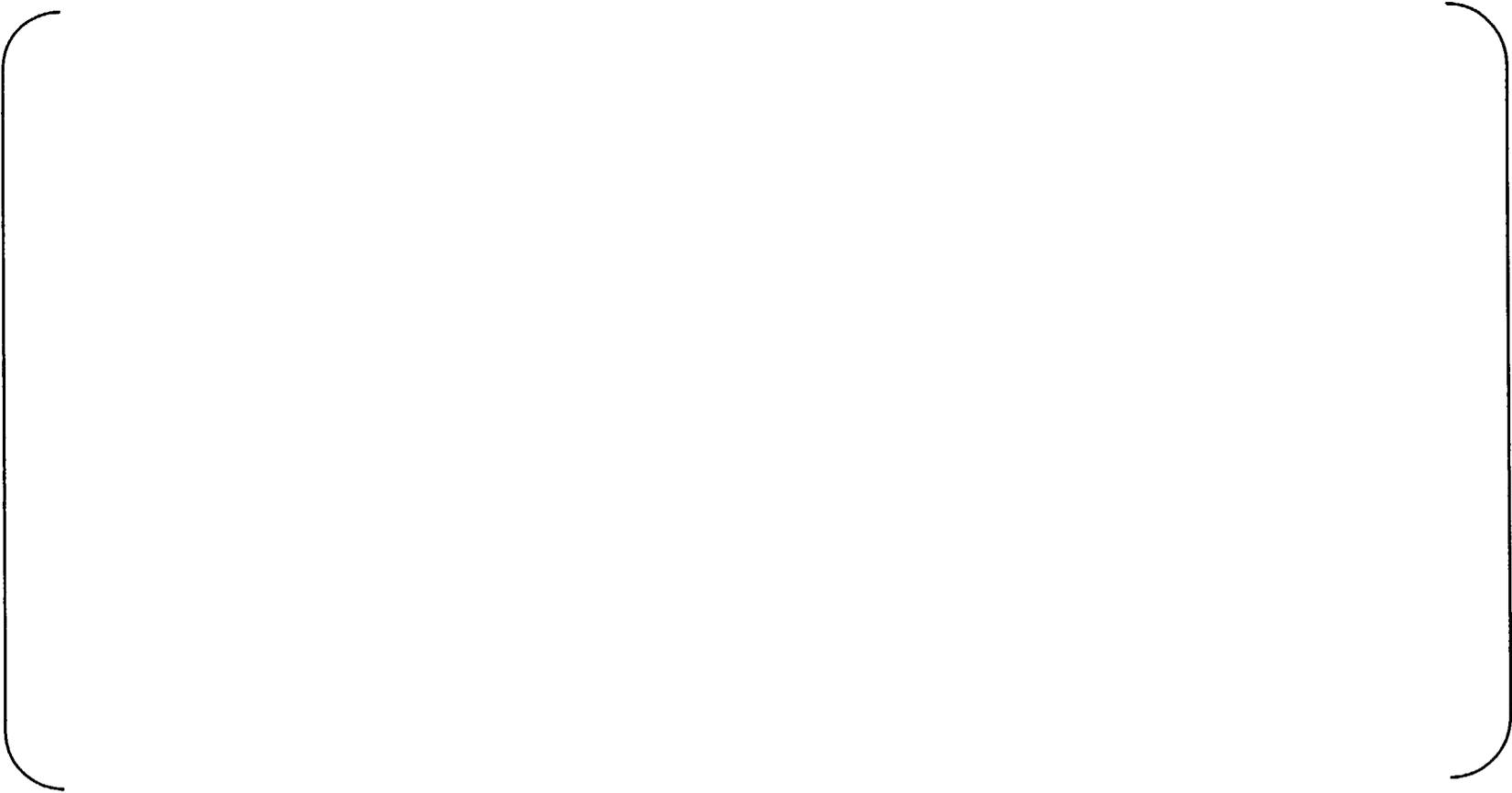


Figure C3.3-2
Under Voltage/Load Shed Surveillance Procedures - Palisades



Figure C3.3-3
EDG Load Sequence Surveillance Procedures - Palisades



C4.0 PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE

As mentioned previously, Westinghouse performed a preliminary categorization and assessment of components tested by the Integrated ESF test functions for Palisades. Palisades used the preliminary assessment as a foundation and starting point to perform the PSA analysis described in this section. The categorization begins with the testing matrix described in Section C3.0. The matrix was used to identify components whose reliability appears to be demonstrated primarily/solely by the integrated ESF test.

The Palisades PSA Master List of basic events was reviewed to determine if and how the model addresses each such component or function. The results of the review were documented in a database which relates the components to the associated basic events. The components were categorized, based on the type of changes to the event frequencies or modeling details that would be needed in order to quantify the change in risk associated with the proposed change in the integrated ESF test frequency. The actual changes to the model and the requantification of the model was performed by Palisades. The remainder of Section C4.0 is derived from the risk analyses performed by Palisades.

This analysis evaluates the risk significance of changing frequency of performing the integrated ESF testing implemented by Surveillance Tests RT-8C and RT-8D. The test intervals would be changed from requiring both tests each refueling outage to conducting one test each refueling outage on a staggered interval such that the tests are conducted on alternate outages. In addition, this analysis evaluates the capability and quality of the Palisades PSA model with respect to logic and components that implement ESF Actuation and Load Shed on Loss of Offsite Power.

Major Assumptions

The plant is assumed to be in either mode 1, 2 or 3 as the initial condition prior to an event.

Average component unavailabilities are included.

Minor Assumptions

The LERF was not evaluated in this analysis for Palisades. The proposed changes do not directly impact the frequency of events that dominate LERF. The proposed changes do not impact the makeup of the expected releases. The changes will result in similar increases in failure rates (due to changes in AC power availability as a result of the test interval extension) of components in systems that would impact release rates (e.g. containment spray).

Methodology

The current Palisades PSA model was evaluated for completeness and accuracy regarding the capability to adequately assess the risk significance of the change in test intervals for the components and functions tested via RT-8C and RT-8D (Engineered Safeguards System - Left Channel/ Engineered Safeguards System – Right Channel). Any problems noted will be rectified or accounted for as part of the evaluation of the test interval extension to assure that modeling issues that could impact the results have been corrected or considered. Necessary changes to the model were identified. In the long term, several basic events need to be added to the model load shed logic. For this analysis the required additional component failures were accounted for by adjusting the probabilities of surrogate events. Two common cause terms were required and were added to the model. The potential for operator intervention was considered and

an operator action was also included in the model. For this analysis a screening value of 0.1 was used for the operator action. The common cause terms and the operator action need to be included in the long-term corrections to the model. The changes for this evaluation are in the form of data changes to the basic event probabilities. Currently, several basic event probabilities for components that are tested use demand failure data versus hourly failure rates. Hourly failure rates are necessary for standby components whose operability is established by testing. The hourly failure rates allow for an evaluation of the impact of the extension of the test interval on the probability that the component may fail to perform its function. Revised component probabilities were developed to evaluate the change in core damage frequency (i.e. Δ CDF) that would result from the test interval extension. The Δ CDF was determined to establish the risk significance category of the proposed change.

C4.1 MODEL ANALYSIS

A review of the current Palisades PSA model determined that there are deficiencies associated with the load shed logic developed under logic gates PLSRE11 and PLSRE21. The load shed circuitry utilizes four relays on each channel to implement the breaker opening operations to load shed components from the safety buses. Currently the PSA model includes a basic event for one relay on each channel. Either the other three relays need to be added to the logic or the current basic events used as surrogates to represent the probability of failure of the four relays with appropriate updates to the model documentation to clarify the use of surrogate events and appropriate data to evaluate the test interval extension. There is no common cause development for the potential failure due to common cause between relays or the additional breakers on opposite channels. The model currently does not include any event that represents the probability that breakers required to be shed from the buses might fail to open and clear the buses. Either individual basic events for the breakers required to open or a surrogate event for each channel needs to be developed with appropriate data to evaluate the test interval extension. In addition, the potential for common cause failure of breakers on each bus failing to open due to common cause factors needs to be developed and included in the model.

In addition, it was determined that the significant contribution (>95%) to the Δ CDF was the result of a major assumption in the current PSA model. In the model for station blackout events for scenarios where offsite power is lost and neither a EDG nor offsite power is recovered station batteries are depleted and it is assumed that makeup sources to the AFW system are failed with a probability of 1.0 due to loss of instrumentation and the operators inability to accurately control secondary cooling. However, the significant contributors to the Δ CDF are the breaker and relay failure for load shed during a loss of offsite power (station blackout). Since the sequences that dominate the change in CDF do not involve events (LOCAs, etc) that require an SIAS signal, the timing of the EDG start and powering the bus are less critical and operator action to correct the conditions and establish onsite AC power are possible and should not be prohibited by the assumption. Sensitivity cases to evaluate the impact of the assumption were performed and discussed below. The assumption should be maintained for other, actual long-term, non-recoverable failures of all AC power.

Because of the model limitations, the evaluation of the change from the extension of the test interval was approximated using surrogate events to represent component failures that are not presently in the model. The model logic at gates PLSRE11 and PLSRE 21 include basic events for breakers 152-106 and 152-202 fail to open due their impact on the EDG breaker closure circuitry. These events are appropriate events to use as surrogates for the breaker failure to open events for load shed. As previously noted each logic gate includes the failure of one of the four relays that actuate the load-shed logic. These events were used as surrogates to represent the impact of the extension of the test interval on the probability of failure of the load shed relays.

A prior activity involved a review of components included in the tests (RT-8C/RT-8D) to identify those that are only tested during the RT-8C/RT-8D tests and those that are included in other tests that are conducted at the same or greater frequency. Components not included in any other tests will be affected by the test interval extension. The extension of the test interval results in longer time frames for time dependent failures to occur in (or reduction in detection capability due to less frequent checks). Components whose functions are verified by RT-8C/RT-8D and also verified by other tests were not impacted since the probabilities of basic events associated with those components will continue to be controlled by the other test(s) as long as those test occur at least once per refueling cycle or greater. Westinghouse, based on information provided by the Palisades plant staff, completed the review of component testing and developed the determination of components that are impacted by changing the test interval. Their results were reviewed and commented on by Palisades' staff and other CEOG staff. The results of this review were used as the basis completing the assessment of the change in CDF due to the test interval extension. The summarization identifies those components that were determined to not be covered by another test and therefore are impacted by the interval extension.

Common cause factors for relays and breakers were developed using the MGL (Multiple Greek Letter) methodology. The factors were used to create common cause event probabilities for breakers (P-CBCC-SG-MA) and relays (R-RECC-LOADSHED) and added to the model at the PLSRE11 and PLSRE21 logic gates with base case values of 3.50E-004 and 3.00E-005, respectively. The probabilities for the common cause basic events were modified by the changes in breaker and relay failure probabilities as part of the change to test interval extension.

Necessary changes to the basic event probabilities for the components identified as affected by the test interval extension are described below.

The current baseline CDF for the Palisades PSA model is { } per/yr. A sensitivity case was developed to provide an initial assessment of the impact of the proposed change. The current probabilities for the surrogate events (P-CBMA-152-106 breaker 152-106, P-CBMA-152-202 breaker 152-202, R-REMB-194-108 relay 194-108, and R-REMB-194-211 relay 194-211) were doubled to account for the test interval extension. Breaker basic event probabilities were changed from { } to { } and relay basic events from { } to { } per/yr.

Based on the results of the preliminary assessment, surrogate event probabilities were modified to account for: (1) the number of breakers that should be in the model and to account for those affected by the change in test interval and (2) the number of relays that should be in the model and to account for those affected by the change in test interval. For this case ten (10) breakers were added to the left channel [the list included 152-105 and 152-106, which are already in the model], seven (7) were added to the right [the list included 152-203 and 152-202, which are already in the model] and three relays were added to each channel. The probabilities assigned to the surrogates were generated based on each of the breakers and relays that are required to operate on load shed. For each component new probabilities were generated based on the test intervals. In addition, for breakers on standby or routinely rotated equipment the probability that the breaker is closed was generated. For normally operating equipment the probability was assigned as 1.0. These probabilities were created since these breakers cannot impact load shed when they are not closed. The probability that they could cause the failure of load shed is a function of the probability that they are closed. The probability that the breakers could affect load shed was calculated as the product of their probability of failure and the probability that they may be closed during the operating cycle. The relays were considered to be in the proper state all of the time and their probabilities of failure

breaker operation twice/year, the updated CDF would be { } per/yr. This would result in a ΔCDF of ~{ } per/yr.

- P-CBMA-152-106 was changed from { }
- P-CBMA-152-202 was changed from { }
- R-REMB-194-108 was unchanged
- R-REMB-194-211 was unchanged
- P-CBCC-SG-MA was unchanged
- R-RECC-LOADSHED was unchanged

The CDF for this case is { } (3877 cut sets – non-subsumed). This CDF is the updated value resulting from the test interval extension with risk informed failure rates for breaker failures.

A review of the results show that the > 99% of the ΔCDF are cut sets that are the result of a Loss of Offsite Power event and failures of components the preclude that ability to provide long term suction sources (transfer from an alternate storage tank, fire protection or service water) to the AFW pumps. These represent scenarios in which the plant response is initially successful with secondary cooling from the turbine-driven AFW pump. The loss of offsite power combined with the failure of both EDGs AND failure to recover offsite power or a EDG results in core damage several hours into the event due to a late failure of secondary cooling. These are not scenarios that require an ESF actuation signal for success. The scenarios that require an ESF (SIAS – all LOCAs. Main Steam Line Breaks and Steam generator Tube Rupture) actuation signal and would be most affected by the extended test interval do not contribute significantly to the ΔCDF.

The initial cases were rerun with the assumption that there is a 1.00E-01 probability of operator action failing to correct the load shed problems and complete aligning a EDG to one of the buses.

The results obtained for core damage frequency and change in core damage frequency per year are:

Case 1a	()
Case 2a	
ΔCDF	
Case 3a	
ΔCDF	

The results are also impacted by a major assumption in the current Palisades PSA model. Currently for Station Blackout (SBO) Events, the PSA model includes an assumption that given a Loss of Offsite Power AND failure to recover offsite power or an EDG within 4 hours, the station batteries are depleted and it is assumed that the resulting lack of instrumentation results in the inability to continue successful secondary cooling. This assumption precludes the use of diesel driven fire pumps to provide makeup to an operating AFW pump. Sensitivity cases were analyzed with the assumption removed and credit taken for two diesel driven fire pumps to provide suction to AFW and makeup to the Condensate Storage Tank. Gate A12F of the Auxiliary Feedwater Model was extracted and used in the SBO event tree for heading “Secondary Cooling Long Term” in place of the assumption in sequence 21-23. Gate A12F was modified to remove the motor-driven fire pump and leave only the two diesel-driven pumps as makeup sources to the AFW pump (P-8B) and Condensate Storage Tank (T-2).

The previous cases were rerun with the assumption altered to represent a human error combined (OR) with the logic for the available makeup sources. Under these conditions the baseline CDF becomes { } per/yr. The CDF from extending the test interval is { } per/yr. This results in a ΔCDF of { } per/yr.

C4.2 SCOPE OF PSA

The Palisades PSA is an at-power, internal events PSA. Both Level 1 and Level 2 are addressed. The model is routinely updated as a result of plant changes, increased fidelity for particular applications and new quantification techniques.

C4.2.1 At-Power Model Structure

Typical large-linked fault tree techniques underlie the analysis. For illustration purposes, Palisades has small event trees that capture the sequences quantified with the model. These illustrations became the basis for the top logic employed in the large fault tree model created for Palisades.

The PSA model has detailed trees for each of the front-line systems identified in the top logic illustrated on the event trees. Likewise, the front-line systems spawn the need for support system trees. To ensure traceability, Palisades keeps a set of documents that catalogue data values and assumptions for the front-line and support system trees.

The PSA model is quantified with a mix of generic and Palisades plant-specific data. The scope of the plant-specific data analysis included initiating event frequencies and equipment for which plant-specific data allows for statistically meaningful estimates of failure rates and failure probabilities. The plant-specific data arises, in part, from a review of Licensee Event Reports, monthly plant reports, and in internal Incident Reports. These capture important plant failure modes, events and trends.

The PSA model includes quantified human failure events. The methods created conservative screening values for human failure events with additional study made of those events that are important to typical plant risk metrics.

C4.2.2 Shutdown Risk Assessment

Shutdown modes are outside the scope of the Palisades PSA model.

C4.2.3 PSA Detail Needed for Change

The Palisades PSA explicitly models the functions associated with ESCS. Key modeling features are discussed below.

C4.2.3.1 Modeling and Quantification

Common Cause

The Multiple Greek Letter (MGL) method is used to specifically model common-cause failures. Common cause basic events have been directly incorporated into the fault tree models, and represent the failure of all components within a defined group by a specified failure mode, e.g. all safety injection pumps fail to start on demand due to common causes. This approach is used throughout the Palisades PSA.

Other key common cause impacts related to the EDGs are 125VDC batteries, SW pumps, ESFAS UV channels and 4kV load breakers.

Quantification

The large linked-fault-tree model for Palisades is configured, edited and analyzed with SAPHIRE.

C4.3 QUALITY OF PALISADES PSA

Palisades utility personnel have constructed the Palisades PSA with a strong commitment toward developing a complete and accurate PSA. This commitment can be seen through the following elements:

- Formal qualification program for the PSA staff
- Use of procedures to control PSA processes
- Independent reviews (checks) of PSA documents
- Comprehensive PSA Configuration Control Program
 - Quarterly plant change monitoring program
 - Process to control PSA quantification software
 - Active open items list
 - Interface with the site corrective action program
 - Process to maintain configuration of previous risk-informed decisions
- Peer reviews
- Participation in the CEOG cross comparison process
- Incorporation, where applicable, of CEOG PSA Technical Positions
- Commitment of continuous quality improvement

C4.4 RESULTS AND CONCLUSIONS

Ninety-nine percent (99%) of the cut sets involve a loss of offsite power and no ESF condition. The component failures that contribute to the Δ CDF (breakers fail to open or relays fail to actuate – failure to load shed the safety-related buses) could be compensated for by operator actions, which were not initially credited in the Palisades PSA model. The dominant contributors to the Δ CDF are failures that prohibit the EDG breakers from closing. Including an operator action to recover from load shed failures would drop the Δ CDF into the region III (not risk significant category). Since the timing of the EDGs accepting the safety loads is not critical for scenarios where safety injection is not required and because the scenarios of interest are ones in which initial plant response is successful providing adequate time for recovery, including an operator action to mitigate the event is an appropriate consideration. The actions considered here are included in the current Emergency Operating Procedure (EOP 3.0) “Station Blackout,” Revision 12, 12/28/01.

The results are driven by the assumption of failure when recovery of offsite power or a EDG was unsuccessful within four hours. Significant portions of the cut sets that are related to the assumption include failures that are not consistent with the assumption as developed. The cut sets include failure to makeup fuel oil to the EDGs, EDGs fail to continue to run, load shed failure that are correctable and if corrected allow the EDG to power the bus (relate to the operator action discussed above), etc. If the EDG starts or is recovered shortly after the event the initial impact on the batteries is significantly minimized or compensated for by the EDG.

The safety significance is based on the increase in Core Damage Frequency (CDF) for the assumed change in the test interval for specified components. Based on changes to the model necessary to evaluate the test interval extension and adjustments made as a result of the review of the results, the Δ CDF { } is considered to be of low safety significance (Region III).

APPENDIX D

APPLICATION OF WCAP-15830-NP TO WATERFORD UNIT 3

TABLE OF CONTENTS

D1.0	ABSTRACT	D-4
D2.0	BACKGROUND	D-5
D2.1	ESFAS Description.....	D-5
D2.1.1	Initiating Logic.....	D-5
D2.1.2	Actuation Logic	D-6
D2.2	Waterford Unit 3 Configuration.....	D-7
D2.2.1	Diesel Generators.....	D-7
D2.2.2	EDG Load Shedding	D-8
D2.2.3	DG Auto Start and Sequencer Operation	D-8
D2.3	Current Technical Specifications	D-9
D2.4	Proposed Changes to Technical Specifications.....	D-10
D3.0	TEST MATRIX AND COMPONENT CATEGORIZATION	D-11
D3.1	Method Discussion.....	D-11
D3.1.1	Integrated ESF Test (OP-903-115 and OP-903-116).....	D-11
D3.2	Input.....	D-13
D3.3	Evaluation, Analyses and Results	D-14
D4.0	PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE.....	D-19
D4.1	Model Analysis	D-21
D4.2	Scope of PSA.....	D-31
D4.2.1	At-Power Model Structure	D-31
D4.2.2	Shutdown Risk Assessment	D-31
D4.2.3	PSA Detail Needed for Change.....	D-32
D4.3	Quality of Waterford Unit 3 PSA	D-32
D4.4	PSA Software.....	D-33
D4.4.1	CAFTA	D-33
D4.4.2	PRAQuant.....	D-33
D4.4.3	FORTE.....	D-33
D4.5	Results and Conclusions	D-33

LIST OF TABLES

D2.2.1a	Emergency Diesel Generators	D-7
D2.3a	Existing Surveillance Test Intervals.....	D-9
D2.4a	Proposed Surveillance Test Intervals	D-10
D3.1a	Applicable Database Fields	D-12
D3.2a	ESF Surveillance Test Procedures.....	D-13
D3.3a	Categorization Summary for Waterford Unit 3	D-14
D4.1.1	Failure to Shed A Train Components	D-23
D4.1.2	Failure to Shed B Train Components	D-26
D4.1.3	Existing Bus Fails to Shed Events.....	D-28
D4.1.4	New Bus Fails to Shed Events.....	D-29
D4.1.5	Wet and Dry Cooling Tower Fail to Sequence Probabilities.....	D-30

LIST OF FIGURES

D3-1	ESFAS Surveillance Procedures – Waterford Unit 2	D-16
D3-2	Under Voltage/Load Shed Surveillance Procedures – Waterford Unit 3	D-17
D3-3	EDG Load Sequence Surveillance Procedures – Waterford Unit 3	D-18

D1.0 ABSTRACT

Combustion Engineering Owners Group (CEOG) Task 2016, "Staggered Integrated ESF Testing" used a risk-Informed approach to demonstrate that any change in risk would be negligible if a staggered test frequency were adopted for integrated Engineered Safety Features (ESF) testing. Currently, integrated ESF testing is performed on both trains each refueling cycle. Using a staggered approach, only one train would be tested each refueling outage. The basic premise of the proposed change is the belief that the integrated ESF test is not the primary/sole operability test for the majority of the components tested. Other surveillance procedures are performed on many of these components and functions on the same or more frequent basis. Therefore, there may be considerable overlap between the integrated ESF test and other testing. For the components/functions that are tested only by the integrated ESF test, the risk model was adjusted, the risk associated with the change recalculated, and the overall risk requantified. In some cases, it was possible to develop a reasonable deterministic basis for assuming the component failure mode addressed by the integrated ESF test was not risk-significant. These components were exempt from further Probabilistic Safety Analysis (PSA) review and analysis. The overall task was broken down into more manageable units of work. The first was the procedure review and matrix development. The second was the categorization of components and functions tested by the integrated ESF test. Third was the preliminary PSA assessment and Category "A" component sub-categorization. Last, was the finalization of the PSA assessment, adjusting the PSA models and calculating the change in risk associated with the change in Surveillance Test Interval (STI).

This Appendix addresses application of staggered integrated ESF testing at Waterford Unit 3 (WSES-3). It describes in detail the plant specific procedure review, component categorization and risk analyses as performed for WSES-3 to support the change to staggered integrated ESF testing. The Technical Specification Surveillance Requirements addressed by the integrated ESF test are listed in Table D2.3a.

The risk contribution associated with the increased frequency, 36 months on a staggered bases, has been quantitatively evaluated using the current plant-specific PSA for WSES-3. The calculated increase in Core Damage Frequency (Δ CDF) due to increasing the surveillance interval from an 18 month interval to a 36 month staggered test interval is []. The estimated change in Large Early Release Frequency (Δ LERF) is [].

The change results in a small, but acceptable, risk increase. There is also some risk reductions associated averting unnecessary plant transients and with reduced risk during shutdown operations, however, these reductions were not quantified.

D2.0 BACKGROUND

The safety related instrumentation and controls of the Engineered Safety Feature Systems (ESFS) include: (1) the Engineered Safety Feature Actuation System (ESFAS) which consists of the electrical and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals that actuate the required ESF systems, and (2) the arrangement of components that perform protective actions after receiving a signal from either the ESFAS or the operator. A CE designed ESFAS is in place at WSES-3.

D2.1 ESFAS DESCRIPTION

The actuation circuits for the ESFAS are all similar except for specific inputs, operating bypasses, and actuation devices. The SIAS described is typical of all ESFAS. The actuation systems consist of the sensors, logic and actuation circuits that monitor selected plant parameters and provide an actuation signal to each individual actuated component in the ESF system if these plant parameters reach preselected setpoints. Each actuation system is identical except that specific inputs (and blocks where provided) vary from system to system and the actuated devices are different.

Two-out-of-four coincidence of like initiating trip signals from four independent measurement channels is required to actuate any ESF system. Each actuation system logic, including testing features, is similar to the logic for the Reactor Protective System, and is contained in the same physical enclosure. The combination of the ESFAS and Reactor Protective System (RPS) is designated Plant Protection System (PPS).

The following actuation signals are generated by the ESFAS when the monitored variables reach the levels that are indicative of conditions that require protective action:

- a) Safety Injection Actuation Signal (SIAS)
- b) Containment Isolation Actuation Signal (CIAS)
- c) Containment Spray Actuation Signal (CSAS)
- d) Main Steam Isolation Signal (MSIS)
- e) Emergency Feedwater Actuation Signal (EFAS)
- f) Recirculation Actuation Signal (RAS)

The following is a brief description of SIAS.

D2.1.1 Initiating Logic

The SIAS initiating logic:

- a) Compares the analog signals received from the protective measurement channels with preset levels.
- b) Provides a variable setpoint for plant start-up, shutdown, and low power testing.
- c) Forms two-out-of-four coincidence of like signals which have reached preset levels.
- d) Provides a means for manual blocking of pressurizer pressure signals if permissive conditions are met.
- e) Provides channel and signal status information to the operator, and
- f) Provides four SIAS initiation signals for each actuation signal to the SIAS actuating logic.

The SIAS initiating logic consists of bistables, bistable output relays, trip relays, matrix relays, initiation channel output relays, manual block controls, block relays, manual testing controls, indicating lights, power supplies and interconnecting wiring.

The SIAS initiating logic is physically located in the PPS cabinet.

Signals from the protective measurement channels are sent to voltage comparator circuits (bistables) where the input signals are compared to predetermined setpoints. Whenever a channel parameter reaches the predetermined setpoint, the channel bistable deenergizes the bistable output relay. The bistable output relay deenergizes the trip relays. Contacts of the trip relays form the SIAS initiating logic. Each set of trip relays (i.e. each channel) is powered from a redundant 120 volt vital AC distribution bus. The bistable setpoints are adjustable from the front of the PPS cabinet. Access is limited by means of a key operated cover, with an annunciator indicating cabinet access. All bistable setpoints are capable of being read out on a meter located on the PPS cabinet and are sent to the plant monitoring computer.

The SIAS initiation signals are generated in four channels, designated A, B, C and D. Two-out-of-four coincidence of initiating signals from the four protective measurement channels generates all four SIAS initiation signals. Tripping of a bistable results in a channel trip characterized by the deenergization of three trip relays.

The contacts of the four sets of three trip relays have been arranged in six logic ANDs designated AB, AC, AD, BC, BD and CD, which represent all possible two-out-of-four combinations for the four protective measurement channels. To form an AND circuit the trip relay contacts of two redundant protective measurement channels are connected in parallel (i.e. one from A and one from B). This process is continued until all combinations have been formed. Since more than one plant parameter can initiate a trip signal, the parallel pairs of trip relay contacts, each pair representing a monitored plant parameter, are connected in series (Logic OR) to form six logic matrices. The six matrices are also designated AB, AC, AD, BC, BD and CD.

Each logic matrix is connected in series with a set of four parallel logic matrix output relays (matrix relays). Each logic matrix is powered from two separate 120 volt vital AC distribution buses through dual dc power supplies

The output contacts of the matrix relays are combined into four trip paths. Each ESFAS trip path is formed by connecting six contacts, one matrix relay contact from each of the six logic matrices, in series. The six series contacts are in series with the trip path output relay. The trip path output relay contacts form the SIAS initiating logic.

D2.1.2 Actuation Logic

The SIAS actuating logic performs the following:

- a) Receives SIAS signal from the SIAS initiating logic,
- b) Forms selective two-out-of-four coincidence logic for actuation of SIAS,
- c) Provides a means for manual initiation of SIAS,
- d) Provides status information to the operator.

The SIAS actuating logic is physically located in two ESFAS auxiliary relay cabinets. One cabinet contains the logic for ESF train A equipment, while the other cabinet contains the logic for ESF train B equipment.

Four SIAS initiation signal contacts are arranged in a selective two-out-of-four coincidence logic. Each initiation signal also deenergizes the seal-in relays of its associated channel. The seal-in relays assure that the signal is not automatically removed once initiated.

Receipt of two selective SIAS initiation signals will deenergize the subgroup relays, which generate the actuation signals. This process is performed independently in both auxiliary relay cabinets, generating both train A and train B signals. Each leg of the selective two-out-of-four circuitry is powered by two (2) auctioneered DC power supplies. The four power supplies in cabinet "A" are connected to 120 V AC vital buses A and B. The four power supplies in cabinet "B" are connected to 120 V AC vital buses C and D. The two redundant power sources within each cabinet are physically separated from each other.

In MSIS there are only two initiating circuits in each channel (steam generator #1 and steam generator #2 pressure) and thus each matrix ladder consists of only two AND circuits in series. The four matrix relay outputs from each logic matrix again form four trip paths. Each trip path output relay, instead of controlling trip circuit breakers as in the RPS, controls a contact of the selective two-out-of-four circuit for the group actuation.

Testing of each ESF subgroup of actuating logic components is accomplished by use of a test module. Groups are selected such that testing may be accomplished without affecting normal plant operation (i.e. unwarranted actuation).

D2.1.2.2 Group Actuation

The components in the safety injection system are placed into various groups. Selection is made such that actuation of a group will not affect normal plant operation. Components of each group are actuated by one (1) group relay. Group relay contacts are in the power control circuit for the actuated components of each ESF system. The actuation logic causes the opening of a contact in a selective two-out-of-four circuit whenever any one of the logic matrices is deenergized. Upon opening of selective contacts in the two-out-of-four logic, the group relays deenergize and actuate the ESF system components. Sequencing of component actuation, where required, is accomplished in the power control circuit of each actuated component.

D2.2 WATERFORD UNIT 3 CONFIGURATION

The ESF functions start/align equipment required to mitigate design basis accidents. A critical aspect of the ESFAS design addresses the loss of the normal (off-site) power supply.

D2.2.1 Emergency Diesel Generators

At WSES-3, the two 4kV ESF buses are each supplied by a dedicated Emergency Diesel Generator (EDG). The table below shows the EDG to bus alignment and naming convention:

**Table D2.2.1a
Emergency Diesel Generators**

Emergency Diesel Generator	Manufacturer	4kV Bus	Channel /Division Supported
3A-S	Cooper/Bessemer	3A3-S	A
3B-S	Cooper/Bessemer	3B3-S	B

D2.2.2 EDG Load Shedding

All loads connected to the 4.16 kV buses shed upon a loss of preferred sources of power, except:

1. The 480V 3A31-S power center
2. The 480V 3B31-S power center
3. The 4.16 kV 3AB3-S bus

Then, the EDG breaker will close within 10 seconds after receipt of an emergency start signal. On EDG 3A-S, one 480V power center (3A31-S) energizes through its station service transformer concurrently with the EDG breaker closing. In addition, one power center (3A32) energizes (if SIAS is not present) through its station service transformer and one 480V MCC (3A315-S) through its station service transformer at 1/2 second intervals. EDG 3B-S energizes Buses 3AB3-S, 3B31-S, 3B32 and 3B315-S in a similar manner.

This sequence avoids the sudden imposition of the transformer inrush currents all at once, but still results in all power centers being energized and ready to assume loads within 11 seconds after EDG receipt of an emergency start signal. When the EDG is the only source of supply, non-essential loads, which can be connected to the ESF supply are not re-energized through the automatic load sequencer.

Subsequent reconnection of these loads to the EDG source can only be done manually under administrative control.

D2.2.3 DG Auto Start and Sequencer Operation

Each EDG can be started automatically either by a Safety Injection Actuation Signal or by the undervoltage relay on the respective 4.16V ESF Bus. Sequencing equipment is provided to the time sequence of loading the safety injection equipment. The sequencing function is performed by the use of time delay relays associated with the equipment.

In the normal state the sequencer circuit is kept continuously energized. Thus, the status of sequencer readiness for operation is continuously monitored. In case of loss of 125V DC power source to the sequencer or failure of any of the sequencer relay, an alarm shall be annunciated in the control room. An alarm is also initiated in the control room each time the sequencer is tested or actuated by SIAS or undervoltage contacts. Any failure in the annunciator circuitry, such as short across the output wires, will be detected the first time the sequencer is tested. Periodic testing is shown in the WSES-3 Technical Specifications.

The operation of sequencer circuit is as follows:

- 1) SIAS is reset, voltage on safety bus is normal

Sequencer relays, 62S, SO through S8, S61, SOX through S5X, S7X and S8X are energized, S6X is deenergized, all contacts to annunciator are closed. In this state sequencer remains continuously ready for action.

- 2) SIAS is tripped

Contact SIAS-1 opens and contact SIAS-2 closes. An interruption of power, for a duration of two seconds to the relays SO through S8, S61 will be created due to a delayed action of relay 62S. Upon

restoration of power, relays S0 through S8, S61 energize. They will start to pick-up relays S0X-S5X, S7X, S8X and S61X and drop out relay S6X in predetermined sequence, thus initiating sequential loading of the EDG.

3) Voltage on safety buses is lost

Undervoltage relay contacts 27-1X, 27-2X, 27-3X, 27-11X, 27-12X and 27-13X will open and remain in open position until the voltage on safety buses is restored. The undervoltage relay contacts will reclose thus starting the sequencing action for loading of EDG.

4) Sequencer circuit is tested

The contact TS/TEST is opened momentarily. The sequencer relays will be momentarily de-energized and then will pick-up in their sequential order. Indicating lights on the main control room will indicate the operation of sequencer relays throughout the test, no other action will ensure from this test.

Change of state of the sequencer relays is also monitored by the Plant Monitoring Computer (PMC). Timing of the change of state can be determined by reviews of the Sequence of Events Recorder from the PMC.

D2.3 CURRENT TECHNICAL SPECIFICATIONS

Table D2.3a lists all the Technical Specification Surveillance Requirements that apply to Integrated ESF Testing at WSES-3.

**Table D2.3a
Existing Surveillance Test Intervals**

SR	SR Description	Frequency
4.4.3.1.3.a	Verify Pressurizer Heater Load Shed on SIAS actuation	18 months
4.6.2.2.b.2	Verify ≥ 1200 gpm of CCW flow through Containment Fan Coolers A and C.	18 months
4.8.1.1.2.e.1	Verify load rejection of ≥ 498 kW while maintaining voltage and frequency.	18 months
4.8.1.1.2.e.2	Load rejection of 4000-4400 kW without tripping	18 months
4.8.1.1.2.e.3	Verify Loss of offsite power with deenergization and load shedding of emergency busses.	18 months
4.8.1.1.2.e.4	Verify SIAS without loss of offsite power with auto start of EDG and operating in standby for ≥ 5 minutes.	18 months
4.8.1.1.2.e.5	Verify Loss of offsite power in conjunction with SIAS with auto start of EDG and deenergization of emergency busses with load shedding.	18 months
4.8.1.1.2.e.6	Verify 24 hour test run.	18 months
4.8.1.1.2.e.7	Verify auto connected loads <u>not</u> exceeding the 2000 hour rating of 4400 kW.	18 months
4.8.1.1.2.e.8	Verify synchronization with offsite power while loaded with emergency loads.	18 months
4.8.1.1.2.e.9	Verify SIAS shifts EDG from Test Mode.	18 months
4.8.1.1.2.e.10	Verify fuel transfer pump test.	18 months
4.8.1.1.2.e.11	Verify sequencer load block timing.	18 months
4.8.1.1.2.e.12	Verify EDG lockout.	18 months

D2.4 PROPOSED CHANGES TO TECHNICAL SPECIFICATIONS

Table D2.4a shows the proposed TS changes that apply to WSES-3. The proposed frequency is based on WSES-3 TS definition for staggered testing.

Table D2.4a
Proposed Surveillance Test Intervals

SR	SR Description	Frequency
4.4.3.1.3.a	Verify Pressurizer Heater Load Shed on SIAS actuation	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.1	Verify load rejection of ≥ 498 kW while maintaining voltage and frequency.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.2	Load rejection of 4000-4400 kW without tripping	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.3	Verify Loss of offsite power with deenergization and load shedding of emergency busses.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.4	Verify SIAS without loss of offsite power with auto start of EDG and operating in standby for ≥ 5 minutes.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.5	Verify Loss of offsite power in conjunction with SIAS with auto start of EDG and deenergization of emergency busses with load shedding.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.7	Verify auto connected loads <u>not</u> exceeding the 2000 hour rating of 4400 kW.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.8	Verify synchronization with offsite power while loaded with emergency loads.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.9	Verify SIAS shifts EDG from Test Mode.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.10	Verify fuel transfer pump test.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.11	Verify sequencer load block timing.	36 months on a STAGGERED TEST BASIS
4.8.1.1.2.e.12	Verify EDG lockout.	36 months on a STAGGERED TEST BASIS

D3.0 TEST MATRIX AND COMPONENT CATEGORIZATION

D3.1 METHOD DISCUSSION

D3.1.1 Integrated ESF Test (OP-903-115 and OP-903-116)

The procedure is performed on A and B trains, one train at a time, every 18 months. The EDG sequencer relays are tested prior to performing the SIAS with Loss of Offsite Power Test. The SIAS Test with Offsite Power tests only subgroup relay K412 that provides an SIAS signal to the EDG start circuit. In this test the EDG does not tie onto the safety bus and load sequencing does not occur. The SIAS Test with concurrent Loss of Offsite Power starts the EDG, verifies load shed, energizes the safety bus and auto sequences loads onto the buses. This test is not used to verify SIAS actuations. Loss of Offsite Power with Integrated Safeguards is initiated by de-energizing the safety bus by opening Switchgear 2A/B Bus Tie to Switchgear 3A/B breaker. After the EDG starts cranking, then SIAS is initiated at the Auxiliary Relay Cabinet using pushbuttons S-61B and S-71B.

Objectives (functions) covered by the integrated ESF test include:

- Load Shed verification
- LOOP with concurrent SIAS Actuation
- LOOP without concurrent SIAS Actuation
- EDG Load Sequencer Response Time verification
- EDG Load Sequence verification
- Permanent Load verifications
- EDG Trips Bypassed (SIAS with LOOP) Functional verification
- SIAS shifts EDG from TEST Mode verification
- EDG Lockout Test verification
- EDG Start on Auto-Start Verification
- EDG 'ready to load' parameter verifications
- EDG Functional Test – 22 Hrs at 100% Load
- EDG Functional Test – 2 Hrs at 110% Load
- EDG Functional Test - Hot Start
- EDG Functional Test - SIAS followed by 498 KW Load Rejection
- EDG Functional Test - Full Load Rejection
- Return to Normal Offsite Power Test
- Containment Cooler CCW flow test
- Response Time Verification

An ESF Testing Matrix was prepared by Westinghouse for WSES-3 as part of CEOG Task 2016, Staggered Integrated ESF Testing. A database was used to create the matrix and to document the results of the ESF procedure review. The primary function of the database is to map the components tested by WSES-3 integrated Emergency Diesel Generator/Engineering Safety Features (EDG/ESF) test (OP-903-115 and OP-903-116), to other surveillances that test the same components and functions. The database contains references to the integrated ESF test and other tests, as well as a preliminary PSA evaluation and assessment. The preliminary PSA assessment performed by Westinghouse provided the foundation for the plant specific PSA calculation performed by WSES-3.

The procedure review portion of the database used to develop the matrix is defined by the following table. PSA evaluations and assessments are addressed in Section D4.0 of this appendix.

**Table D3.1a
Applicable Database Fields**

Column Heading	Explanation
Temporary Original Sort	The data sort order in the data base previously sent to WSES-3
Data Entry Order	The order that data was originally entered into the database.
Procedure Number	OP-903-115 or OP-903-116
Component ID	Component ID used in OP-903-115 and OP-903-116.
Component Description	Component description used in OP-903-115 and OP-903-116.
Functions tested by the Integrated test.	The large blue section of the database shows the location in OP-903-115 or OP-903-116 where a particular component was identified for a particular ESF function. For each component, the database shows the position verified. A blank field indicates that that function is not tested by the integrated test.
Integrated test Summary	Summarizes the functions tested by the integrated test (OP-903-115 or OP-903-116) for each component. Note that this field is filled in once for each component (sort by Component Description)
Additional Information	Additional information included by Westinghouse.
Waterford Comments	Comments supplied by WSES-3.
Cat	Component category, "A", "B" or "C". Categories are defined and explained below. The initial PSA assessment further divides Category "A" components into A-1, A-2, A-3 or A-4 to facilitate requantification of risk by WSES-3. The screening process used to sort components into subcategories is described in section 4.0 of the topical report and is related specifically to WSES-3.
Assessment	An initial assessment that supports why the component is initially categorized "A", "B" or "C". Only one Assessment was written for each component (sort by Component Description)
Other Test 1 through 5	Lists references to other WSES-3 surveillance procedures that overlap the integrated ESF test OP-903-115 and OP-903-116.

The matrix was developed as follows: First, integrated ESF tests, OP-903-115 and OP-903-116 were reviewed to identify the components and functions being tested and the results entered into the database. To facilitate future sorting of the data, the component type was also added to the database. To facilitate locating the component being tested, the procedure step or attachment was also recorded. Under each applicable function, the component end condition following the test was entered. Fields that are not needed to support this appendix (i.e. notes and comments) have been hidden. Following the individual functions, a summary of all the functions tested was added.

Once all components and functions tested by the integrated ESF test were identified, other related TS surveillance tests were reviewed to determine if they tested any of the same components tested by the integrated ESF test on the same or more frequent bases. During this review, care was taken to ensure that the other more frequent test demonstrated operability of the same component and tested the same function. Those tests that satisfied the criteria were logged under an 'other test' column adjacent to the specific component. After reviewing all candidate 'other test' procedures provided by WSES-3, Westinghouse made an assessment as to whether or not the integrated ESF test was the sole/primary test

for each component. An initial categorization of the components was then made. The 'categories' are defined as follows:

- Category A The integrated ESF test is the sole/primary test which demonstrates the operability or function of these components. These components perform an engineered safeguards function. The PSA model addresses (or should address) failure of these components. They may be modeled explicitly, modeled via a subsuming component, or modeled via a surrogate event.

- Category B Similar to Category A, the integrated test is the sole/primary test that demonstrates the operability or function of these components. Unlike the Category A components, the Category B components are not included in the PSA model. Failure of these components therefore does not affect the calculated risk. The rationale for excluding them from the model is provided in the database. For example, valves which are normally in their safeguards-actuated position may not be modeled because the safeguards signal is "confirmatory" - the signal is necessary only if the event should occur while the associated system is in an unusual or infrequent configuration.

- Category C The integrated test is not the sole/primary test which demonstrates the operability or function of these components. Other, more frequently performed surveillance tests ensure that changes to the integrated ESF test frequency would not affect the failure probabilities for these components.

The category 'A' components then became the focus and were reviewed further to determine the PSA impact. The PSA review and analyses are documented in Section D4.0.

D3.2 INPUT

Westinghouse used electronic copies of current TS surveillance procedures provide by WSES-3 on a Compact Disc (CD) to perform the review and develop the matrix database. The following table provides a list of the surveillance procedures included in the review, including the integrated ESF procedures:

Table D3.2a ESF Surveillance Test Procedures		
Procedure Number	Procedure Title	Frequency
OP-903-115, Rev. 6	Train A Integrated Emergency Diesel Generator/Engineering Safety Features Test	Once every 18 months
OP-903-116, Rev. 7	Train B Integrated Emergency Diesel Generator/Engineering Safety Features Test	Once every 18 months
OP-903-029, Rev. 9	Safety Injection Actuation Signal Test	Once every 18 months
OP-903-094, Rev. 10	ESFAS Subgroup Relay Test – Operating	Once every Quarter
OP-903-095, Rev. 7	ESFAS Subgroup Relay Test – Shutdown	Once every 18 months
OP-903-068, Rev. 12	EDG and Subgroup Relay Actuation Verification	Once every 62 days
OP-903-011, Rev.8	High Pressure Safety Injection Pump Pre-service Operability Check	Once every 18 months
OP-903-107 Rev.14	Plant Protection system Channel Functional Test	Once every Quarter
OP-903-028, Rev.4	Pressurizer Heater Emergency Power Supply Functional Test	Once every 18 months

Table D3.2a ESF Surveillance Test Procedures		
Procedure Number	Procedure Title	Frequency
OP-903-001 Rev. [Not provided]	Operations Shift and Daily Logs	Once Every 12 hours
OP-903-003, Rev.10	Charging Pump Operability Check	Once every Quarter
OP-903-004, Rev.10	Boric Acid Pump Operability Check	Once every Quarter
OP-903-030, Rev.13	Safety Injection Pump Operability Verification	Once every Quarter
OP-903-035 Rev.11	Containment Spray Pump Operability Check	Once every Quarter
OP-903-050 Rev.16	Component Cooling Water and Auxiliary Cooling Water Pump and Valve Operability test	Once every Quarter
OP-903-129 Rev.1	Component Cooling Water Makeup Pump Operability test	Once every Quarter
OP-903-063 Rev.11	Chilled Water Pump Operability test	Once every Quarter
OP-903-46, Rev. 15	Emergency Feedwater Pump Operability test	Once every Quarter
MI-003-219, Rev. 4	Plant Protection System Sensor Bi-Stable Response Time Verification Channel A,B,C,D	Once every 18 months
MI-003-221, Rev. 4	Plant Protection System Sensor Bi-Stable Response Time Verification Channel A,B,C,D	Once every 18 months
MI-003-222, Rev. 2	Matrix Response Time Verifications for Plant Protection System and Engineered Safety Features System, Channel A,B,C,D	Once every 18 months

D3.3 EVALUATION, ANALYSES AND RESULTS

The component categorization process is described in detail in the body of the topical report, Section 4.0, therefore it shall not be repeated here. Table D3.3a provides a numerical summary of the classification results specifically for WSES-3.

**Table D3.3a
Categorization Summary for Waterford Unit 3**



Figures D3-1, D3-2 and D3-3 illustrate where there is overlap in integrated ESF testing at WSES-3. They are simplified illustrations and therefore depict only a rough approximation of overlap. They are not

intended to provide engineering and system design detail. The figures were constructed starting with the basic components of the logic path from the sensor to the end equipment. Then the tests covering various components in the logic path were added. Figure D3-1 illustrates testing that addresses SIAS actuation. Figure D3-2 covers Undervoltage sensing and Load shedding. Figure D3-3 covers EDG load sequencing. The test procedures referenced in these diagrams are also mapped to specific components in the project database (Appendix D1) under the headings of “Other Test 1, 2, 3” etc.

Figure D3.3-1
ESFAS Surveillance Procedures - Waterford Unit 3

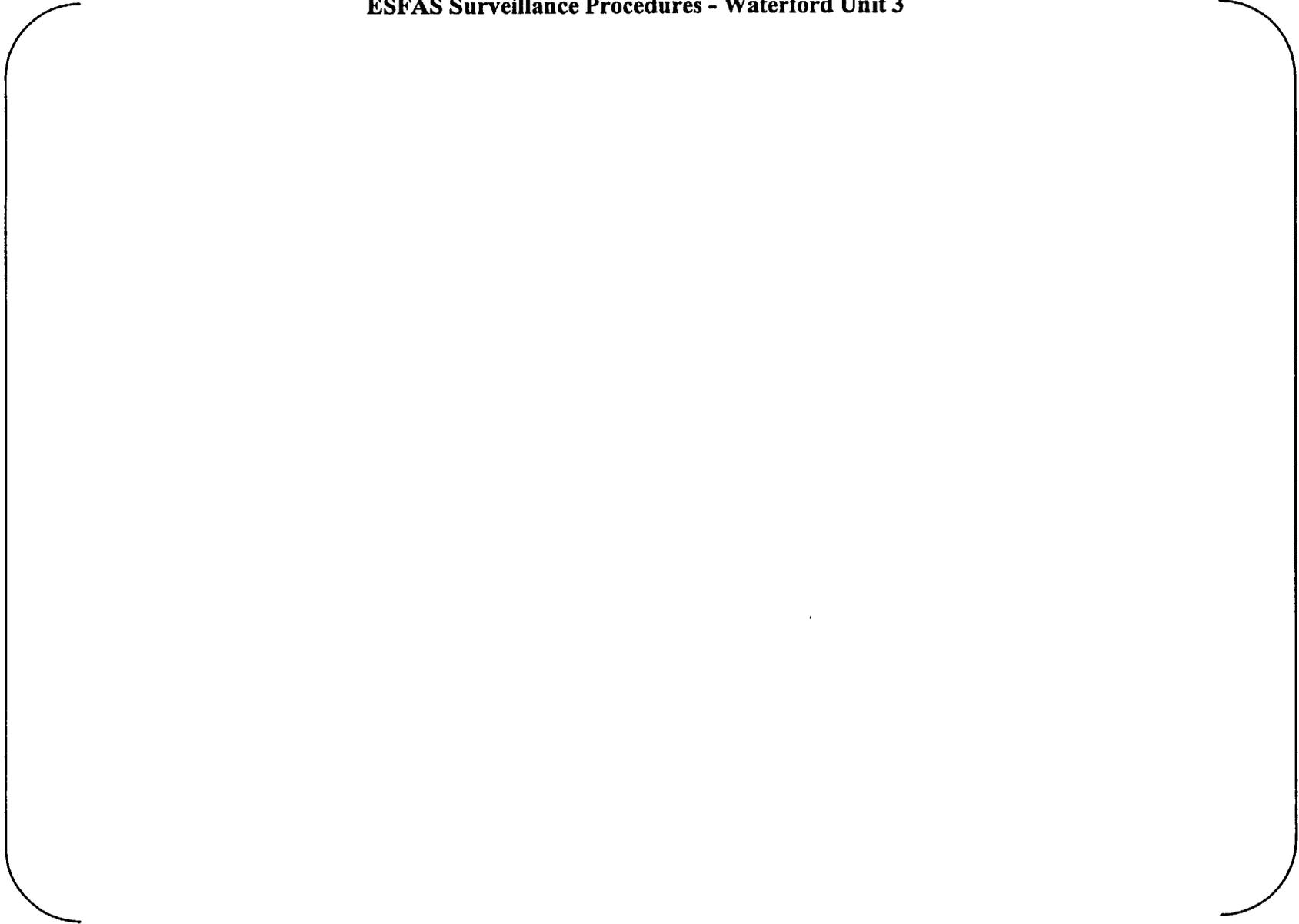


Figure D3.3-2
Under Voltage/Load Shed Surveillance Procedures - Waterford Unit 3



Figure D3.3-3
EDG Load Sequence Surveillance Procedures - Waterford Unit 3



D4.0 PROBABILISTIC ASSESSMENT OF THE PROPOSED STI CHANGE

As mentioned previously, Westinghouse performed a preliminary categorization and assessment of components tested by the integrated ESF test for WSES-3. WSES-3 used the preliminary assessment as a foundation and starting point to perform the PSA analysis described in this section. The categorization begins with the testing matrix described in Section D3.0. The matrix was used to identify components whose reliability appears to be demonstrated primarily/solely by the integrated ESF test.

The WSES-3 PSA Master List of basic events was reviewed to determine if and how the model addresses each such component or function. The results of the review were documented in a database that relates the components to the associated basic events. The components were categorized, based on the type of changes to the event frequencies or modeling details that would be needed in order to quantify the change in risk associated with the proposed change in the integrated ESF test frequency. The actual changes to the model and the requantification of the model was performed by WSES-3. The remainder of Section D4.0 is derived from the risk analyses performed by WSES-3.

The purpose of this plant-specific evaluation was to determine the change in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) that would be due to extending the current 18 month integrated engineered safety features testing (OP-903-115 and OP-903-116). The change would extend the interval to a staggered 36 month schedule with one train being tested each refueling outage.

The justification for the Containment Fan Cooler (CFC) flow verification test interval was not addressed by this evaluation.

Component functions tested solely by Integrated ESF Testing were determined by Westinghouse.

Load block components from Engineered Safety Features component loads were taken from FSAR Table 8.3-1, Emergency Diesel Generator Loading Sequence.

Each EDG has the capacity to start and accelerate the largest single load out of sequence with all other loads running.

Failure of a sequencer load block and component reload is tested in OP-903-029, OP-903-068, OP-903-094 and OP-903-095.

Common cause failure beta factor for breakers to trip is assumed to be 0.2 if not already calculated. The assumption is required due to scarcity of failure data.

Assumed that the independent failures of component breakers to trip on Loss of Offsite Power (LOOP) are adequately addressed by the binomial theorem for 2 or more of the component breakers failing.

Failure of the timing relay to actuate within the specified time interval is assumed to result in failure of the entire load block sequenced on the ESF bus in conjunction with another load block resulting in EDG failure. The frequency of this type of failure is conservatively assumed the same as for relay failure to actuate.

Failure to open one of the safety to non-safety tie breakers is assumed to fail the EDG. This is applicable to SSD Breakers for Buses 312A, 312B, 313A, 313B, 314A and 314B. This is already assumed for the

Revision 3 of the WSES-3 PSA model.

Failure to separate the safety bus from the grid on LOOP is assumed to fail the EDG. This is applicable to 4KV breakers 2A-8 and 3A-11 for EDG A and 2B-8 and 3B-11 for EDG B. This is addressed as a CCF between the breakers and independent failures.

Failure to strip a bus is assumed to fail the associated EDG. The breakers that are open on loss of offsite power are designated with a symbol consisting of a "T" in a box. This is applicable to Station Service Distribution (SSD) Breakers for Buses 3A32, 315A, 312AB, 313AB, 3B32 and 315B. The SSD Breakers for Buses 3A316 and 3B316 are already isolated from the EDGs by the stripping of the 3A32 and 3B32 breakers. That is, the 3A316 and 3B316 buses failing to trip would not fail the EDG unless the breakers for the 3A32 or 3B32 had already failed to strip the load.

Component trains with installed spare components that only have one component running per train are assumed to be susceptible to only one breaker failing to shed in order to account for idle swing components. The failure to strip would only be a confirmation since the components would already be separated from their associated bus. This assumption is used for swing components of High Pressure Safety Injection, Component Cooling Water and Essential Chillers.

Components needed to sequence back on include the swing components in an attempt to address potential recovery problems while recovering for an initially failed component.

The probability of breaker failing to trip on under-voltage assumed to be bounded by generic breaker failure probability.

The probability of a component failing to sequence on following EDG start and permissive signal from EDG is assumed to be bounded by the generic breaker failure probability.

Loss of Offsite Power initiator, %T5, is assumed to be the dominant initiator for sequences requiring components to be sequenced back on using the sequencer and tested only by the integrated ESF testing.

Common cause failure for buses and components failing to shed from both the 3A and 3B safety buses is assumed to be adequately addressed by ECC31XSHED event already in the model. This event is currently used to account for common cause failure of non-safety buses failing to shed from the safety buses. The common cause factor is adjusted for 36 month staggered vs. 18 month non-staggered testing intervals.

An incremental increase in CDF produces a proportional incremental increase in LERF. Ten percent of the proportional increase in CDF is conservatively assumed to result in LERF. The inability of plant operators to remove decay heat following a LOOP due to the failure of Emergency AC power or sequence on required components is assumed to result in a high-pressure core damage scenario. The high-pressure core damage scenario is assumed to result in an energetic reactor vessel head failure and containment failure from 1% to 10% of the time.

The AB electrical buses are aligned to the safety related 3A electrical train.

The failure of two or more components (as apposed to entire buses) to shed is conservatively assumed to result in EDG failure. The EDG is designed to start and accelerate the largest single load out of sequence, so the calculation conservatively bounds the many combinations that could result in failure by assuming any two loads failing to strip would fail the EDG when it attempted to start.

There are many components that are normally idle and would only get a confirmatory signal to strip. Except for swing components, all components are conservatively assumed as initially running and required to be stripped if they were designed to strip on loss of offsite power.

The conditional probability of containment isolation failure is assumed to be 1E-3.

D4.1 MODEL ANALYSIS

The integrated ESF surveillance procedures demonstrate that the systems will respond properly to an actuation signal. Many of the components tested by this test are tested by other surveillance tests that demonstrate the operability of the individual components on a more frequent basis.

Determination of Tested Components

The components that are only tested by the integrated ESF test were identified in order to determine the change in risk due to changing the surveillance interval of the integrated ESF test. Components that are tested by another action or surveillance on a the same or higher frequency as the current 18 month interval would have no impact due to the change in integrated ESF testing frequency.

Component Classification

Westinghouse identified the components that are only tested during the integrated ESF test and compared them to the PSA model logic to determine the impact on core damage due to failure of the component. The component functions were sorted into three categories, A, B and C (see Section D3.1.1).

The Category A components were divided into four subcategories to delineate the actions required to support the determination of the change in CDF and LERF.

- Category A1 These components and the tested functions are explicitly modeled in the PSA. These events were addressed by changing the event probability for basic events already in the model. The event probabilities were adjusted for the increase in standby time of a factor of two. This resulted in essentially doubling the failure probability for the component functions tested. The common cause failure factor would not change but the failure probability that it is used to determine the common cause failure probability would be increased.
- Category A2 These components and the tested functions are not modeled explicitly, but the model includes another component which subsumes the tested component. The failure of the modeled component was increased to account for the increase in failure probability of the subsumed component. This results in essentially doubling the failure probability of the subsumed component.
- Category A3 These components/functions have a potential adverse indirect impact on a modeled component, where this indirect effect is covered appropriately in the PSA model. For these components/functions, the model element representing the indirect effect was adjusted to reflect the proposed change in the integrated ESF test frequency.
- Category A4 These components are similar to Category A3 components except that the components are not modeled. The majority of these components are breakers that are

required to shed loads on the loss of offsite power. These components were added to the model in order to account for the indirect effects that were not already modeled.

The functions and components identified by Westinghouse were checked against the PSA model and basic events were added to the model to account for the functions that were required to be modeled. The individual basic events and their functions are described in the original Westinghouse categorization report.

Integration of Changes

The model was then updated to incorporate the changes required in order to model all the components/functions for the nominal 18 month testing frequency.

Quantification of Changes

The model was quantified two times in order to determine the increase in CDF and LERF due to changes in the testing frequency. The first quantification consisted of determining the CDF with the additional components included in the model with failure rates representative of an 18 month test interval. The model was then quantified with the failure rates corresponding to a 36 month test interval.

Change in CDF Determination

The difference between the 18 month CDF and the 36 month CDF is the increase in CDF due to extending the surveillance interval.

Change in LERF Determination

The change in LERF was determined using the following logic. The change in CDF is relative to the change in LERF. There are three possible components of LERF: (1) containment isolation failure, (2) containment bypass sequences and (3) sequences that challenge containment directly.

The conditional probability of containment isolation failure is assumed as 1E-3. The increase in LERF due failure of containment isolation failure would then be the increase in CDF times the conditional probability of containment isolation failure.

The probability of the containment bypass sequences of steam generator tube rupture and intersystem LOCA are unchanged by the equipment functions tested by the integrated ESF test. The safety injection actuation signal testing is performed in a different surveillance test.

The loss of AC coupled with the eventual failure of the EFW AB pump results in a high-pressure melt challenge to containment. The high-pressure melt phenomenon was assumed to result in containment failure up to 10% of the time. The corresponding change in LERF would then be bounded by 10% of the change in CDF.

The total change in LERF would be the sum of the individual components. This results in a change in LERF of .101 times the change in CDF. This is for all practical purposes 10% of the change in CDF.

Determination of Tested Components and Component Classification

The determination of tested components and component classification is based on component screening and categorization provided by Westinghouse. WSES-3 reviewed the Westinghouse report and finalized the categories prior to requantifying the change in risk.

Integration of Changes

Failure to shed – Individual Components

There are many components in which the failure to shed is not included in the model. In order not to complicate the model, the failure to shed of all the components is combined into two basic events that would cause a fail-to-start for each EDG. The probability of failure to shed on loss of offsite power is from the basic event database for the WSES-3 PSA model, Revision 3.

The failure to shed basic events was added to the EDG fails-to-start. The loads that did not shed would be loaded back onto the EDG when it starts resulting in the EDG being overloaded. The failure to shed basic events was tied to the EDG fails to start logic in order to keep the remaining Station Black Out (SBO) logic valid.

The polar crane breaker CRNEBKR31A-8A was excluded from the fails to shed list since it is a locked open breaker per OP-903-130.

The failure to shed individual components was handled using the binomial distribution to determine the likelihood of two or more components failing to shed resulting in a failure of the associated EDG to run. The "A" train has more components due to the "AB" train aligned to the "A" electrical bus for the quantification of the PSA model. The listing of "A" train components that could fail to shed is given in Table D4.1.1. The listing of "B" train components that could fail to shed is given in Table D4.1.2.

No.	Associated Breaker	Component Short Description
1	ACCEBKR315A-10H	ACCW WET COOLING TOWER A FAN 1 ACCEBKR315A-10H
2	ACCEBKR315A-10M	ACCW WET COOLING TOWER A FAN 2 ACCEBKR315A-10M
3	ACCEBKR315A-11H	ACCW WET COOLING TOWER A FAN 3 ACCEBKR315A-11H
4	ACCEBKR315A-11M	ACCW WET COOLING TOWER A FAN 4 ACCEBKR315A-11M
5	ACCEBKR315A-12H	ACCW WET COOLING TOWER A FAN 5 ACCEBKR315A-12H
6	ACCEBKR315A-12M	ACCW WET COOLING TOWER A FAN 6 ACCEBKR315A-12M
7	ACCEBKR315A-13H	ACCW WET COOLING TOWER A FAN 7 ACCEBKR315A-13H
8	ACCEBKR315A-13M	ACCW WET COOLING TOWER A FAN 8 ACCEBKR315A-13M
9	ACCEBKR3A-3	ACCW PUMP A ACCEBKR3A-3
10	BAMEBKR312A-2D	BORIC ACID MAKEUP PUMP B BAMEBKR312A-2D
11	BAMEBKR313A-3D	BORIC ACID MAKEUP PUMP A BAMEBKR313A-3D
12	CC EBKR315A-1F	DRY COOLING TOWER A FAN 1 CC EBKR315A-1F
13	CC EBKR315A-1M	DRY COOLING TOWER A FAN 2 CC EBKR315A-1M
14	CC EBKR315A-2F	DRY COOLING TOWER A FAN 3 CC EBKR315A-2F
15	CC EBKR315A-2M	DRY COOLING TOWER A FAN 4 CC EBKR315A-2M

**Table D4.1.1
Failure to Shed A Train Components**

No.	Associated Breaker	Component Short Description
16	CC EBKR315A-3F	DRY COOLING TOWER A FAN 5 CC EBKR315A-3F
17	CC EBKR315A-3M	DRY COOLING TOWER A FAN 6 CC EBKR315A-3M
18	CC EBKR315A-4F	DRY COOLING TOWER A FAN 7 CC EBKR315A-4F
19	CC EBKR315A-4M	DRY COOLING TOWER A FAN 8 CC EBKR315A-4M
20	CC EBKR315A-5F	DRY COOLING TOWER A FAN 9 CC EBKR315A-5F
21	CC EBKR315A-5M	DRY COOLING TOWER A FAN 10 CC EBKR315A-5M
22	CC EBKR315A-7F	DRY COOLING-TOWER A FAN 11 CC EBKR315A-7F
23	CC EBKR315A-7M	DRY COOLING TOWER A FAN 12 CC EBKR315A-7M
24	CC EBKR315A-8F	DRY COOLING TOWER A FAN 13 CC EBKR315A-8F
25	CC EBKR315A-8M	DRY COOLING TOWER A FAN 14 CC EBKR315A-8M
26	CC EBKR315A-9F	DRY COOLING TOWER A FAN 15 CC EBKR315A-9F
27	CC EBKR3A-2	COMPONENT COOLING WATER PUMP A CC EBKR3A-2
28	CCSEBKR317A-2M	CONTAINMENT COOLING FAN A CCSEBKR317A-2M
29	CCSEBKR317A-3M	CONTAINMENT COOLING FAN C CCSEBKR317A-3M
30	CDCEBKR31A-8B	CEDM COOLING FAN A CDCEBKR31A-8B
31	CDCEBKR31A-9B	CEDM COOLING FAN C CDCEBKR31A-9B
32	CHWEBKR311A-5M	CHILLED WATER PUMP A CHWEBKR311A-5M
33	CMUEBKR311A-4M	CCW MAKEUP PUMP A CMUEBKR311A-4M
34	CS EBKR3A-6	CONTAINMENT SPRAY PUMP A CS EBKR3A-6
35	CVCEBKR31A-5C	Charging Pump A
36	CVCEBKR31AB-4C	CHARGING PUMP AB CVCEBKR31AB-4C
37	DC-EBKR-311A-14D	Battery Charger A1
38	DC-EBKR-311AB-2D	Battery Charger AB1
39	DC-EBKR-311AB-2H	Battery Charger AB2
40	DC-EBKR-312A-3B	Battery Charger A2
41	EFWEBKR3A-10	EMERGENCY FEEDWATER PUMP A EFWEBKR3A-10
42	EGAEBKR312A-4F	EDG 3A-S AIR COMPR #1 EGA-EBKR-312A-4F
43	EGAEBKR312A-5F	EDG 3A-S AIR COMPR #2 EGA-EBKR-312A-5F
44	EG-EBKR312A-4D	EDG 3A-S SPACE HTR ES-EBKR-312A-4D
45	EGLBKR-312A-5D	EG A LUBE OIL HEATER EGL-EBKR-312A-5D
46	FP EBKR31AB-5A	MOTOR DRIVEN FIRE PUMP FP EBKR31AB-5A
47	HT-EBKR-312A-5M	CVCS SYSTEM A TRACING HT-EBKR-312A-5M
48	HVCEBKR311A-4H	CR AIR HANDLING UNIT A HVCEBKR311A-4H
49	HVCEBKR311A-5B	CR EMERGENCY FLTR UNIT A HVCEBKR311A-5B
50	HVC-EBKR311A-5D	CONT RM TOILET EXH FAN A E-34 HVC-EBKR-311A-5D
51	HVCEBKR313A-4F	CR HVAC EQUIPMENT ROOM AHU A HVCEBKR313A-4F
52	HVFEBKR314A-1G	FHB EQUIP RM EXH FAN E-21A HVFEBKR314A-1G
53	HVFEBKR314A-1J	FHB EFU E-35A HVFEBKR314A-1J
54	HVREBKR311A-14B	EFW PUMP ROOM A AHU HVR-EBKR-311A-14B
55	HVREBKR311A-14K	CHARGING PUMP ROOM A AHU HVREBKR311A-14K
56	HVREBKR311A-3H	RCA HVAC EQUIP RM EXHAUST FAN A HVREBKR311A-3H

Table D4.1.1 Failure to Shed A Train Components		
No.	Associated Breaker	Component Short Description
57	HVREBKR311A-5	CVAS EXHAUST FAN A HVREBKR311A-5F
58	HVREBKR311AB-5B	CCW PUMP ROOM AB AHU A HVREBKR311AB-5B
59	HVREBKR311AB-5H	CHARGING PUMP ROOM AB AHU A HVREBKR311AB-5H
60	HVREBKR313A-2M	RCA HVAC EQUIPMENT ROOM AHU A HVREBKR313A-2M
61	HVREBKR313A-4D	SDC HX A RM COOLER AH-3A HVREBKR313A-4D
62	HVREBKR313A-4K	SI PUMP ROOM A AHU-2 (SA) HVREBKR313A-4K
63	HVREBKR313A-4M	CCW PUMP ROOM A AHU HVREBKR313A-4M
64	HVREBKR313A-5D	CCW HX A RM COOLER AH-24A HVREBKR313A-5D
65	HVREBKR313A-5K	SI PUMP ROOM A AHU-2 (SC) HVREBKR313A-5K
66	HVREBKR3A-7	RAB NORMAL EXHAUST FAN A HVREBKR3A-7
67	IA-EBKR31A-9A	INST AIR COMPRESSOR A IA EBKR31A-9A
68	ID-EBKR311A-14F	SUPS MC NORMAL SUPPLY ID-EBKR-311A-14F
69	ID-EBKR311A-3M	SUPS A BYPASS SUPPLY ID-EBKR-311A-3M
70	ID-EBKR-311AB-3H	SUPS AB NORMAL SUPPLY ID-EBKR-311AB-3H
71	ID-EBKR312A-2B	SUPS MA NORMAL SUPPLY ID-EBKR-312A-2B
72	ID-EBKR312A-2F	SUPS A NORMAL SUPPLY ID-EBKR-312A-2F
73	ID-EBKR313A-4H	SUPS MA BYPASS SUPPLY ID-EBKR-313A-4H
74	ID-EBKR31A-8C	COMPUTER SUPS NORMAL SUPPLY
75	ID-EBKR31AB-3B	COMPUTER SUPS BYPASS SUPPLY
76	RFREBKR311A-2M	ESSENTIAL CHILLER A OIL PUMP RFR-EBKR-311A-2M
77	RFREBKR3A-9	ESSENTIAL CHILLER A RFREBKR3A-9
78	SBVEBKR31A-5B	SBV EXHAUST FAN A SBVEBKR31A-5B
79	SI-EBKR3A-4	HIGH PRESSURE SAFETY INJECTION PUMP A SI EBKR3A-4
80	SI-EBKR3A-5	LOW PRESSURE SAFETY INJECTION PUMP A SI EBKR3A-5
81	SVSEBKR311A-13K	BATTERY ROOM AB EXHAUST FAN A SVSEBKR311A-13K
82	SVSEBKR-311A-14H	BATTERY ROOM EXH FAN A SVS-EBKR-311A-14H
83	SVSEBKR311A-2F	BATTERY ROOM A EXHAUST FAN A SVSEBKR311A-2F
84	SVSEBKR311A-2H	COMPUTER BATTERY ROOM EXH FAN A SVSEBKR311A-2H
85	SVSEBKR311A-3F	BATTERY ROOM B EXHAUST FAN A SVSEBKR311A-3F
86	SVSMAHU001A & SVSEBKR313A-5H	SWITCHGEAR A MAIN AIR HANDLING UNIT SVSEBKR313A-5H
87	SVSMAHU002A & SVSEBKR311A-13B	SWITCHGEAR A AUX AIR HANDLING UNIT SVSEBKR311A- 13B

EDG A has 87 component loads that are tested for load shedding by OP-903-115. The failure probability using the binomial distribution for having two or more failures out of 87 components is [] per demand for an eighteen-month surveillance interval. The failure probability for the having two or more failures out of 87 components is [] per demand for a thirty-six month surveillance interval.

Table D4.1.2
Failure to Shed B Train Components

No.	Associated Breaker	Component Short Description
1	ACCEBKR315B-10H	ACCW WET COOLING TOWER B FAN 1 ACCEBKR315B-10H
2	ACCEBKR315B-10M	ACCW WET COOLING TOWER B FAN 2 ACCEBKR315B-10M
3	ACCEBKR315B-11H	ACCW WET COOLING TOWER B FAN 3 ACCEBKR315B-11H
4	ACCEBKR315B-11M	ACCW WET COOLING TOWER B FAN 4 ACCEBKR315B-11M
5	ACCEBKR315B-12H	ACCW WET COOLING TOWER B FAN 5 ACCEBKR315B-12H
6	ACCEBKR315B-12M	ACCW WET COOLING TOWER B FAN 6 ACCEBKR315B-12M
7	ACCEBKR315B-13H	ACCW WET COOLING TOWER B FAN 7 ACCEBKR315B-13H
8	ACCEBKR315B-13M	ACCW WET COOLING TOWER B FAN 8 ACCEBKR315B-13M
9	ACCEBKR3B-6	ACCW PUMP B ACCEBKR3B-6
10	CC EBKR315B-1F	DRY COOLING TOWER B FAN 1 CC EBKR315B-1F
11	CC EBKR315B-1M	DRY COOLING TOWER B FAN 2 CC EBKR315B-1M
12	CC EBKR315B-2F	DRY COOLING TOWER B FAN 3 CC EBKR315B-2F
13	CC EBKR315B-2M	DRY COOLING TOWER B FAN 4 CC EBKR315B-2M
14	CC EBKR315B-3F	DRY COOLING TOWER B FAN 5 CC EBKR315B-3F
15	CC EBKR315B-3M	DRY COOLING TOWER B FAN 6 CC EBKR315B-3M
16	CC EBKR315B-4F	DRY COOLING TOWER B FAN 7 CC EBKR315B-4F
17	CC EBKR315B-4M	DRY COOLING TOWER B FAN 8
18	CC EBKR315B-5F	DRY COOLING TOWER B FAN 9
19	CC EBKR315B-5M	DRY COOLING TOWER B FAN 10
20	CC EBKR315B-7F	DRY COOLING TOWER B FAN 11
21	CC EBKR315B-7M	DRY COOLING TOWER B FAN 12
22	CC EBKR315B-8F	DRY COOLING TOWER B FAN 13
23	CC EBKR315B-8M	DRY COOLING TOWER B FAN 14
24	CC EBKR315B-9F	DRY COOLING TOWER B FAN 15
25	CC-EBKR3B-8	COMPONENT COOLING WATER PUMP B CC EBKR3B-8
26	CCSEBKR317B-2M	CONTAINMENT COOLING FAN D CCSEBKR317B-2M
27	CCSEBKR317B-3M	CONTAINMENT COOLING FAN B CCSEBKR317B-3M
28	CDCEBKR31B-8B	CEDM COOLING FAN B CDCEBKR31B-8B
29	CDCEBKR31B-9B	CEDM COOLING FAN D CDCEBKR31B-9B
30	CHWEBKR311B-5M	CHILLED WATER PUMP B CHWEBKR311B-5M
31	CMUEBKR311B-4M	CCW MAKEUP PUMP B CMUEBKR311B-4M
32	CS EBKR3B-5	CONTAINMENT SPRAY PUMP B CC EBKR3B-5
33	CVCEBKR31B-6C	Charging Pump B
34	DC-EBKR-311B-14D	Battery Charger B1
35	DC-EBKR-312B-3B	Battery Charger B2
36	EFWEBKR3B-2	EMERGENCY FEEDWATER PUMP B EFWEBKR3B-2
37	EGAEBKR312B-4F	EDG 3B-S AIR COMPR #1 EGA-EBKR-312B-4F
38	EGAEBKR312B-5F	EDG 3B-S AIR COMPR #2 EGA-EBKR-312B-5F
39	EG-EBKR312B-4D	EDG 3B-S SPACE HTR ES-EBKR-312B-4D
40	EGLBKR312B-5D	EG B LUBE OIL HEATER EGL-EBKR-312B-5D
41	HT-EBKR-312B-5M	CVCS SYSTEM B TRACING HT-EBKR-312B-5M

Table D4.1.2 Failure to Shed B Train Components		
No.	Associated Breaker	Component Short Description
42	HVCEBKR311B-4H	CR AIR HANDLING UNIT B HVCEBKR311B-4H
43	HVCEBKR311B-5B	CR EMERGENCY FLTR UNIT B HVCEBKR311B-5B
44	HVC-EBKR311B-5D	CONT RM TOILET EXH FAN B E-34 HVC-EBKR-311B-5D
45	HVCEBKR313B-4F	CR HVAC EQUIPMENT ROOM AHU B HVCEBKR313B-4F
46	HVFEBKR314B-1G	FHB EQUIP RM EXH FAN E-21B HVFEBKR314B-1G
47	HVFEBKR314B-1J	FHB EFU E-35B HVFEBKR314B-1J
48	HVREBKR-311B-14B	EFW PUMP ROOM B AHU HVR-EBKR-311B-14B
49	HVREBKR311B-14K	CHARGING PUMP ROOM B AHU HVREBKR311B-14K
50	HVREBKR311B-5F	CVAS EXHAUST FAN B HVREBKR311B-5F
51	HVREBKR313B-4D	SDC HX B RM COOLER AH-3B HVREBKR313B-4D
52	HVREBKR313B-4K	SI PUMP ROOM B AHU 1B HVREBKR313B-4K
53	HVREBKR313B-4M	CCW PUMP ROOM B AHU HVREBKR313B-4M
54	HVREBKR313B-5D	CCW HX B RM COOLER AH-24B HVREBKR313B-5D
55	HVREBKR313B-5K	SI PUMP ROOM B AHU-2 (SD) HVREBKR313B-5K
56	HVREBKR3B-13	RAB NORMAL EXHAUST FAN B HVREBKR3B-13
57	IA-EBKR31B-9A	INST AIR COMPRESSOR B IA EBKR31B-9A
58	ID-EBKR-311B-14F	SUPS MD NORMAL SUPPLY ID-EBKR-311B-14F
59	ID-EBKR312B-2B	SUPS MB NORMAL SUPPLY ID-EBKR-312B-2B
60	ID-EBKR312B-2F	SUPS 3B (Norm Feeder)
61	ID-EBKR313A-2B	SUPS MC BYPASS SUPPLY ID-EBKR-313A-2B
62	ID-EBKR313B-2B	SUPS MD BYPASS SUPPLY ID-EBKR-313B-2B
63	ID-EBKR313B-3H	SUPS B BYPASS SUPPLY ID-EBKR-313B-3H
64	ID-EBKR313B-4H	SUPS MB BYPASS SUPPLY ID-EBKR-313B-4H
65	RFREBKR311B-2M	ESSENTIAL CHILLER B OIL PUMP RFR-EBKR-311B-2M
66	RFREBKR3B-14	ESSENTIAL CHILLER B RFREBKR3B-14
67	SBVEBKR31B-5B	SBV EXHAUST FAN B SBVEBKR31B-5B
68	SI-EBKR3B-3	HIGH PRESSURE SAFETY INJECTION PUMP B SI EBKR3B-3
69	SI-EBKR3B-4	LOW PRESSURE SAFETY INJECTION PUMP B SI EBKR3B-4
70	SVSEBKR311B-13K	BATTERY ROOM AB EXHAUST FAN B SVSEBKR311B-13K
71	SVSEBKR311B-14H	BATTERY ROOM EXH FAN B SVS-EBKR-311B-14H
72	SVSEBKR311B-2F	BATTERY ROOM A EXHAUST FAN B SVSEBKR311B-2F
73	SVSEBKR311B-2H	COMPUTER BATTERY ROOM EXH FAN B SVSEBKR311B-2H
74	SVSEBKR311B-3F	BATTERY ROOM B EXHAUST FAN B SVSEBKR311B-3F
75	SVSMAHU001B & SVSEBKR313B-5H	SWITCHGEAR B MAIN AIR HANDLING UNIT SVSEBKR313B-5H
76	SVSMAHU002B & SVSEBKR311B-13B	SWITCHGEAR B AUX AIR HANDLING UNIT SVSEBKR311B-13B

EDG B has 76 component loads that are tested for load shedding by OP-903-116. The failure probability using the binomial distribution for having two or more failures out of 76 components is { } per demand for an eighteen-month surveillance interval. The failure probability for the having two or more failures out of 76 components is { } per demand for a thirty-six month surveillance interval.

The CCF failure rate for the eighteen-month surveillance interval would be { } per demand using the CCF beta factor of 0.2. The CCF Beta factor was implemented as a lambda factor in the basic event data base multiplied with the fail-to-shed basic event probability. The CCF failure rate for the thirty-six month surveillance interval would be { } per demand. These values would be the same value for both trains of safety related power.

The basic events added to the model for these events were:

- ECBSTRIPAY – CCF probability for train A components failing to shed on LOOP
- ECBSTRIPBY – CCF probability for train B components failing to shed on LOOP
- EBNSTRIPAA – Binomial probability for train A components failing to shed on LOOP
- EBNSTRIPBB – Binomial probability for train B components failing to shed on LOOP

The individual component fail-to-shed assessments and model changes are keyed on the breaker associated with each component.

Failure to shed – Electrical Buses

The applicable existing electrical bus fail to shed basic events are ECB312A8MD, ECB312B8MD, ECB313A8MD, ECB313B8MD, ECB314A2MD and ECB314B2MD. These basic events are for the failure to shed the safety to non-safety tie-breakers for the 312A, 313A, 314A, 312B, 313B and 314B. The existing bus fails to shed events are listed in Table D4.1.3.

The basic event, ECC31XSHED, is the common cause failure term between the 3A and 3B safety buses for buses/breakers failing to shed. The failure to shed the other buses that are designed to shed on under-voltage and not already included in the model was explicitly included in the model. The CCF failure between the 3A and 3B buses will change from a non-staggered to a staggered interval. The change in the CCF factor for staggered testing was calculated using the same methodology as was used for Revision 3 of the WSES-3 Level 1 model.

**Table D4.1.3
Existing Bus Fails to Shed Events**

Component UNID	Basic Event	Short Description
SSDEBKR312A-8M	ECB312A8MD	MCC-312A SAFETY TO NONSAFETY TIE
SSDEBKR312B-8M	ECB312B8MD	MCC-312B SAFETY TO NONSAFETY TIE
SSDEBKR313A-8M	ECB313A8MD	MCC-313A SAFETY TO NONSAFETY TIE
SSDEBKR313B-8M	ECB313B8MD	MCC-313B SAFETY TO NONSAFETY TIE
SSDEBKR314A-2M	ECB314A2MD	MCC-314A SAFETY TO NONSAFETY TIE
SSDEBKR314B-2M	ECB314B2MD	MCC-314B SAFETY TO NONSAFETY TIE
CCF	ECC31XSHED	Common Cause Between Safety Buses

For the eighteen-month surveillance interval the failure rate would be { } per demand. For the thirty-six month interval the failure rate would be { } per demand. The new bus fails to shed events are listed in Table D4.1.4.

The breakers that tie the 3 safety bus to the 2 non-safety bus (4KVEBKR3A(B)-8 and 4KVEBKR3A(B)-11) were considered as independent failures and as having potential common cause failures. The CCF failure rate for the eighteen-month surveillance interval would be { } per demand using a CCF beta

factor of 0.2. The CCF failure rate for the thirty-six month surveillance interval would be { } per demand.

**Table D4.1.4
New Bus Fails to Shed Events**

Component UNID	Basic Event	Short Description
4KVEBKR2A-8	ECB0002A8Y	2A BUS Tie to 3A
4KVEBKR2B-8	ECB0002B8Y	2B BUS TIE TO SWITCHGEAR 3B
SSDEBKR3A-8	ECB0003A8Y	32A SUPPLY SSDEBKR3A-8
SSDEBKR3B-7	ECB0003B7Y	MCC-315B SUPPLY
SSDEBKR3B-9	ECB0003B9Y	32B SUPPLY SSDEBKR3B-9
4KVEBKR3A-11	ECB003A11Y	3A BUS TIE TO SWITCHGEAR 2A
SSDEBKR3A-13	ECB003A13Y	MCC-315A SUPPLY
4KVEBKR3B-11	ECB003B11Y	3B BUS TIE TO SWITCHGEAR 2B
SSDEBKR31AB-2C	ECB31AB2CY	MCC-312AB SUPPLY
SSDEBKR31AB-3A	ECB31AB3AY	MCC-313AB SUPPLY
CCF	ECB2TO3BAY	CCF 3A BUS TIE TO SWITCHGEAR 2A
CCF	ECB2TO3BBY	CCF 3B BUS TIE TO SWITCHGEAR 2B

The individual bus breaker fails to shed assessments and model changes are keyed on the associated breaker.

Failure of timing relays in sequencer – Incorrect timing

The failure of a sequencer timing relay to actuate is included in the model and tested by another surveillance, but the failure of a sequencer timing relay to actuate within the correct time interval is not addressed in the model. The failure of the timing of the sequencer relays is added to the model as a basic event for the associated EDG failing to start in order to capture the potential failure mechanism of two load blocks being sequenced on at the same time.

The A sequencer has 10 timing relays and a single failure of one is assumed to fail the EDG due to sequencing two loads on at the same time. The number of timing relays is different between sequencers A and B due to the computer SUPS being connected by the A sequencer. The modeled event, ERETIMESAX, was an aggregate of all the relays. The failure rate of the individual relays was assumed to be the same as that for failure of a relay. The value used for the eighteen-month surveillance interval was { } per demand. This is the { } per demand failure rate times the ten relays for the A train. The thirty-six month failure rate was twice the eighteen-month failure rate to account for the increase in time between the surveillances.

The B sequencer has 9 timing relays and a single failure of one is assumed to fail the EDG due to sequencing two loads on at the same time. The modeled event, ERETIMESSBX, was an aggregate of all the relays. The failure rate of the individual relays was assumed to be the same as that for failure of a relay. The value used for the eighteen-month surveillance interval was { } per demand. This is the { } per demand failure rate times the nine relays for the B train. The thirty-six month failure rate was twice the eighteen-month failure rate to account for the increase in time between the surveillances.

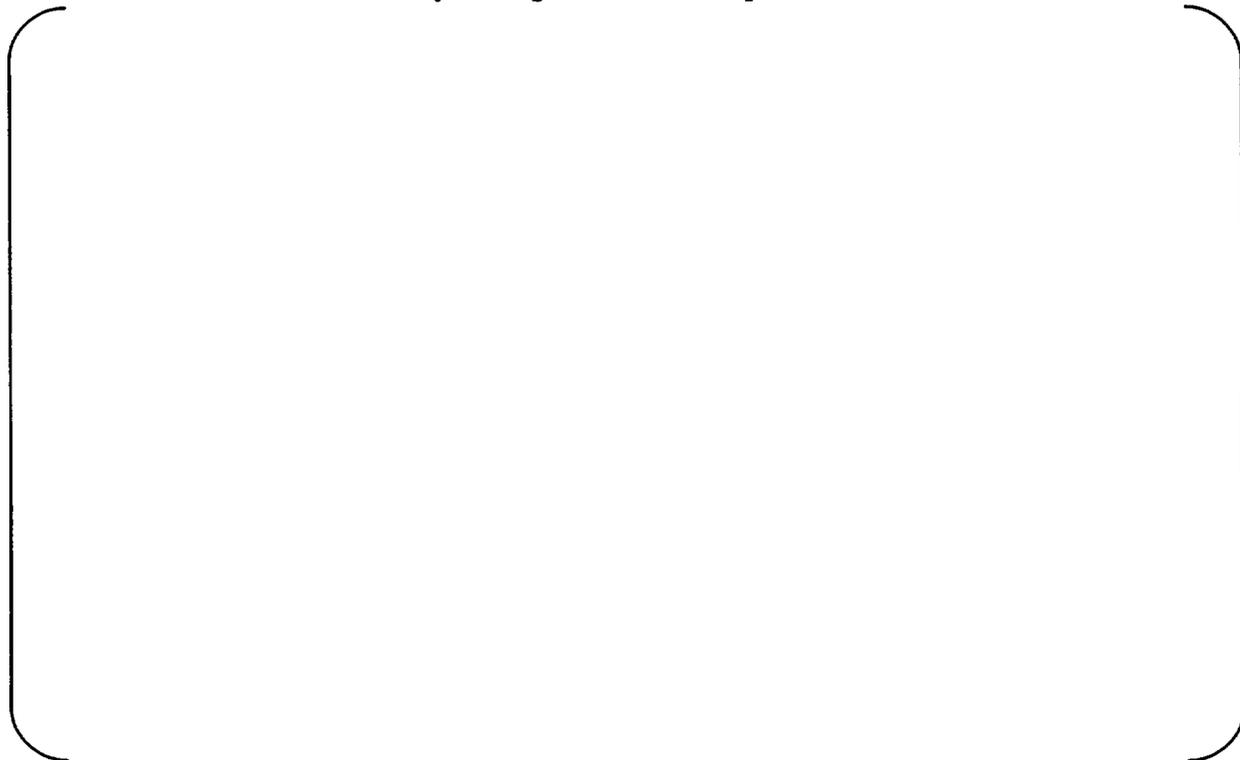
Failure of components to sequence on following LOOP – Failure to sequence on

The failure of the components required for success in the PSA from sequencing-on would result in the failure to provide the PSA functions provided by the component. This would result in failure of the components to sequence on following a LOOP. The probability of this failure was assumed to be equal to that of a circuit breaker demand failure. All of the components except for the wet and dry cooling towers are handled as individual basic events “AND’ed” with the loss of offsite power initiator (%T5) and incorporated into the PSA model in the fails to start logic of the component.

The wet and dry cooling towers are handled as a combination of independent failures with binomial probabilities and common cause failure factors. The binomial treatment is required to account for the different success criteria for LOCAs and transients. For the case of a LOCA, the wet cooling towers are assumed to fail if all eight fans in a train fail and the dry cooling tower is assumed to fail when eight or more fans fail. For the case of a transient, the wet cooling tower is assumed to fail if two or more fans were to fail and the dry cooling tower is assumed to fail if two or more fans fail.

The failure probabilities for the case of the wet and dry cooling towers during LOCA and transient conditions are given in Table D4.1.5. The total failure probability used in the model was the sum of the common cause and binomial failure probabilities.

Table D4.1.5
Wet and Dry Cooling Tower Fail to Sequence Probabilities



Quantification of Changes

The altered Revision 3 of the PSA model was quantified twice. Once with the eighteen-month failure probabilities for the basic event tested by the integrated ESF surveillance, and once with the thirty-six month failure probabilities. The model with the eighteen-month failure probabilities resulted in a CDF of { } per/yr. The model with the thirty-six month failure probabilities resulted in a CDF of { } per/yr.

Change in CDF Determination

The resulting change in CDF is then the difference between the thirty-six month CDF and eighteen month CDF. The difference is { }, which is a { } per/yr increase.

Change in LERF Determination

The change in LERF was assumed to be 10% of the change in CDF. The change in LERF is { } per/yr which is an { } per/yr increase.

D4.2 SCOPE OF PSA

The WSES-3 Revision 3 PSA model is an at-power, internal-events PSA. Only Level 1 is explicitly modeled. The model is routinely updated as a result of plant changes, increasing fidelity for particular applications and new quantification techniques.

D4.2.1 At-Power Model Structure

Typical large-linked fault tree techniques underlie the analysis. For illustration purposes, WSES-3 has small event trees that capture the sequences quantified with the model. These illustrations became the basis for the top logic employed in the large fault tree model created for WSES-3.

The model has detailed trees for each of the front-line systems identified in the top logic illustrated on the event trees. Likewise, the front-line systems spawn the need for support system trees. To ensure traceability, Entergy Operations keeps a set of documents that catalogue data values and assumptions for the front-line and support system trees.

The model is quantified with a mix of generic and WSES-3 plant-specific data. The scope of the plant-specific data analysis included initiating event frequencies and equipment for which plant-specific data allows for statistically meaningful estimates of failure rates and failure probabilities. The plant-specific data arises, in part, from a review of Licensee Event Reports, monthly plant reports, and in internal Condition Reports. These capture important plant failure modes, events, and trends.

The model includes quantified human failure events. The Human Reliability Analysis (HRA) was completely reanalyzed since the Peer Review using an industry standard HRA methodology (EPRI Sharp1), with input from a SRO.

D4.2.2 Shutdown Risk Assessment

Shutdown modes are outside the scope of the WSES-3 Revision 3 PSA model.

D4.2.3 PSA Detail Needed for Change

The WSES-3 Revision 3 PSA model explicitly models the functions associated with ESFAS. Key modeling features are discussed below.

D4.2.3.1 Modeling and Quantification

Common Cause

CEOG Task 1029 Guidelines were used to evaluate what components were candidate groups for CCF. The CCF factors were implemented as Beta factors in the Revision 3 model. The CCF Common cause basic events have been directly incorporated into the fault tree models, and represent the failure of all components within a defined group by a specified failure mode, e.g. all safety injection pumps fail to start on demand due to common causes. Other key common cause impacts related to the EDGs are 125VDC batteries, CCW pumps and failure of load breakers to strip.

Quantification

The large linked-fault-tree model for WSES-3 is configured, edited, and analyzed with the CAFTA suite of codes from EPRI. The quantification was done with the powerful FORTE engine.

D4.2.3.2 Truncation Limits

The truncation for CDF was set at 1.0E-10. That is three to four orders of magnitude below the most significant sequences identified in the analysis.

D4.3 QUALITY OF WATERFORD UNIT 3 PSA

Entergy Operations utility personnel have constructed the Revision 3 PSA model with a strong commitment toward developing a complete and accurate PSA. This commitment can be seen through the following elements:

- Formal qualification program for the PSA staff
- Use of procedures to control PSA processes
- Independent reviews (checks) of PSA documents
- Comprehensive PSA Configuration Control Program
 1. Process to control PSA quantification software
 2. Active open items list
 3. Interface with the site corrective action program
 4. Process to maintain configuration of previous risk-informed decisions
- Peer reviews
- Participation in the CEOG cross comparison process
- Incorporation, where applicable, of CEOG PSA Technical Positions
- Commitment of continuous quality improvement

The Revision 2 – Change 1 model was peer reviewed in January 2000. The Revision 3 PSA model for this analysis contains several refinements, but uses techniques and practices similar to the peer reviewed version.

Considering the scope, level of detail, processes and peer review results, the Revision 3 PSA model is sufficient to support a technically defensible and realistic evaluation of the risk associated with this amendment request.

D4.4 PSA SOFTWARE

A variety of MS Windows executables and DLLs from the CAFTA suite are used for this analysis. All software executed in a configuration documented according to QA procedures.

D4.4.1 CAFTA

CAFTA is a commercial product. It comprises a fault tree editor and event data base editor built to easily edit and create input files for any number of cutset quantification engines. CAFTA also includes a cutset editor, which is used to analyze the results of a quantification.

D4.4.2 PRAQuant

PRAQuant is an executive program for the CATA suite. In this analysis it was used to direct a serial quantification of CDF for the base case and the hypothetical case.

D4.4.3 FORTE

FORTE is the powerful quantification engine that allows rapid quantification of cutsets from large linked fault trees down to user selected truncation limits.

D4.5 RESULTS AND CONCLUSIONS

The calculated increase in Core Damage Frequency (Δ CDF) due to increasing the surveillance interval from an 18 month interval to a 36 month staggered test interval is [].

The estimated change in Large Early Release Frequency (Δ LERF) is [].

WCAP 15830-NP, Rev 00

Westinghouse Non-Proprietary Class 3



Westinghouse Electric Company LLC
2000 Day Hill Road
Windsor, CT 06095-0500